Bundesamt
für Sicherheit in der
Informationstechnik

ITIL und Informationssicherheit

Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Der Trend zum Outsourcing und der zunehmende Druck, immer aufwendigere IT-Prozesse zu steuern, haben ITIL in den Blickpunkt von Behörden und Unternehmen gerückt.

Diese Studie bietet für CEOs, Manager und Entscheider eine Einführung in ITIL und stellt dar, wie durch ein Zusammenspiel von IT-Sicherheit, IT-Betrieb und IT-Services Synergieeffekte erzielt werden können, die zu geringen Kosten, mehr IT-Sicherheit, besserer Servicequalität und gesteigerter Kundenzufriedenheit führen.

Die Studie wurde im Auftrag des BSI von der HiSolutions AG in Berlin erstellt (Internet: http://www.hisolutions.com).

Bundesamt für Sicherheit in der Informationstechnik
Referat I 1.4 IT-Sicherheitsmanagement und IT-Grundschutz
Postfach 200363
53133 Bonn
Tel.: +49 (0) 1888-9582-369
E-Mail: gshb@bsi.bund.de
Internet: http://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2005

Inhaltsverzeichnis

1 Einleitung 4

2 ITIL im Überblick 5

2.1 ITIL und der Weg zur Service- und Kundenorientierung in der IT 5

2.2 Ursprung und Entwicklung von ITIL 6

2.3 Philosophie und Einflüsse 7

2.4 Organisationen, Standards und Zertifizierbarkeit 7

2.4.1 BS 15000 – Standardisiertes Management von IT-Services 7

2.4.2 BS 7799 / ISO 17799 – Standardisiertes Management der Informationssicherheit 8

2.5 ITIL: Stärken und Schwächen 8

2.6 ITIL: Chancen und Risiken aus Sicht des Sicherheitsmanagements 9

3 Die wichtigsten ITIL-Bestandteile 10

3.1 The Business Perspective 10

3.2 Service Delivery 11

3.3 Service Support 11

3.4 Infrastructure Management 12

3.5 Applications Management 12

3.6 Sicherheitsmanagement (Security Management) 12

3.7 Zusammenfassung 13

4 Zusammenhänge zwischen IT-Service- und IT-Sicherheitsmanagement 14

4.1 Service Support und Sicherheitsmanagement 14

4.1.1 Service Desk 14

4.1.2 Störungsmanagement (Incident Management) 15

4.1.3 Problemmanagement (Problem Management) 17

4.1.4 Änderungsmanagement (Change Management) 19

4.1.5 Versionsmanagement (Release Management) 20

4.1.6 Konfigurationsmanagement (Configuration Management) 22

4.2 Service Delivery und Sicherheitsmanagement 23

4.2.1 Service Level Management 23

4.2.2 Verfügbarkeitsmanagement (Availability Management) 25

4.2.3 Kapazitätsmanagement (Capacity Management) 26

4.2.4 Service Continuity Management 27

4.2.5 Finanzmanagement (Financial Management) 28

5 Gegenüberstellung ITIL und IT-Grundschutzhandbuch 30

6 Fazit 31

7 Verweise 32

1 Einleitung

Das Thema IT-Sicherheit wurde von vielen Unternehmen und Behörden, gerade durch den Druck einer zunehmenden Abhängigkeit kritischer Prozesse von der IT, oftmals völlig unabhängig von den existierenden IT-Serviceprozessen behandelt. Ein IT-Sicherheitsbeauftragter befindet sich demzufolge – oft unfreiwillig – in einer eher konfrontativen Position gegenüber dem IT-Bereich. Dabei spielt es weniger eine Rolle, wo das Thema IT-Sicherheit in Behörden oder Unternehmen organisatorisch angesiedelt ist, als dass das jeweilige Selbstverständnis des Aufgabenschwerpunktes und der Vorgehensweise in den Bereichen IT-Sicherheit und IT-Betrieb fehlt. So wie die Revision als reine abschließende Prüfinstanz oder als projektbegleitender Partner betrachtet werden kann, so kann auch der IT-Sicherheitsbeauftragte sowohl als eine aus Sicherheitsgründen notwendige „Bremse“ oder als produktiver Partner des IT-Betriebs aufgefasst werden.

ITIL ist ein Best Practice Referenzmodell für IT-Serviceprozesse und sieht als solches Sicherheitsaspekte als unverzichtbaren Bestandteil eines ordnungsgemäßen IT-Betriebs an – denn was wären Best Practice IT-Prozesse, deren Sicherheit nicht gewährleistet ist? ITIL bietet somit die Basis, Verbindungen bezüglich der Sicherheitsanforderungen zwischen Geschäfts- und IT-Prozessen zu erkennen und Synergiepotenziale zu nutzen.

Diese Veröffentlichung soll somit nicht nur als kurze Einführung in das Thema ITIL dienen, sondern gerade auch Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management aufzeigen.

2 ITIL im Überblick

Die „IT Infrastructure Library“ (ITIL) hat sich inzwischen als weltweit akzeptierter Defacto-Standard für Gestaltung, Implementierung und Management wesentlicher Steuerungsprozesse in der IT etabliert. ITIL ist eine Verfahrensbibliothek, die hierfür Best Practices liefert – also Erfahrungen aus der Praxis zusammenträgt und vermittelt.

Das Ziel von ITIL besteht im Wesentlichen darin, die bislang meist technologiezentrierte IT-Organisation prozess-, service- und kundenorientiert auszurichten. Damit sind die ITIL-Empfehlungen eine entscheidende Grundlage für zuverlässige, sichere und wirtschaftliche IT-Dienstleistungen (IT-Services).

ITIL ist technologie- und anbieterunabhängig. ITIL ist so generisch gehalten, dass die dort formulierten Empfehlungen unabhängig von der konkret eingesetzten Hardware und Software bzw. von Dienstleistern (wie etwa Outsourcing-Anbietern) sind. Allerdings weisen Vorgehens- und Beratungsmodelle vieler Dienstleister starke Ähnlichkeiten und Parallelen mit ITIL auf – entweder setzen sie direkt auf ITIL-Vorschlägen oder aber auf den hierfür zugrunde liegenden Erfahrungen im IT-Betrieb auf.

Das gesammelte ITIL-Wissen ist öffentlich zugänglich. Es ist in einer Bibliothek von circa 40 englischsprachigen Publikationen verfügbar. Zwei wesentliche Bestandteile von ITIL, die Managementprozesse zur Unterstützung und Lieferung von IT-Services (Service Support, Service Delivery), wurden zudem bereits in einer deutschsprachigen Ausgabe zusammengefasst, übersetzt und überarbeitet (siehe [1]).

2.1 ITIL und der Weg zur Service- und Kundenorientierung in der IT

Informationsmanagement hat sich in den vergangenen 25 Jahren dank einer rasanten technologischen Entwicklung zu einem der zentralen Erfolgsfaktoren für alle Arten von Institutionen - Unternehmen, Behörden, aber auch Forschungsinstitutionen - entwickelt.

Der erste Zyklus dieser Entwicklung fand wahrscheinlich zur Jahrtausendwende mit der raschen Etablierung von Internet-Dienstleistungen und Electronic Business seinen Höhepunkt.

Die IT-Organisationen haben in dieser Zeit vor allem gelernt, Informations- und Kommunikationstechnologien zu beherrschen. Entstanden sind IT-Betriebsorganisationen, deren Teams sich in starkem Maß auf konkrete Technologien oder Anwendungen (Netze, Server, Speicher, ...) spezialisiert haben. IT-Organisationen mit einseitigem Technologie-Fokus haben zunehmend ein Problem, das von verschiedenen Faktoren getrieben wird:

1. Die Anwender verbinden mit dem Betrieb ihrer IT wachsende Qualitätsansprüche bei zunehmendem Kostenbewusstsein.
2. Die hohe Abhängigkeit von der IT in Verbindung mit zunehmender Komplexität und anhaltenden Unsicherheiten im gesellschaftlichen Umfeld erhöhen zudem Risikobewusstsein und Sicherheitsanforderungen. Dazu tragen auch zunehmend gesetzliche Anforderungen bei.
3. Die Kunden und Anwender fordern von der IT mehr Flexibilität und Anpassbarkeit. Bei verändertem IT-Bedarf sollen auch die Leistungs- und Kostenstrukturen der IT mitziehen.
4. Die kürzeren Technologie- und Produktlebenszyklen in der IT führen dazu, dass schon längst nicht mehr jedes Know-how in Behörden und Unternehmen selbst entwickelt und gesichert werden kann. Die wachsenden Anforderungen müssen durch eine begrenzte Zahl von IT-Fachkräften erfüllt werden. Umfassendes Know-how in allen IT-Belangen können heute nur noch die großen IT-Organisationen vorhalten, so dass der Reiz des Outsourcings steigt.
5. Ein weiterer Trend ist die zunehmende Verfügbarkeit von qualifiziertem Fachpersonal in Entwicklung und Betrieb auch in Niedriglohnländern. Mit der Globalisierung von IT-Bedarf und -Nachfrage globalisieren sich daher auch die Serviceangebote.

6. Bei der Gestaltung von Verträgen (SLAs) und der Definition von Prozessen wurden bisher in der Praxis viele Fehler gemacht, da keine standardisierten Prozesse und Vorgehensmodelle zur Anwendung kamen.

Daraus resultieren einige Herausforderungen, die für IT-Organisationen heute einen hohen Veränderungsdruck hervorrufen: Die zentralen Herausforderungen bestehen darin,

- durch Prozessorientierung die Fähigkeit zu gewinnen, Ergebnisse mit konstanter Qualität und Sicherheit zu liefern.
- durch Serviceorientierung die eigenen Leistungen in Leistungspakete zu bündeln und möglichst weitgehend zu standardisieren, diese mit Kunden verbindlich zu vereinbaren sowie externe Service Provider zielgerichtet zu steuern.
- durch Kundenorientierung die Fähigkeit zu entwickeln, IT-Bedarf und Wünsche der Kunden früher und besser zu verstehen und sich schneller an veränderte Anforderungen anzupassen.
- die Komplexität des IT-Sicherheitsmanagements durch moderne Managementmethoden, die Erfahrungen aus anderen Fachgebieten wie Qualitätsmanagement und Betriebswirtschaft nutzen, besser zu beherrschen und in bestehende Organisationsstrukturen und Abläufe zu integrieren.

Hier tritt also lediglich beim IT-Betrieb eine Entwicklung ein, die in anderen Branchen und Dienstleistungsbereichen längst wirksam wurde und deshalb folgerichtig und sinnvoll ist.

ITIL liefert für die Umsetzung dieser Veränderungen in konkreten Prozessen

- grundsätzliche Anforderungen,
- konkrete Prozessziele,
- grobe Gestaltungsvorschläge in Form von Mustern für Verfahren und Rollen,
- Schnittstellenempfehlungen für die Prozessintegration,
- Hinweise zu kritischen Erfolgsfaktoren und Einführungsrisiken,
- Vorschläge möglicher Messgrößen für das Prozessmanagement (Key Performance Indikatoren) und
- Wissen über das Wirken der Steuerungsprozesse im Zusammenhang.

2.2 Ursprung und Entwicklung von ITIL

Seinen Ursprung hat das ITIL-Rahmenwerk in der zweiten Hälfte der achtziger Jahre, als in britischen Regierungsbehörden grundsätzliche Zweifel an der Effizienz des IT-Einsatzes aufkamen. Festgestellt wurde ein Mangel an standardisierten Verfahren zur zweckmäßigen Etablierung und Abwicklung von IT-Dienstleistungen.

Mit dem Ziel, Qualität, Sicherheit und Wirtschaftlichkeit der IT-Services mit geeigneten Prozessen steuerbar zu machen, erhielt die britische Central Computer and Telecommunications Agency (CCTA) den Auftrag, hierfür bewährte Verfahren zu dokumentieren und zu vereinheitlichen. Dies war der Grundstein für den Aufbau einer Bibliothek namens ITIL.

Die CCTA ging 2001 im britischen Office of Government Commerce (OGC) auf, einer Behörde, die britische Regierungsbehörden bei der Modernisierung ihrer Einkaufsaktivitäten und IT-Services unterstützt. Das OGC garantiert auch heute die kontinuierliche Pflege und Weiterentwicklung von ITIL.

Über die Jahre wurde ITIL ständig weiterentwickelt und verfeinert. Dabei wurde das Verfahrenswerk auch den Anforderungen der Industrie angepasst. Gerade diese Öffnung trug wesentlich dazu bei, dass sich ITIL inzwischen weltweit als Defacto-Standard etablieren konnte.

2.3 Philosophie und Einflüsse

ITIL basiert auf der Erkenntnis, dass die Anforderungen an Akzeptanz, Qualität, Sicherheit und Wirtschaftlichkeit von IT-Services nur stetig erfüllbar sind, wenn IT-Services entsprechend gelenkt und organisiert werden. Die Managementsysteme für Qualität und Sicherheit müssen hierfür verzahnt, am Kunden ausgerichtet sowie über die Dienstleistungen mit Prozessen und Infrastruktur wirksam verbunden werden. Dabei bezeichnet der Begriff Infrastruktur bei ITIL die Gesamtheit von Anwendungen, IT-Systemen, Netzwerkkomponenten, die zugehörigen Gebäude sowie die Haustechnik.

Hierfür berücksichtigt ITIL in starkem Maß Erkenntnisse aus dem Qualitäts- und Prozessmanagement. Zu den Einflüssen zählen beispielsweise:

- Prozessmanagement, hier vor allem Prozessgestaltung und -integration, ergebnis- und kennzahlenorientiertes Management von Prozessen, Prozessreifemodelle (siehe [2])
- Qualitätsmanagement, z. B. ISO 9000, EFQM-Modell (siehe [3])
- Strategisches Management, z. B. kritische Erfolgsfaktoren, Zieldefinition und Balanced Score Card, Planbarkeit, Messbarkeit und Umsetzbarkeit von Zielen
- Führung und Kultur, wie etwa Policy-Management, Motivation und Leistungsorientierung, Kompetenz- und Veränderungsmanagement
- Kundenbeziehungsmanagement mit dem Ziel der Gestaltung strategischer, taktischer und operativer Kundenschnittstellen

2.4 Organisationen, Standards und Zertifizierbarkeit

Neben dem OGC sind noch weitere Organisationen im Zusammenhang mit ITIL zu nennen. Eine besondere Rolle spielt das 1992 in Großbritannien gegründete Information Technology Service-Management Forum (siehe [4]). Dies ist die inzwischen in vielen Ländern präsente ITIL User Group.

So verfolgt seit 2001 die Anwendergruppe itSMF Deutschland e.V. den Zweck, „das Allgemeinwissen zu einer anforderungsgerechten und gesamtheitlichen Denkweise zur Implementierung von IT-Strukturen zu fördern“ (siehe [4]).

Personen können ihr erworbenes ITIL-Wissen zertifizieren lassen. Hierfür werden verschiedene Zertifizierungsstufen angeboten. Der Einstieg ist das ITIL Foundation Certificate, auf dem das ITIL Service Manager Certificate aufbaut. Für beide Zertifikate muss in Prüfungen das entsprechende Wissen nachgewiesen werden.

Daneben entwickeln zwei Organisationen ITIL-Trainingsstandards und akkreditieren Anbieter für ITIL-Zertifizierungen. Dies sind das britische Information Systems Examination Board (ISEB) (siehe [5]) und das Exameninstituut voor Informatica (EXIN) in den Niederlanden ([6]). Um auch Institutionen zertifizieren zu können, wurde ein ITIL entsprechender britischer Standard geschaffen.

2.4.1 BS 15000 – Standardisiertes Management von IT-Services

Das Service-Management als zentraler Teil des ITIL-Rahmenwerks ist zudem von der nationalen britischen Standardisierungsorganisation British Standards Institution (BSI) als BS 15000 standardisiert (siehe [7]).

BS 15000 gliedert sich in zwei Teile:

- Part 1: *Specification for Service-Management* definiert die Anforderungen an das Management von IT-Dienstleistungen
- Part 2: *Code of Practice for Service-Management* liefert Empfehlungen zur Etablierung des Service-Managements.

Zum Standard BS 15000 gehören auch zwei Ergänzungsdokumente:

- PD 0005: *IT-Service-Management - A Managers Guide* liefert einen Überblick für das Management über Ziele und Inhalt des IT-Service-Managements (siehe [8])
- PD 0015: *IT-Service-Management - Self-Assessment Workbook* liefert einen Fragenkatalog zur Selbstbewertung gemäß den Anforderungen von BS 15000 (siehe [9])

2.4.2 BS 7799 / ISO 17799 – Standardisiertes Management der Informationssicherheit

ITIL sieht das IT-Sicherheitsmanagement als integralen Bestandteil der Steuerungsprozesse in der IT an. Dies war Grundlage für den britischen Standard BS 7799. Hiervon wurde der erste Teil als ISO-Standard 17799 übernommen (siehe [10]). Der Standard beschreibt allgemein gültige Vorgaben zum Aufbau eines Informationssicherheitsmanagements und basiert auf einen Best Practice Ansatz (siehe [11]). ITIL trifft selbst keine Aussagen zur IT-Sicherheit, sondern verweist auf den britischen Standard BS 7799.

Definiert sind 10 Kategorien des Managements von Informationssicherheit, die sich in 36 generische Sicherheitsziele und 127 konkretere Sicherheitsanforderungen unterteilen.

Der Standard BS 7799 gliedert sich in zwei Teile:

- *Part 1: Code of Practice for Information Security Management* liefert einen Leitfaden zum Management der Informationssicherheit mit Darstellung entsprechender Maßnahmen
- *Part 2: Information Security Management Systems - Specification with guidance for use* liefert Anforderungen an Sicherheitsmanagement-Systeme und damit ein Raster zur Beurteilung als Grundlage für Zertifizierungen

2.5 ITIL: Stärken und Schwächen

Besondere Stärken von ITIL sind:

- umfassendes Rahmenwerk für die IT-Prozessorganisation mit hoch integriertem Prozessansatz
- als Sammlung von Best Practices ist es praxis- und umsetzungsorientiert
- es setzt auf vielfältigen, bewährten Managementsichten und -modellen auf
- es ist ein fest verankertes, integriertes Qualitäts- und Sicherheitsmanagement
- es hat eine starke Kunden- und Serviceorientierung,
- eine standardisierte Methodik und Darstellung
- und außerdem eine breite Akzeptanz bei den Marktteilnehmern und in IT-Bereichen

ITIL weist auch Schwächen auf, unter anderem:

- Die Hauptbestandteile von ITIL weisen einen unterschiedlichen Reifegrad auf.
- ITIL ist auf der Management-Ebene, aus nicht technischer Sicht (beispielsweise Planung und Organisation), unzureichend strukturiert.
- Der Schwerpunkt wird in ITIL einseitig auf den IT-Betrieb gelegt, in den Prozessen der Softwareentwicklung ist das Werk schwach.
- ITIL beschreibt keinen IT-Sicherheitsprozess, sondern verweist zur Umsetzung eines Sicherheitsprozesses lediglich auf die britische Norm BS 7799.
- Die Bereiche IT-Einkauf und IT-Beschaffungsabwicklung sind unzureichend integriert.

2.6 ITIL: Chancen und Risiken aus Sicht des Sicherheitsmanagements

Bei richtiger Umsetzung der ITIL-Empfehlungen in die Praxis ergeben sich erhebliche Chancen für ein noch wirksameres und effizienteres IT-Sicherheitsmanagement:

- durch enge Verzahnung der Managementsysteme für Sicherheit, Qualität und Services
- durch frühzeitige Berücksichtigung der Sicherheitsanforderungen in Gestaltung, Planung und Steuerung der IT-Services
- durch Professionalisierung der Schnittstellen zu Kunden und zu Lieferanten von IT-Services
- durch Messbarkeit und Objektivierung der IT-Leistung
- durch mehr Verbindlichkeit in den Anforderungen und Vereinbarungen an und über IT-Services
- durch mehr Transparenz in den Zusammenhängen zwischen Anforderungen, Services, IT-Prozessen und Infrastrukturnutzung und
- durch mehr Durchgängigkeit in Planung und Steuerung der IT-Services unter Qualitäts-, Sicherheits- und Effizienzgesichtspunkten
- Kosten für IT und IT-Sicherheit, die häufig als Gemeinkosten betrachtet werden, können durch konkrete Zuordnung zu Prozessen und Produkten in Stückkosten überführt werden.

Die Einführung von Prozessen, die einen serviceorientierten IT-Betrieb steuern sollen, hat tief greifende Auswirkungen auf die gesamte IT-Organisation. Damit sind auch typische Umsetzungsrisiken verbunden, wie sie in komplexen Veränderungsprozessen häufig hervorgerufen werden. Vermeiden lassen sich solche Risiken dadurch, dass

- der konkrete Veränderungsbedarf ermittelt und pauschale Einführungen vermieden werden. Das bedeutet, vor der Einführung von ITIL-Prozessen sollte genau geprüft werden, ob vorhandene Probleme gelöst werden können, bzw. ob durch die Einführung der Prozesse für die IT-Organisation tatsächlich spürbare Verbesserungen entstehen.
- die Umsetzung auf allen Managementebenen gleichermaßen unterstützt wird und eine vertrauensvolle und Veränderung fördernde Atmosphäre geschaffen wird,
- eine gemeinsame Servicekultur geschaffen wird, die alle Leistung erstellenden und steuernden Bereiche der IT teilen,
- die Kunden und Dienstleister der IT frühzeitig in den Veränderungsprozess eingebunden werden,
- realistisch und stufenweise geplant wird,
- nicht zu formal und zu technisch an die Einführung herangegangen wird und
- der erreichte Grad stetig gesichert und verbessert wird.

3 Die wichtigsten ITIL-Bestandteile

ITIL besteht aus 7 Schwerpunktpublikationen, die eng miteinander verzahnt sind. Neben fünf Prozessfeldern für das Management des IT-Betriebs (Service Support), der IT-Services (Service Delivery), der Anwendungen (Applications Management) und der IT-Infrastruktur (ICT Infrastructure Management) widmet sich jeweils ein weiterer Band dem Sicherheitsmanagement (Security Management) und der Einführung von IT-Service-Management (Planning to implement Service-Management).

Abbildung 1: ITIL-Überblick, Quelle: OGC

In der Summe zeigt ITIL, wie IT-Steuerungsprozesse zwischen Kundenanforderungen und Technologieeinsatz zusammenwirken. Nachfolgend werden die inhaltlichen Schwerpunkte im Überblick zusammengefasst:

3.1 The Business Perspective

Im Band "The Business Perspective" beschreibt ITIL Anforderungen an das IT-Management. Dazu zählen folgende Aspekte:

- Business Continuity Management (Notfallvorsorge und Notfallmanagement)
- Partnerschaften und Outsourcing
- Änderungsmanagement
- Gestaltung der IT-Service-Organisation
- Planung und Steuerung von IT-Services
- Qualitätsmanagement für IT-Services
- Business- und Management-Fähigkeiten
- Kundenbeziehungsmanagement

3.2 Service Delivery

Mit dem Band "Service Delivery" (Erbringung von Dienstleistungen) liefert ITIL die taktischen Prozesse des Service-Managements. Diese steuern Gestaltung, Planung, Vereinbarung, Überwachung, Berichtswesen und Optimierung der IT-Services und ihrer Eigenschaften. Hierfür werden folgende fünf Prozesse definiert:

- Service Level Management
- Finanzmanagement (Financial Management for IT-Services)
- Verfügbarkeitsmanagement (Availability Management)
- Kapazitätsmanagement (Capacity Management)
- Kontinuitätsmanagement (IT Service Continuity Management)

3.3 Service Support

Im Band "Service Support" werden von ITIL die operativen Prozesse des Service-Managements beschrieben. Diese steuern die Servicequalität direkt in den Leistungserstellungsprozessen. ITIL empfiehlt hier einerseits die Bündlung der Anwenderschnittstellen in einer Service Desk Funktion und andererseits die Unterscheidung von fünf zentralen Unterstützungsprozessen, die eng zusammenwirken:

- Service Desk Funktion
  Der Service Desk, also die Anwenderbetreuung, stellt die zentrale Kommunikationsschnittstelle zum Kunden dar.
- Störungsmanagement (Incident Management)
  Das Störungsmanagement stellt bei der Beeinträchtigung eines vereinbarten Service diesen so schnell wie möglich und mit kleinstmöglichen Auswirkungen für andere Anwender wieder her.
- Problemmanagement (Problem Management)
  Das Problemmanagement hält Fehler, die in der IT-Infrastruktur entstehen, möglichst gering und versucht das wiederholte Auftreten von Störungen zu verhindern.
- Änderungsmanagement (Change Management)

  Das Änderungsmanagement führt Änderungen

  - effizient,
  - mit standardisierten Methoden und Verfahren,
  - mit möglichst geringen Auswirkungen und
  - aufeinander abgestimmt durch.
- Versionsmanagement (Release Management)
  Das Versionsmanagement plant den Roll-out von Hard- und Software und stellt sicher, dass nur getestete und autorisierte Hard- und Softwareversionen in Betrieb genommen werden.
- Konfigurationsmanagement (Configuration Management)
  Das Konfigurationsmanagement erfasst, kontrolliert und verifiziert den Status aller IT-Komponenten und deren Beziehungen untereinander. Es stellt eine einheitliche Datenbasis für alle anderen Prozesse zur Verfügung (Beispielsweise Name der Komponente, Besitzer, Standort, Lieferant, Einführungsdatum und Status).

3.4 Infrastructure Management

Unter dem Begriff "Infrastructure Management" wurden früher bei ITIL eine Reihe von Publikationen zusammengefasst, die sich z. B. mit Netzwerkmanagement, Management dezentraler IT-Einheiten, Installationsmanagement und Applikationsmanagement befassen. (Unter "Infrastruktur" fasst ITIL die Gesamtheit von Anwendungen, IT-Systemen und die für den Betrieb der IT erforderliche baulich-technische Infrastruktur zusammen.)

Später erschien eine Schwerpunktpublikation "ICT Infrastructure Management", die Prozesse für einen standardisierten Management-Lebenszyklus im Systembetrieb zusammenfasst:

- Strategie und Richtlinien, Planung des Einsatzes von Infrastrukturkomponenten (Design and Planning).
- Einführungsvorbereitung und Inbetriebnahme (Deployment)
- Management des Betriebs von Infrastrukturkomponenten (Operations)
- Technische Unterstützung durch Forschung und Entwicklung, Herstellersupport und Wartung (Technical Support)

3.5 Applications Management

In der Publikation "Applications Management" fasst ITIL den Software-Lebenszyklus zusammen. Hier werden die Anwendungen in den Fokus gerückt und das Zusammenwirken der IT-Prozesse entlang des Lebenszyklus einer Anwendung beschrieben. Folgende Phasen werden unterschieden:

- Analysieren (Anforderungsmanagement)
- Entwickeln (Hard- und Softwareentwicklung)
- Test (Testen von Hard- und Software)
- Inbetriebnahme (der fertigen IT-Systeme)
- Applikationsbetrieb
- Optimierung (des Applikationsbetriebs)

ITIL hat hier nicht den Anspruch, konkrete Empfehlungen zur Ausgestaltung von Software-Entwicklungsprozessen zu liefern, wie das für Service-Management der Fall ist. Der Aufbau der Publikation ähnelt daher eher dem des „ICT Infrastructure Managements“. Hier werden die grundsätzlichen Anforderungen an das Lebenszyklusmanagement von Anwendungskomponenten in den Vordergrund gerückt.

3.6 Sicherheitsmanagement (Security Management)

Es liegt derzeit im Trend, IT-Prozesse auf Basis von ITIL zu restrukturieren oder neu zu entwickeln. Dies bietet die Chance, den häufig isoliert betrachteten Bereich der Informationssicherheit stärker in die IT-Prozesse einzubeziehen und damit nicht nur potenzielle Konflikte zu vermeiden, sondern auch zu einer sauberen Arbeitsverteilung zwischen IT-Bereich und IT-Sicherheit zu kommen. Für einen IT-Sicherheitsbeauftragten beinhaltet dies sogar noch einen weiteren Vorteil, da die Ankoppelung an das geschäftsprozessorientierte Thema ITIL für ihn die Chance zu einer erhöhten Aufmerksamkeit bei der Behörden- bzw. Unternehmensleitung und Akzeptanz bietet. Auch die stets aktuelle Frage nach ökonomischer Rechtfertigung der IT-Sicherheit findet in der Integration mit ITIL eine Antwort.

Im ITIL-Konstrukt wird das Thema IT-Sicherheit grundsätzlich bereits im Band "Service Continuity Management" definiert und durch die britische Norm BS 7799 (die auch die Basis für den internationalen Standard ISO 17799 bildet) detailliert spezifiziert.

BS 7799 unterscheidet sich vom deutschen IT-Grundschutzhandbuch (siehe [12]) des Bundesamtes für Sicherheit in der Informationstechnik [13] durch einen deutlich höheren Abstraktionsgrad. BS 7799 beschreibt den Aufbau und die Verankerung eines IT-Sicherheitsmanagements ohne detaillierte Umsetzungshinweise. Das IT-Grundschutzhandbuch geht darüber hinaus und gibt auch detaillierte Maßnahmen vor.

Im Folgenden sollen daher an konkreten Praxissituationen Gemeinsamkeiten zwischen IT-Service und Sicherheitsmanagement aufgezeigt werden, die über die abstrakten Anforderungen in BS 7799 hinausgehen.

3.7 Zusammenfassung

ITIL liefert also Best Practices auf allen Management-Ebenen der IT sowie auf allen Sachebenen beginnend bei der Geschäftsausrichtung, über die Servicegestaltung und Gewährleistung der Informationssicherheit bis hin zum Betrieb von Anwendungen und Infrastruktur und dem hiermit verbundenen Technologieeinsatz.

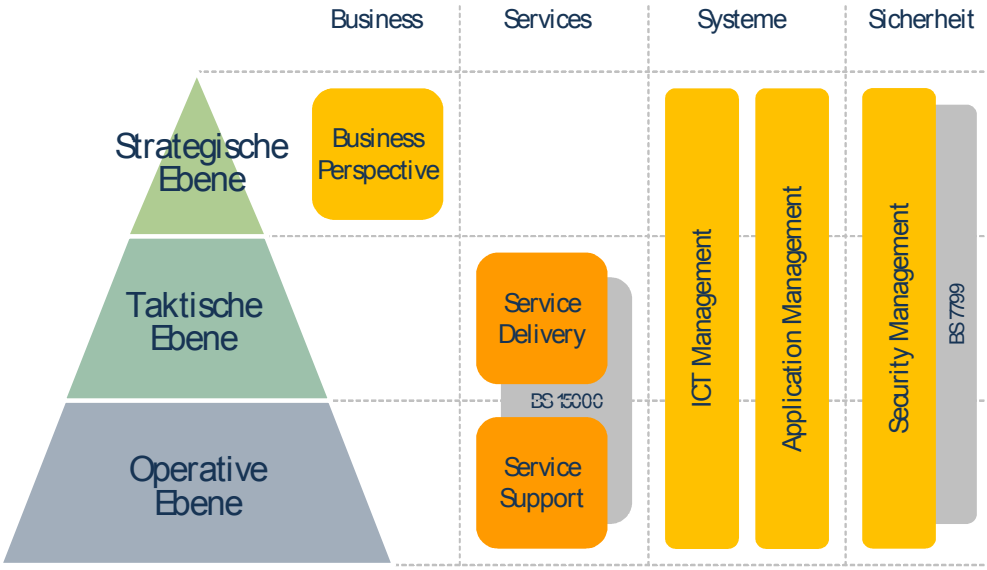

Abbildung 2: ITIL-Prozesse auf den Management-Ebenen, Quelle: HiSolutions AG

In der Abbildung verstehen wir „Systeme“ als Zusammenfassung der IT-Infrastruktur- und -Anwendungskomponenten.

ITIL stellt die Integrationsanforderungen von Servicemanagement, Architekturmanagement und Leistungserstellung im IT-Betrieb heraus - insbesondere über das „ICT Infrastructure Management“. Dagegen wird die Integration mit Architekturmanagement und Leistungserstellungsprozessen in der Softwareentwicklung nur sehr abstrakt formuliert - als Teil des Lebenszyklusmanagements für Anwendungen. Diese Lücken werden durch andere Ansätze bereits besser geschlossen, die aber mit den ITIL-Grundsätzen gut vereinbar sind.

4 Zusammenhänge zwischen IT-Service- und IT-Sicherheits-management

4.1 Service Support und Sicherheitsmanagement

ITIL empfiehlt im Rahmen des Service Support Managements fünf Prozesse für die Steuerung der Servicequalität im operativen IT-Geschäft sowie mit dem Service Desk einen zentralen Anlaufpunkt („Single Point of Contact“) für die Anwenderunterstützung:

4.1.1 Service Desk

Aufgaben und Ziele

Der Weg von der prozess- zu einer serviceorientierten IT führt zur Anforderung, den Anwendern einen schnellen und einfachen Zugang zur IT zu liefern - unabhängig von der internen Organisation der IT-Prozesse. Dieser zentrale Anlaufpunkt soll eine professionelle Anwenderunterstützung sicherstellen, indem er

- möglichst durchgängig erreichbar ist,
- die Anwenderprobleme verstehen lernt,
- eine kontinuierliche Anwenderbetreuung sicher stellt,
- die Schnittstelle zu Spezialisten (zur Lösungsfindung) her stellt,
- eine hohe Problemlösungsquote ermöglicht
- und gleichzeitig die Spezialisten in Betrieb und Entwicklung entlastet.

Die Anwender richten sich aus verschiedenen Gründen an den Service Desk - zur Unterstützung bei spezifischen Fragen, zur Meldung von Produktfehlern und Servicestörungen oder zur Erteilung von standardisierten Aufträgen (z. B. in der Beschaffungsabwicklung oder im User- und Berechtigungsmanagement). Der Service Desk stellt die Beantwortung bzw. Bearbeitung dieser Service Requests sicher und löst entsprechende Vorgänge in den jeweiligen Abwicklungsprozessen aus.

Gestaltung

Der Service Desk selbst kann in vielfältiger Weise strukturiert sein, um eine optimale Anwenderbetreuung sicher zu stellen:

- Räumlich / organisatorisch: Möglich sind zentrale wie auch dezentrale Service Desks. In verteilten Anwenderorganisationen bewähren sich in der Praxis meist Mischformen aus zentraler und dezentraler Betreuung. ITIL sieht daneben auch virtuelle Service Desks vor, in denen die Rolle des Service Desks von verschiedenen Personen in der IT-Organisation wahrgenommen wird.
- Fachlich / wissensorientiert: Daneben werden Service Desks auch nach den Fähigkeiten und der Betreuungstiefe unterschieden. ITIL differenziert
  - Call Center (ausschließliche Annahme und Weiterleitung)
  - Unskilled Service Desks (mit Dokumentation und Qualifikation der Serviceanfragen)
  - Skilled Service Desks (mit bestimmter Lösungskompetenz)
  - Expert Service Desks (mit eigenem Expertenwissen)

Mitunter führt die Einführung des Service Desks zu Akzeptanzproblemen, wenn er nicht in geeigneter Weise realisiert wird (z. B. mangelnde zeitliche oder geografische Erreichbarkeit, mangelnde Kompe-

tenz, fehlende Prozesse, Verantwortlichkeiten etc.). Die Vorteile eines Service Desks liegen aber klar auf der Hand: Die Mitarbeiter des Service Desks können sich auf den Anwender und seine Probleme konzentrieren. Sie sind erreichbar und bauen schrittweise eigene Problemlösungskompetenz auf. Flächenstörungen können sie oft früher erkennen als Spezialisten in konkreten Betriebsbereichen. Sie ermöglichen eine standardisierte Erfassung der Anfragen und liefern damit eine ganz wesentliche Grundlage für das Servicemanagement, zudem kommunizieren sie in der Regel professioneller mit den Fragenden als die IT-Spezialisten in Betrieb und Entwicklung und ermöglichen eine kontinuierliche und proaktive Information der Anwender. Gleichzeitig entlasten sie die Spezialisten und ermöglichen somit eine höhere Produktivität in der Störungsbearbeitung.

Synergien mit dem Sicherheitsmanagement

Das Sicherheitsmanagement stellt in bestimmten Fällen ähnlich hohe Anforderungen an die Qualität der Anwenderschnittstelle - z. B. hinsichtlich Erreichbarkeit und Reaktionsschnelligkeit. Gleichzeitig kann es die Stärken eines Service Desks nutzen, um z. B. standardisierte Routineprozesse effizient abwickeln zu lassen. Die Aussage, dass der Service Desk der jedem Anwender bekannte zentrale Anlaufpunkt zur IT-Serviceorganisation ist, sollte also auch das IT-Sicherheitsmanagement einschließen. Beispiele:

- „Security-Frontoffice“: Der Service Desk sollte in der Lage sein, im Zusammenhang mit Anfragen der Anwender evtl. sicherheitsrelevante Aussagen zu erkennen, mit aufzunehmen, zu klassifizieren und richtig weiter zu leiten. Der Service Desk gewährleistet damit auch für das Sicherheitsmanagement eine hohe Erreichbarkeit und Reaktionsfähigkeit, indem er folgende Aufgaben wahr nimmt:
  - **Annahme und Erfassung von Sicherheitsvorfällen** bei Anwendern bzw. Erkennung möglicher Sicherheitsvorfälle aus gemeldeten Fehlern bzw. Störungen
  - **Feststellung von Flächenstörungen** als Folge möglicher Sicherheitsvorfälle
  - **Sicherstellung der Dokumentation** und Bereitstellung von Historiendaten
  - **Sensibilisierung der Anwender an der Betreuungsschnittstelle** entsprechend der Vorgaben des Sicherheitsmanagements
  - **Alarmierung von Verantwortlichen** bei möglichen IT-Sicherheitsvorfällen

    Möglich ist dies aber nur, wenn das Sicherheitsmanagement die Anwenderbetreuung in Zusammenarbeit mit dem Service Desk organisiert und ihn entsprechend befähigt.
- Standardprozesse der IT-Sicherheit: Der Service Desk ist meistens auch für die Annahme konkreter Standardaufträge verantwortlich, oft auch für deren Bearbeitung. Häufig betrifft dies z. B. auch Prozesse wie das User & Profile Management (Nutzeranmeldung, Berechtigungsvergabe, Kennwortrücksetzung, Nutzersperrung etc.). Ein Beispiel hierfür ist z. B. die Einrichtung der Registrierungsstelle (Registration Authority, RA), einer PKI im Service Desk. Damit hat der Service Desk auch eine ausführende Funktion für das Sicherheitsmanagement, indem er entsprechende Policies zur Gewährleistung der Informationssicherheit umsetzt. Dies macht eine Arbeitsteilung und Zusammenarbeit entsprechend der Anforderungen des Sicherheitsmanagements sinnvoll und notwendig.

4.1.2 Störungsmanagement (Incident Management)

Ziele und Aufgaben

Der Störungsmanagementprozess hat die Aufgabe, tatsächliche oder absehbare Servicebeeinträchtigungen aufzunehmen und zügig zu beheben. Dies übt einen wesentlichen Einfluss auf die Zufriedenheit der Anwender aus, zumal ein Großteil der Störungen in der Regel von ihnen selbst festgestellt und gemeldet wird. Mit der Qualität des Störungsmanagements steigt die Effizienz in der Störungsbearbei-

tung. Zu den Zielen gehört auch, Aktionismus zu vermeiden, einen hohen Anteil der Störungen bereits im 1st-Level-Support zu beheben, weitere Support-Stufen (Spezialisten und Hersteller) effektiv zu nutzen und natürlich die Störungen in der sinnvollen Reihenfolge oder ggf. im Zusammenhang zu beheben. Mit der durchgängigen Dokumentation der Störungen stehen anderen Servicemanagement-Prozessen zudem wichtige Informationen für die Steuerung der Servicequalität zur Verfügung.

Gestaltung

Störungsbearbeitung gab es in der IT von Anfang an. Auch die Unterscheidung von Support-Stufen (1st-, 2nd-, 3rd-, ...Level-Support) ist gängige Praxis. ITIL liefert für die Störungsbearbeitung einen Prozessansatz, der eine durchgängige Bearbeitung von Störungen sicher stellt. Dabei können je nach Qualität einer Störung ein oder mehrere Support-Stufen beteiligt sein.

Der Prozess umfasst:

- Störungsannahme und -erfassung
- Klassifikation, Priorisierung nach Dringlichkeit und Auswirkungen, erste Unterstützung
- Prüfung auf bekannte Störungsmuster
- Analyse und Diagnose
- Behebung und Service-Wiederherstellung
- Abschluss des Störungsvorgangs

Störungen können von jeder Person festgestellt und gemeldet werden. Für die Annahme der Störungsmeldungen von Anwendern ist der Service Desk verantwortlich. Er übernimmt in der Regel die weitere Verfolgung der Störungen bis zur Behebung und die anschließende Anwenderinformation. Daneben werden die entsprechenden Werkzeuge (Störungsmeldungs- oder Ticketing-Systeme) auch direkt von den IT-Spezialisten in Entwicklung und Betrieb genutzt, so dass Störungen meist auch dezentral erfasst werden. Dies ist schon deshalb notwendig, weil die Spezialisten als 2nd-Level-Support im Störungsmanagement-Prozess tätig werden, wenn Störungen nicht durch den Service Desk selbst behoben werden können. Zusätzlich bieten Werkzeuge zur Überwachung des System- und Applikationsbetriebs die Möglichkeit, Störungen im Servicemanagement über entsprechende Schnittstellen automatisch zu melden. Dies wird genutzt, um häufige Störungsursachen (z. B. Überlastung, Kapazitätsengpässe etc.) frühzeitig zu erkennen und zu behandeln.

ITIL empfiehlt, Störungen im Zusammenhang mit den betroffenen IT-Komponenten zu erfassen. Zudem sollen Flächenstörungen auch als solche erkannt und dokumentiert werden.

Im Prozess sind auch die Eskalationsverfahren zu regeln, z. B.

- die Einbeziehung weiterer Support-Stufen (funktionale Eskalation)
- oder die Alarmierung von Managementebenen (vertikale Eskalation).

Synergien mit dem Sicherheitsmanagement

Sicherheitsvorfälle sind Störungen in IT-Services und müssen entsprechend behandelt werden. Umgekehrt können Störungen in IT-Services auch Folge unerkannter Sicherheitsvorfälle sein. Wenn das Sicherheitsmanagement also Verfahren zur Behandlung von Sicherheitsvorfällen etabliert, wird dabei nur eine bestimmte Form des Störungsmanagements behandelt. Eine serviceorientierte IT-Organisation wird sich derartige isolierte Prozesse nicht lange leisten können und verzahnt die Anforderungen des Sicherheits- und Service-Managements in einem gemeinsamen Störungsmanagementprozess. Drei Beispiele sollen die Notwendigkeit verdeutlichen:

- **Intrusion Detection und andere Monitoringssysteme**: Einer der aktuell häufigsten Fehler in der IT-Sicherheit ist die Etablierung von Intrusion Detection Systemen (IDS), Integritätscheckern oder auch z. B. von Windows-eigenen Überwachungsmechanismen ohne prozessuale und organisatorische Einbindung. Die Konsequenz ist, dass die hohen Investitionskosten für ein IDS

häufig verpuffen, weil Probleme für den IT-Betrieb entweder nicht erkannt werden oder nicht adäquat auf sie reagiert wird. Mit der Einbindung des Monitorings in das Störungsmanagement bietet ITIL eine sinnvolle Verzahnung der Themen: Erkannte Störungen werden nach Prozessvorgaben zentral gemeldet und erfasst. Damit kann die Bearbeitung durch den Prozess sicher gestellt und überwacht werden. In gleicher Weise sollten Überwachungssysteme in den Störungsmanagement-Prozess eingebunden und die erkannten Sicherheitsvorfälle durch den Service Desk und die Spezialisten im Prozess bearbeitet werden.

- **Sicherheitsvorfallbehandlung** (Security Incident Response): Sicherheitsvorfallbehandlung muss heute in der IT-Service-Organisation als eines von mehreren Prozess-Szenarien des Störungsmanagements verstanden werden. Es stellt die Behebung erkannter Sicherheitsstörungen auf Grundlage der mitunter servicespezifischen Sicherheitsanforderungen betroffener IT-Services sicher. Hier geht es also nicht nur darum, durchgängige Prozess-Standards zu schaffen und Mehrfachaufwand in der Etablierung zu vermeiden. Noch wichtiger ist es, dass die Verfahren zur Behebung von Sicherheitsstörungen nicht nur technologiezentriert zu sehen sind sondern im Servicezusammenhang wirksam werden müssen. Die Anforderungen hierfür sind mitunter sehr service- oder gar kundenspezifisch. Hier haben Service und Sicherheitsmanagement dieselbe Sichtweise.
- **Forensische Analyse**: Die Bearbeitung von Sicherheitsvorfällen ist für die IT-Service-Organisation mit Zielkonflikten verbunden: Während das Servicemanagement in der Regel an der schnellen Wiederherstellung der betroffenen Services interessiert ist, konzentrieren sich die Forensiker auf die detaillierte Analyse der genutzten Sicherheitslücken, die Spurensicherung und erste Täterverfolgung. Auch hier wird deutlich, wie wichtig ein integriertes Störungsmanagement ist. Die Wiederanlaufverfahren für IT-Services sollten im Fall von Sicherheitsvorfällen mit den Anforderungen der Spurensicherung so weit wie möglich in Übereinklang gebracht werden und im IT-Betrieb entsprechend wirksam werden. Somit ist auch geregelt, wie die Anforderungen des Sicherheitsmanagements im Betrieb einzuhalten sind.

Bindet man die IT-Sicherheit in die Gestaltung der Servicemanagement-Prozesse ein, so besteht hier die Möglichkeit, die Sicherheitsvorfallbehandlung in Störungsmanagement- und Problemmanagement-Prozesse zu integrieren. Umgekehrt kann gerade auch die Erfahrung der Sicherheitsexperten beim zeitkritischen Reagieren auf Vorfälle, die den IT-Betrieb stören, eine Qualitätssteigerung für das „klassische“ Störungsmanagement bedeuten.

Dies ist aber nicht die einzige Möglichkeit für IT-Sicherheit, sich in die praktische Durchführung des Störungsmanagements einzubringen. Bestimmte Aufgaben des Meldeverfahrens oder die Ergänzung von SLAs um entsprechende Sicherheitsanforderungen und Mitwirkungspflichten sind Aufgaben, die der Sicherheitsbeauftragte als interner Partner und Dienstleister des IT-Servicemanagements leisten kann.

4.1.3 Problemmanagement (Problem Management)

Ziele und Aufgaben

ITIL unterscheidet das Management von Störungen und Problemen. Störungsmanagement verfolgt das Ziel, den Service möglichst schnell wiederherzustellen - egal wie. Nicht für jede Störung ist die eigentliche Ursache offensichtlich. Mitunter kann die Störung über eine Ausweichlösung beseitigt werden, so führt dann die unerkannte Ursache immer wieder zu ähnlichen Störungen. Dies zu verhindern ist Aufgabe des Problemmanagements. Wenn man berücksichtigt, dass ein Großteil des Tagesgeschäfts im IT-Betrieb und Support mit der Behebung von Störungen verbunden ist, dann wird deutlich, welchen Beitrag das Problemmanagement für die Zuverlässigkeit und Wirtschaftlichkeit von IT-Services leisten kann, wenn es entsprechend wirksam wird. Probleme sind also unbekannte Ursachen für mögliche Störungen. Bekannte Ursachen werden Fehler (Known Error) genannt.

Gestaltung

ITIL empfiehlt einen Problemmanagement-Prozess, der aus zwei Stufen besteht:

- Problembehandlung (Problem Control): Im ersten Schritt wird zunächst die Ursache aufgedeckt - also dem Problem ein bekannter Fehler zugeordnet oder dieser ermittelt.
- Fehlerbehandlung (Error Control): Im zweiten Schritt wird dann für den Fehler eine sinnvolle Lösung gesucht, deren Umsetzung überwacht und die Wirksamkeit der Lösung geprüft wird, um den Problem-Vorgang abschließen zu können.

Häufig wird Problemmanagement tätig, wenn Störungen nicht behoben werden können und für die Aufdeckung und Behebung der Ursache ein Spezialistenteam (Problem Task Force) zusammengestellt werden muss. Das Problemmanagement reicht aber noch weiter. Reifere Problemmanagement-Prozesse organisieren neben diesem reaktiven auch ein proaktives Problemmanagement, um unerkannte Probleme - u. a. für wiederkehrende Störungen - zu erkennen oder präventive Maßnahmen zur Problemvermeidung zu entwickeln. Dies erfolgt auf Grundlage von Trendanalysen. Je aussagekräftiger die Störungs- und Monitoring-Daten sind, umso leistungsfähiger kann hier das proaktive Problemmanagement sein.

Synergien mit dem IT-Sicherheitsmanagement

Einige der originären Aufgaben des IT-Sicherheitsmanagements, wie etwa die Auditierung von Systemen zwecks Aufdeckung von Sicherheitslücken, die Analyse aufgetauchter Probleme und die Entwicklung von Lösungsvorschlägen korrelieren eng mit den Aufgaben des klassischen Problemmanagements.

Grundsätzlich lässt sich vereinfacht sagen: Sicherheitslücken sind Problems! Sie können Ursache oder Wirkung von Service-Beeinträchtigungen sein. Fehler haben oft Auswirkungen auf die Sicherheit; Sicherheitslücken wiederum führen zu Problemen. Lösungen für Probleme sind auf sicherheitstechnische Konsequenzen hin zu untersuchen.

Es ist nicht nur so, dass ein Service-Management nach ITIL dem Sicherheitsmanagement hilft, seine Verfahren zur Problemanalyse, -behebung und -vermeidung prozessorientiert zu gestalten und in den Problemmanagement- Prozess einzubringen. Das proaktive Problemmanagement kann auch von Best Practices im Sicherheitsmanagement lernen, beispielsweise wie über systematische Audits die Verletzung von Sicherheitsrichtlinien
(z. B. Architekturrichtlinien, Installations- und Konfigurationsrichtlinen) und somit mögliche Ursachen für Störungen frühzeitig aufgedeckt werden können.

Nach ITIL Definition sind Problems die noch unbekannte Ursache für Betriebsstörungen. Das Problemmanagement analysiert die Ursachen der Störungen (Störungen mit bekannter Ursache sind Fehler) und schlägt Lösungen zur Behebung des Fehlers vor.

Erfahrungsgemäß ist dieses Vorgehen eine der großen Stärken des Sicherheitsmanagements, so dass sich durch die Integration des Sicherheitsmanagements mit der ITIL Disziplin Problemmanagement eine deutliche Kompetenzsteigerung erwarten lässt. Als Spezialist wirkt das Sicherheitsmanagement also an der Problemanalyse und Lösungssuche mit und übernimmt das proaktive Management von Sicherheitsproblemen. Hier muss berücksichtigt werden, dass in der Problemanalyse häufig noch nicht bekannt ist, ob die Störungsursache mit Sicherheitsproblemen verbunden ist. Deshalb muss geklärt sein, wann die IT-Sicherheit in Problemmanagement Task Forces einzubinden ist. Ebenso muss geklärt sein, wie das proaktive Management von Sicherheitsproblemen in den Prozess eingebunden ist und entsprechend Wirkung entfalten kann.

4.1.4 Änderungsmanagement (Change Management)

Ziele und Aufgaben

Änderungen - also verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren - sollen steuer- und kontrollierbar sein. Dies ist Aufgabe des Änderungsmanagement-Prozesses. Dabei sollen Störungen infolge von Änderungen vermieden und die Effizienz der Änderungen verbessert werden. Letzteres ist möglich, wenn z. B. Änderungen vermieden werden, die keinen angemessenen Nutzen bringen, nicht gewünscht sind oder mangels Durchführbarkeit wieder zurück genommen werden müssen. Die Wirtschaftlichkeit wird auch verbessert, wenn Änderungen sinnvoll gebündelt werden können. Die Sicherheit der Durchführung von Änderungen kann beeinflusst werden, in dem angemessene Rückfallverfahren für den Fall vorgesehen werden, dass der ursprüngliche Zustand schnell wieder hergestellt werden muss. Der Änderungsprozess setzt auch die Dokumentationsstandards für Änderungen und einen ordentlichen Abschluss der Änderungsarbeiten durch. ITIL empfiehlt auch hier, Änderungen im Zusammenhang mit den geänderten Konfigurationskomponenten zu dokumentieren. Somit können ggf. Störungen infolge von Änderungen schnell aufgeklärt und behoben werden. Gleichzeitig nutzt das Problemmanagement diese Informationen in der Diagnose von Störungsursachen.

Gestaltung

Die wichtigste Aufgabe in der Etablierung des Änderungsmanagements besteht darin, ein Optimum zwischen Flexibilität und Stabilität der Verfahren herzustellen. Hierbei ist sicher zu stellen, dass alle Änderungen unter Kontrolle des Managementprozesses gestellt werden. Durch Differenzierung der Änderungen und Standardisierung regelmäßig durchzuführender Änderungen kann der Managementaufwand angemessen gestaltet werden. Die Best Practices empfehlen hierfür, standardisierte Änderungsverfahren zu entbürokratisieren und für dringliche Änderungen schnelle Genehmigungsverfahren zu ermöglichen. Entscheidend ist aber, dass alle Änderungen wirksam gesteuert und dokumentiert werden. Für Änderungsfreigaben sieht ITIL ein so genanntes Änderungsfreigabe-Gremium (Change Advisory Board, CAB) vor. Wichtig für die Akzeptanz des Änderungsmanagements sind transparente Freigabe-Regeln, die technische, betriebswirtschaftliche und geschäftliche Interessen berücksichtigen sollten. Zudem empfiehlt ITIL die Pflege eines Änderungskalenders, um Änderungskonflikte oder Möglichkeiten zur Bündelung von Änderungen erkennen zu können.

Das Änderungsmanagement gliedert sich grundsätzlich in die Stufen:

- Annahme: Erfassung von Änderungsanträgen (RfC, Requests for Change), Akzeptieren und Filtern anstehender Änderungen
- Planung: Klassifikation und Priorisierung nach Dringlichkeit und Auswirkungen, Planung von Durchführung, Rückfallverfahren, benötigter Ressourcen etc. Unter Rückfallverfahren wird dabei die Möglichkeit verstanden, beim Scheitern der Umsetzung einer Änderung zur letzten funktionierenden Konfiguration zurückzukehren.
- Steuerung: Entwickeln, Testen und Umsetzen der Änderung, Evaluieren des Änderungsergebnisses und Abschluss der Änderung bzw. Durchführung eines Rückfallverfahrens bei Scheitern der Änderung

Jeder Änderungsvorgang muss durch einen Verantwortlichen für Änderungen überwacht werden. Grundlage für die Planung von Änderungen sind neben dem Änderungskalender vor allem auch die Konfigurationsdaten der betroffenen Komponenten und Informationen über deren Abhängigkeiten innerhalb der Infrastruktur sowie der Servicezusammenhänge. Letzteres ist Grundlage dafür, dass die Auswirkung der Änderungen im Rahmen der Planung richtig abgeschätzt werden können (Impact-Analyse).

Synergien mit dem Sicherheitsmanagement

Das Sicherheitsmanagement ist bei ITIL in verschiedener Hinsicht eingebunden in den Änderungsmanagementprozess:

- **als Initiator von Änderungen**: Sicherheitsprobleme, die das Sicherheitsmanagement im Rahmen des Problemmanagements feststellt, führen in der Regel zu notwendigen technischen und organisatorischen Änderungen. Diese werden durch das Sicherheitsmanagement beantragt.
- **als Realisierer von Änderungen**: Das Sicherheitsmanagement hat häufig auch konkrete Betriebsverantwortung für Teile der Sicherheitsinfrastruktur. Hier greift das Änderungsmanagement in gleicher Weise wie in anderen Bereichen des IT-Betriebs.
- **als Planungs- oder Freigabeinstanz für Änderungen**: Änderungen mit möglichen Auswirkungen auf die Sicherheitsmerkmale von IT-Services sollten unter Mitwirkung des Sicherheitsmanagements geplant und freigegeben werden. Hierfür ist abzustimmen, welche Änderungen sicherheitsrelevant sind und wie das Sicherheitsmanagement eingebunden wird. Das Sicherheitsmanagement stellt hierfür geeignete Test- und Abnahmeverfahren bereit. Hierzu gehört nicht nur die Unterstützung explizit sicherheitsrelevanter Änderungen, sondern die sicherheitstechnische Überprüfung aller Änderungen, um die Entstehung von Sicherheitslücken durch Änderungen zu verhindern.

Zwingender Grundstein für diese Schritte sollte die Integration des Sicherheitsmanagements in das Änderungsfreigabe-Gremium sein.

Ein besonderes Änderungsmanagementszenario stellt das Patchmanagement dar. Sicherheitsrelevante Patches haben nicht nur eine hohe Brisanz und müssen in der Regel unter Termindruck ausgerollt werden, sie greifen teilweise tief in bestehende Funktionalitäten und Prozesse ein. Hier gilt es, über gemeinsame Vorgaben Wege zu definieren, die den Zielkonflikt zwischen Reaktionsschnelligkeit und Qualitätssicherung ausgewogen beantworten.

4.1.5 Versionsmanagement (Release Management)

Das ITIL-Versionsmanagement umfasst alle Verfahren von der Anforderungsbearbeitung über die Planung der Umsetzung, Test und Abnahme von Soft- und Hardwareversionen bis hin zur organisatorischen und technischen Vorbereitung der Einführung einer Komponente. Das Änderungsmanagement führt die Inbetriebnahme von Komponenten durch.

Ziele und Aufgaben

Eine Version fasst eine Reihe neuer oder geänderter Konfigurationselemente zusammen, die zusammenhängend getestet und in Betrieb genommen werden. Durch diese Bündelung kann der Planungs-, Test- und Einführungsaufwand für Änderungen deutlich reduziert werden. Dies gilt für Softwareversionen wie auch für Systeme. Versionsmanagement greift also auch bei Modellwechseln - z. B. für standardisierte Arbeitsplätze.

Das Versionsmanagement plant Versionen, prüft die Versionsqualität und autorisiert Versionen für den Einsatz. Für Softwareversionen stellt es die Annahme und Archivierung der Master-Kopien sicher. Es prüft auch die Dokumentation der Softwareversionen auf Grundlage der in der Versions-Policy festgelegten Dokumentationsanforderungen. Softwareversionswechsel sind in der Regel mit einem höheren Planungs- und Testaufwand verbunden. Sie können auch organisatorische Veränderungen und Schulungsaufwand erfordern. Das Versionsmanagement sorgt im Rahmen der Roll-out-Planung dafür, dass die für die Inbetriebnahme erforderlichen Änderungen bekannt sind und in der richtigen Weise beim Änderungsmanagement beantragt werden.

Gestaltung

Das Versionsmanagement kann in drei Stufen unterteilt werden:

- Entwicklungsumgebung: In der ersten Stufe werden die Grundsätze der Versionen definiert (Versions-Policy) und die Versionsanforderungen geplant. Die Umsetzung der Versionsanforderungen wird für Individuallösungen beauftragt bzw. durch Bestellung von Standardlösungen realisiert. Die Stufe endet mit der Erstellung der Softwareversionen. Bei Eigenentwicklungen überlappt hier das Softwareversionsmanagement mit den Prozessstandards in der Softwareentwicklung. So wird aber auch deutlich, wie sich die Entwicklungsprozesse in den gesamten Applikationslebenszyklus einbetten.
- Testumgebung: Die zweite Stufe beginnt mit der Annahme der Lieferung der Softwareversionen und deren formeller Prüfung (Version, Dokumentation der Version). Verschiedenartige Tests dienen anschließend der Qualitätsprüfung. Diese Tests grenzen sich von den Entwicklungstests insofern ab, als dass sie auf Anwenderakzeptanz, Erfüllung der Softwareversionsanforderungen und Betreibbarkeit in der Produktivumgebung konzentriert sind. Neben den Tests sind auch die Einführungsmaßnahmen (organisatorische wie technische) zu planen. Die Tests und Planungen führen zur Autorisierung der Softwareversionen (Versions- bzw. Produktionsfreigabe).
- Produktionsumgebung: Die dritte Stufe verfolgt den eigentlichen Roll-out. Hierfür beantragt das Versionsmanagement entsprechende Änderungen, die unter Kontrolle des Änderungsmanagements ausgeführt und an das Versionsmanagement zurückgemeldet werden. Da die Rückfallverfahren hier häufig komplexer sind als bei standardisierten Änderungen, werden diese meistens im Rahmen der Roll-out-Planung durch das Versionsmanagement definiert.

Versionsmanagement ist also ein sehr umfassender Service-Management-Prozess, der Schnittstellen zu verschiedenen IT-Prozessen unterhält: insbesondere zu IT-Beschaffung und Vertragsmanagement, Anforderungsmanagement und Softwareentwicklung sowie Applikations- und Systembetrieb.

Synergien mit dem Sicherheitsmanagement

Es liegt auf der Hand, dass die Einführung neuer Komponentenversionen auch mit Sicherheitsanforderungen verbunden ist und dass Versionsmanagement auch für die Einführung von Sicherheitslösungen notwendig ist. Daraus ergeben sich drei wesentliche Integrationsanforderungen:

- **Anforderungsmanagement**: Das Sicherheitsmanagement muss über geeignete Vorgaben frühzeitig im Versionsmanagementprozess wirksam werden, um sicher zu stellen, dass die notwendigen Sicherheitsanforderungen bereits in der Versionsplanung Berücksichtigung finden. Wenn die Abnahmekriterien für die Versionen nicht frühzeitig bekannt sind, bleibt dem Sicherheitsmanagement dann häufig nur die Rolle des Verhinderers im Vorfeld der Inbetriebnahme. Viele Sicherheitsanforderungen können über geeignete Richtlinien (Gestaltungsgrundsätze, Policies) standardisiert werden. Andere sind lösungsspezifisch und erfordern die direkte Einbindung des Sicherheitsmanagements in die Versionsplanung. Das Sicherheitsmanagement sollte aber auch entwicklungsbegleitend wirksam werden, indem es Prüfpunkte für Risiko- und Sicherheitsbewertung festlegt.
- **Versionstest und -freigabe**: Die Autorisierung der Versionen für den produktiven Einsatz muss auch auf Grundlage der formulierten Sicherheitskriterien erfolgen. Jede Version muss auch Anforderungen an Stabilität, Integrität und Vertraulichkeit erfüllen. Hierfür stellt das Sicherheitsmanagement Testverfahren bereit und erteilt die notwendigen Freigaben aus dem Blickwinkel der Sicherheit.
- **Softwareversionsmanagement für Sicherheitslösungen und -patches**: Eingesetzte Sicherheitslösungen werden ebenso im Rahmen des Versionsmanagement-Prozesses geplant und eingeführt. Der Einsatz von sicherheitsrelevanten Patches wird mit ähnlichen Verfahren vorbereitet, so dass die Vorbereitungsphase im Patchmanagement als Szenario des Versionsmanagements verstanden werden kann.

4.1.6 Konfigurationsmanagement (Configuration Management)

Ziele und Aufgaben

Das Konfigurationsmanagement stellt die integrierte Informationsgrundlage für alle Service-Management-Prozesse sicher. Dies betrifft

- Informationen über Eigenschaften der eingesetzten Konfigurationselemente, wie Applikationen, IT-Systeme, Infrastruktur und deren Zusammenhänge und
- Informationen über aufgezeichnete Störungen, Probleme und Änderungen im Zusammenhang mit den Konfigurationselementen.

Konfigurationselemente können ganze Infrastrukturbereiche, konkrete Anwendungen und Anwendungskomponenten, Systeme und Systemkomponenten wie auch Dokumentationen sein. In Erweiterung zum klassischen Asset Management stellt das Konfigurationsmanagement auch die wesentlichen Zusammenhänge zwischen Services, Infrastruktur und Servicemanagement-Vorgängen dar. Dies ist eine wesentliche Voraussetzung, z. B. um die Folgen von Änderungen oder Störungen an konkreten Komponenten für die betroffenen Services einschätzen zu können oder um eine verursachungsgerechte Verrechnung von IT-Services zu ermöglichen.

Das Konfigurationsmanagement stellt auch sicher, dass Verfahren für die Beurteilung der Datenqualität und für die Identifizierung von Abweichungen zwischen Soll- und Ist-Konfigurationen entwickelt werden.

Gestaltung

Folgende Verfahren sollten im Rahmen des Konfigurationsmanagement-Prozesses sicher gestellt werden:

- Konfigurationsplanung: Festlegung der Konfigurationsmanagement Policy (Umfang, Namens- und Versionierungsgrundsätze etc.), Design der Konfigurationsmanagement-Datenbank (CMDB) für die Verwaltung der Konfigurationsdaten.
- Identifizierung: Identifizierung neuer oder geänderter Komponenten mit Bezeichner, Versionsstand, Status, Klassifikation bzw. Kategorisierung etc., Festlegung logischer Beziehungen, Definition so genannter Referenzkonfigurationen (Baselines)
- Statusüberwachung: Verfolgung des Betriebsmittelstatus, Verhinderung unzulässiger Vorgänge an Betriebsmitteln
- Konfigurationskontrolle: Kontrolle der Vollständigkeit und Aktualität der Betriebsmittelinformationen
- Verifizierung: Ermittlung von Soll-Ist-Abweichungen zwischen geplanten/dokumentierten und tatsächlichen Konfigurationseigenschaften

Synergien mit dem Sicherheitsmanagement

Bei konsequenter Umsetzung entwickelt sich die CMDB sehr schnell zu einer zentralen Datenbank zur Verwaltung von IT-Komponenten (IT-Repository), in der neben Services, Rollen und der eigentlichen Hardware, Software und anderen Elementen der IT-Infrastruktur (Configuration Items) auch Prozesse abgebildet werden. Ergänzt man dieses Beziehungsnetz nun auch noch um Anforderungen gemäß Verfügbarkeit, Vertraulichkeit und Integrität, entwickelt sich dies sehr schnell in Richtung eines universellen Werkzeuges auch für das Sicherheitsmanagement. Hierauf lässt sich z. B. eine Umsetzung des IT-Grundschutzes abbilden.

Ebenso ist dies auch der entscheidende Schritt zu einer toolgestützten Notfallplanung. Klingt dies nun nach einem einseitigen Vorteil für den Sicherheitsbeauftragten, so liefert dies auch praktischen Nutzen für das Service-Management. Hieraus ergeben sich zum Beispiel auch Service-Anforderungen und

Regelungsbedarf in Service Level Agreements, da sich aus der Kritikalitätsbewertung der Anwenderprozesse auch Service- und Infrastrukturanforderungen ableiten lassen.

Folgende Integrationsanforderungen lassen sich zusammen fassen:

- Transparenz: Zunächst liefert die CMDB die benötigte Service- und Infrastrukturtransparenz. Das Sicherheitsmanagement ist also ein wichtiger Nutzer der CMDB und dessen Anforderungen sollten in der CMDB-Planung Berücksichtigung finden.
- Sicherheitssicht in der CMDB: Das Sicherheitsmanagement liefert zudem zusätzliche Informationen wie Kritikalitäts- und Risikobewertungen, die von den Anwenderprozessen auf konkrete Services und Betriebsmittel übertragen werden können. Eine leistungsfähige CMDB unterstützt hiermit Planungs- und Steuerungsprozesse sowohl im Service- als auch im Sicherheitsmanagement.
- Maßnahmenplanung: Zudem lassen sich neben den Service-Management-Vorgängen an Betriebsmitteln auch Sicherheitsmaßnahmen dokumentieren und verfolgen, die in Folge von Audits oder Zertifizierungen geplant werden.

4.2 Service Delivery und Sicherheitsmanagement

Während Service Support Management die operative Unterstützung der Services in der Anwenderbetreuung und in den Leistungsprozessen der IT gewährleistet, stellt Service Delivery Management die taktischen Prozesse des Servicemanagements sicher.

Hier rückt der interne oder externe Kunde als Auftraggeber der Services mit seinen Anforderungen und die vereinbarungsgerechte Lieferung dieser Services in den Mittelpunkt. Als interne Kunden werden Mitarbeiter oder Verantwortliche bezeichnet, die einen Service in Auftrag geben.

4.2.1 Service Level Management

Ziele und Aufgaben

Das Service Level Management (SLM) ist für die Umsetzung der Kundenanforderungen in konkrete Serviceangebote, deren Vereinbarung und Überwachung verantwortlich. Mit der Spezifikation von Services werden die Leistungen der IT-Organisation in Angeboten gebündelt, die für den Kunden eine Problemlösung liefern und deshalb konkreten Bedarf haben. An dieser Problemlösung macht er Anforderungen fest, die sich auch auf Qualität, Sicherheit und Wirtschaftlichkeit der hierfür nötigen Infrastruktur und IT-Prozesse übertragen lassen. Dies ist deshalb sinnvoll, weil der Kunde sich weniger mit Infrastruktur- und Prozess-Details der IT auseinandersetzen muss und die IT-Organisation ihre Services lösungsorientiert und anforderungsgerecht definiert.

Gestaltung

Der SLM-Prozess organisiert den Service-Lebenszyklus. Hierfür stellt er folgende Verfahren bereit:

- Service Level Anforderungsmanagement (Requirements Management): Nimmt Kundenanforderungen an bestehende oder neue Services auf und bewertet diese.
- Service Design: Definiert den Service und spezifiziert den Leistungs- und Infrastrukturinhalt; Ergebnis ist eine Servicespezifikation.
- Service Planung und Implementierung (Planning & Implementation): Plant und testet den Service mit Unterstützung der anderen Service Delivery Prozesse, der Service wird in den Servicekatalog aufgenommen, die Qualitätsanforderungen werden in einem Servicequalitätsplan (Quality Plan, SQP) festgeschrieben.
- Management von Servicevereinbarungen (Service Contracting): stellt das Management von Servicevereinbarungen sicher; dies betrifft Serviceverträge und Service Level Agreements mit den

Kunden, die Absicherungsverträge mit Lieferanten und externen Service Providern sowie Vereinbarungen mit internen Leistungserstellern (OLA, Operational Level Agreements).

- Service Level Monitoring: überwacht die Einhaltung der vereinbarten Service Levels, misst deren Erreichung und analysiert die Abweichungen.
- Service Berichtswesen: Erstellt die Serviceberichte für IT-Management und Kunden.
- Service Optimierung: Analysiert Potenziale und entwickelt Verbesserungsmaßnahmen für die Services und den SLM-Prozess (SIP, Service Improvement Program).

Das Service Level Management ist der zentrale Integrationsprozess im Service Delivery Management. Er integriert aber nicht nur die anderen Delivery-Management-Prozesse, sondern auch das Kundenbeziehungs- und Lieferanten-/Providermanagement. Mit dem Management des Servicekatalogs spielt er ebenso eine wichtige Rolle in der Umsetzung der IT-Service-Strategie und in der Ausrichtung der IT-Leistungsorganisation auf die Serviceanforderungen der Kunden.

Synergien mit dem Sicherheitsmanagement

Sicherheit ist eine der zentralen Anforderungen an IT-Services. In der Analyse, Planung und Überwachung der Sicherheitsmerkmale von IT-Services ist das Sicherheitsmanagement vergleichbar mit anderen Delivery Prozessen - z. B. zur Sicherstellung der Wirtschaftlichkeits-, Performance- und Verfügbarkeitsmerkmale. Deshalb eignen sich auch dieselben Integrationspunkte für die Zusammenarbeit von SLM und Sicherheitsmanagement:

- **Anforderungsmanagement und Service Design**: Überwiegend macht die Festlegung angemessener Sicherheitsanforderungen an IT-Services die Beratung des Kunden durch das Sicherheitsmanagement erforderlich. Daneben sind in der Regel Basisanforderungen an die IT-Sicherheit geregelt, die unabhängig von konkreten Kundeninteressen in den IT-Services zu berücksichtigen sind, z. B. weil hierfür gesetzliche Rahmenbedingungen einzuhalten sind, Zertifizierungsanforderungen aufrecht erhalten werden müssen oder eine organisationsweite Sicherheitsstrategie Eckpfeiler setzt. Das Sicherheitsmanagement unterstützt mit entsprechenden Empfehlungen bzw. Vorgaben das Anforderungsmanagement für IT-Services und beeinflusst hierüber die Servicespezifikation.
- **Serviceplanung und -implementierung**: Um die definierten Sicherheitsmerkmale der IT-Services in der Praxis der Serviceerstellung durchzusetzen, müssen hieraus konkrete Sicherheitsanforderungen an die Gestaltung von IT-Prozessen und Infrastruktur abgeleitet und umgesetzt werden. Dies ist der Hebel für das Sicherheitsmanagement, die festgelegten Anforderungen im Rahmen der Serviceplanung und -implementierung wirksam zu machen. Dies schließt natürlich auch entsprechende Sicherheitsüberprüfungen im Rahmen der Serviceeinführung ein.
- **Vereinbarungen und Richtlinien**: Neben den grundsätzlichen Sicherheitszusagen für konkrete Services sind auch die Mitwirkungspflichten der Servicenehmer und Leistungsersteller zu regeln. Dies erfolgt in der Praxis auf verschiedenen Wegen und Stufen. Bestimmte Vereinbarungen werden über die Rahmenverträge und SLA mit Kunden und Lieferanten getroffen, andere werden innerhalb einer Behörde oder eines Unternehmens über Richtlinien und Anweisungen (Policies) geregelt (z. B. Policies zur sicheren Service-Nutzung, Policies für den sicheren Betrieb von Anwendungen und Systemen, etc.) oder über die Leistungsvereinbarungen (OLA). Hier wird deutlich, dass es eine besondere Herausforderung ist, eine konsistente Methodik für sicherheitsrelevante Vereinbarungen nach innen und außen bereitzustellen, die gut strukturiert und aktuell ist. Hierfür müssen SLM und Policy Management eine gut abgestimmte Umsetzungsstrategie entwickeln und die Einhaltung der Service-Vereinbarungen und Policies sicher stellen.

4.2.2 Verfügbarkeitsmanagement (Availability Management)

Ziele und Aufgaben

Das Verfügbarkeitsmanagement liefert die Standards für die Definition, Planung und Überwachung geeigneter Verfügbarkeitsstufen für IT-Services. Daneben definiert es auch die Anforderungen an die Wartung von Hardware- und Softwarekomponenten. Im Fokus des Verfügbarkeitsmanagements stehen die Zuverlässigkeit und Verfügbarkeit der eigenen IT-Services, die Verwaltbarkeit und Servicefähigkeit externer Lieferanten sowie die Wartbarkeit eingesetzter IT-Komponenten. Somit verwaltet und optimiert das Verfügbarkeitsmanagement auch die Wartungsverträge.

Gestaltung

Der Managementprozess kann in drei wesentliche Stufen gegliedert werden:

- Verfügbarkeitsplanung: Analyse der Geschäftsanforderungen an die Service-Verfügbarkeit, Analyse der Umsetzbarkeit über entsprechende Bewertungsmodelle und Referenzarchitekturen, Definition möglicher Verfügbarkeitsstufen für die Gestaltung der Service Levels.
- Verfügbarkeitsumsetzung: Anforderungen an die Servicefähigkeit der externen Provider definieren und in Absicherungsverträgen mit SLM vereinbaren, Anforderungen an die Systemverfügbarkeit definieren und in Architekturen und Leistungsprozessen umsetzen.
- Verfügbarkeitskontrolle: Überwachung und Analyse der erzielten Serviceverfügbarkeit, Ableitung von Verbesserungsmaßnahmen.

Für die Planung realistischer Verfügbarkeitszusagen und die Analyse von Schwachstellen haben sich zahlreiche Methoden etabliert. Darüber hinaus macht die Schaffung von Entwurfskriterien für Verfügbarkeit und Wiederherstellung eine enge Zusammenarbeit mit dem Architekturmanagement und den Spezialisten im Betrieb konkreter Plattformen erforderlich. Gleiches gilt für die Entwicklung geeigneter Verfahren zur Verfügbarkeitsüberwachung.

Hier wird auch deutlich, warum ITIL einen integrierten Management-Prozess empfiehlt: Die Serviceverfügbarkeit und -stabilität sind vom zuverlässigen Zusammenwirken verschiedenster IT-Komponenten abhängig.

Synergien mit dem Sicherheitsmanagement

Verfügbarkeit ist eines der zentralen Sicherheitsziele. Somit kann der Verfügbarkeitsmanagement-Prozess nicht nur als Service-Management-Prozess sondern auch als Teil des Sicherheitsmanagement verstanden werden. Der Prozess liefert nicht nur Standards für die Verfügbarkeit und Wartbarkeit der IT-Komponenten, er bewertet auch die Chancen und Risiken der Auslagerung von Prozessen und Infrastruktur für die Zuverlässigkeit der Services.

Folgende Beispiele sollen den Integrationsbedarf unterstreichen:

- **Analyse Verfügbarkeitsbedarf und Verwundbarkeit**: Das Sicherheitsmanagement leistet einen wesentlichen Beitrag im Verfügbarkeitsmanagement, wenn es um Business-Impact-Analysen zur Bewertung der Auswirkungen von Nichtverfügbarkeit geht. Auch in der Analyse und Bewertung der Zuverlässigkeit und Wiederherstellbarkeit von Services und hierfür benötigter Komponenten spielt das Sicherheitsmanagement eine wichtige Rolle. Dies betrifft auch die Überprüfung von Architekturen und Verfahren zur Gewährleistung von Hochverfügbarkeit.
- **Prävention**: Das Sicherheitsmanagement entwickelt Maßnahmen zur Vermeidung von Serviceausfällen in Folge von Sicherheitsvorfällen - insbesondere durch Denial-of-Service-Angriffe und Virenbefall.
- **Wiederanlauf und forensische Analyse**: Im Rahmen des Verfügbarkeitsmanagements werden geeignete Wiederanlaufverfahren definiert, die auch die notwendigen forensischen Maßnahmen berücksichtigen müssen. Auch hierfür bringt das Sicherheitsmanagement Anforderungen und Methoden mit ein.

4.2.3 Kapazitätsmanagement (Capacity Management)

Ziele und Aufgaben

Während das Verfügbarkeitsmanagement die Verfügbarkeit von Services sicher stellt, kümmert sich das Kapazitätsmanagement um den wirtschaftlichen Umgang mit (IT-)Ressourcen.

Das Kapazitätsmanagement analysiert die Kapazitätsanforderungen, plant und steuert den Ressourceneinsatz mit Blick auf die Wirtschaftlichkeits- und Performanceanforderungen an IT-Services und liefert Verfahren für die Überwachung von Servicekapazitäten und -performance.

Mit dem Kapazitätsmanagement steht der IT-Service-Organisation also ein wichtiges Instrument zur Reduzierung und Flexibilisierung der Servicekosten zur Verfügung.

Gestaltung

Der Kapazitätsmanagementprozess muss in der Praxis auf drei Ebenen greifen: auf Geschäfts-, Service- und Ressourcenebene. Die Performance- und Kapazitätsanforderungen lassen sich also aus den Geschäftsanforderungen an IT-Services ableiten und auf die hierfür benötigten Ressourcen übertragen.

In Feldern mit stark schwankendem IT-Bedarf hat das Geschäfts- und Service-Kapazitätsmanagement eine wichtige Funktion, um Veränderungen frühzeitig zu erkennen. Auf der Ressourcenebene des Kapazitätsmanagements müssen dann Performance und Wirtschaftlichkeit aufeinander abgestimmt werden. Optimierungsansätze wie z. B. Konsolidierung, Virtualisierung, Tuning oder Kapazitätserweiterung sollten also direkt aus dem Kapazitätsmanagement heraus verfolgt werden.

Auch hier wird deutlich, warum ITIL einen durchgängigen Managementprozess empfiehlt: Die Leistungsfähigkeit der Services wird letztendlich durch gut aufeinander abgestimmte Teilkomponenten bestimmt. Mit Blick auf die Serviceanforderungen des Kunden wird deshalb ein integriertes Management benötigt, das in allen Bereichen des IT-Betriebs gleichermaßen wirksam wird.

- Kapazitätsmanagement auf Geschäftsebene: stellt die Kapazitätsplanung auf Grundlage von Prognosen zum IT-Bedarf sicher (Planning), entwickelt Modelle für Szenarioanalysen (Modelling) und bestimmt die erforderlichen Kapazitäten für die Unterstützung der Anwendungen (Application Sizing).
- Kapazitätsmanagement auf Service & Ressourcenebene: stimmt die Ressourcen auf die Anforderungen ab (Tuning) und implementiert diese, misst, überwacht und analysiert die Performance und leitet Optimierungsmaßnahmen ab. Grundlage für die Messung sind hierbei in der Regel definierte Schwellwerte für Kapazität und Leistung konkreter Ressourcen oder für entsprechende Service Levels konkreter Services.

Synergien mit dem Sicherheitsmanagement

Eine Zusammenarbeit zwischen Kapazitäts- und Sicherheitsmanagement ist empfehlenswert, wenn Kapazität und Leistung von Services und Ressourcen Sicherheitsrelevanz besitzen. Da die Bereitstellung angemessener Kapazitäten die Service-Verfügbarkeit beeinflusst, liegen die wichtigen Zusammenhänge auf der Hand. Zwei Beispiele sollen die Berührungspunkte veranschaulichen:

- **Mindestkapazitäten bei Sicherheitsvorfällen**: Sicherheits-, Verfügbarkeits- und Kapazitätsmanagement arbeiten z. B. in der Wiederanlaufplanung zusammen, wenn notwendige Mindestkapazitäten zur vorübergehenden Wiederherstellung von Services zu ermitteln und zu planen sind, die durch bestimmte Angriffsszenarien beeinträchtigt wurden. Dies ist auch in Verbindung mit der Anforderung zu sehen, dass Services ggf. auf Ausweichressourcen wieder hergestellt werden müssen, z. B. um eine Beweismittelsicherung zu ermöglichen.
- **Erkennung von Sicherheitsvorfällen**: Abweichungen im Lastverhalten von Konfigurationselementen können Symptom vielfältiger Sicherheitsvorfälle sein. Hier geht es darum, Anomalien zu erkennen und in richtiger Weise zu behandeln. Der Problemmanagement Prozess kann hierfür

sensibilisiert werden, wenn Kapazitäts- und Sicherheitsmanagement auffällige Muster beschreiben und Verfahren für die Vorfallerkennung aus dem Performance-Monitoring bereit stellen.

4.2.4 Service Continuity Management

Ziele und Aufgaben

Die Aufgabe des Continuity Management für IT-Services liegt in dem Support des übergeordneten Business Continuity Management (BCM), indem sicher gestellt wird, dass die IT-Infrastruktur und die IT-Services (einschließlich Support und Service Desk) nach einer Katastrophe möglichst rasch wieder hergestellt werden. Die Zielsetzungen des ITSCM (IT-Service Continuity Management) können jedoch recht unterschiedlich sein. Da das ITSCM ein integraler Bestandteil des BCM ist, muss zunächst der Umfang des ITSCM aus den geschäftlichen Zielvorgaben abgeleitet werden.

Wichtig für die erfolgreiche Umsetzung des Gesamtkomplexes Continuity Management ist die saubere Definition der Begriffe Service-, Systems- und Business Continuity. In der Praxis werden diese oft vermischt. Konsequenz hieraus ist in vielen Fällen, dass zwar das technisch orientierte Thema Systems Continuity behandelt wird, dieses aber inhaltlich mit der Business Continuity verwechselt und dieses daher unberücksichtigt bleibt.

- Das Business Continuity Management (BCM) beschäftigt sich mit der Analyse und dem Management der Risiken, damit die Organisation jederzeit die erforderliche Mindestproduktionskapazität und/oder Mindest-Service gewährleisten kann.
- Das Service Continuity Management (ITSCM) ist der Prozess, der erforderlich ist, um innerhalb des IT-Service Katastrophen aufzufangen und zu überleben, damit eine Institution ihren Betrieb fortsetzen kann. Basis für eine erfolgreiche Abwicklung ist selbstverständlich die Definition sauberer Services und SLAs, hier insbesondere aus dem Blickwinkel Verfügbarkeit. Diese stellen somit auch das Bindeglied zwischen den betrieblichen Anforderungen aus dem Business Continuity Management und den technischen Verfügbarkeitsaussagen einzelner Systeme aus dem Systems Continuity Management. Die Definition von Services kann hier also den oft aufwendigen Prozess der Zuordnung von Prozessen über Anwendungen zu Systemen deutlich vereinfachen. Ein gemäß ITIL aufgebautes Service Continuity Management beinhaltet im Normalfall bereits das Systems Continuity Management.
- Das Systems Continuity Management (SCM) sorgt für die technische Umsetzung der Verfügbarkeitsanforderungen auf die konkreten Systeme sowohl im Sinne der Vorsorge (z. B. durch Doppplung von Systemen, Aufteilung von Rechenzentren etc.) als auch im Sinne der Gewährleistung eines optimalen Wiederanlaufs, falls die proaktiven Maßnahmen einen Notfall nicht verhindern konnten. Ein eigenständiges Systems Continuity ist nur dann sinnvoll und erforderlich, wenn eben nicht gerade analog zu ITIL der Servicegedanke eine entscheidende Größe im IT-Management darstellt.

Gestaltung

Organisatorisch ist der Gesamtprozess Continuity Management noch stärker als andere hier genannte Themen von Haus zu Haus unterschiedlich. Durch den Querschnittscharakter der Aufgabe und dem hohen Integrationsgrad verschiedenster Aspekte wird dieses Thema in der Praxis sowohl beim Risikomanagement, in der Organisation, im Sicherheitsmanagement als gesonderte Stabsstelle oder integriert im IT-Management angegliedert. Jede dieser Ausprägungen kann erfolgreich umgesetzt werden, wobei die IT hier eine besondere Rolle spielt: übernimmt sie das Thema komplett, droht oft das oben beschriebene Szenario der Technik-Lastigkeit. Wird sie ausgeklammert, bleibt die Anbindung an die konkrete Technik oft im luftleeren Raum hängen. Daher ist die erfolgversprechendste Variante oft die Kombination aus der Anlagerung technischer Verantwortung im IT-Bereich und der Gesamtverantwortung an einer der anderen oben beschriebenen Stellen.

Dies entspricht somit auch genau der ITIL-Philosophie der Trennung von Service und Business Continuity, da sich Service Continuity auf rein technische Aspekte beschränkt, während das Business Continuity Management die Geschäftsprozesse in den Vordergrund stellt und somit die Basis für ein sinnvolles Service Continuity Management bildet. Es beschreibt genau den übergreifenden Ablauf des Continuity Managements:

- Definition der Grundsätze und inhaltlichen Schwerpunkte: Was ist ein Notfall? Was wird bewusst ausgeklammert?
- Folgeschädenanalyse (Business Impact Analyse): Bewertung der Kritikalität von Geschäftsprozessen und Zuordnung der erforderlichen IT-Services sowie benötigter Infrastrukturkomponenten. Dann erfolgt eine Folgeschädenabschätzung für den Wegfall einzelner Geschäftsprozesse bzw. betroffener Infrastrukturkomponenten.
- Risikoanalyse: Analyse der Bedrohungen und Schwachstellen, Risikobewertung
- Continuity-Strategie: Präventivmaßnahmen und Wahl der Kontinuitätsoptionen
- Planung: Katastrophenplan, Wiederherstellungsprozesse, Krisenmanagement etc.
- Implementierung: Vorsorgemaßnahmen, Notfallorganisation, Wiederherstellungsverfahren
- Operatives Management: Übungen, Schulungen, Weiterentwicklung

Synergien mit dem Sicherheitsmanagement

Beim Service Continuity Management ist die Beziehung zur IT-Sicherheit von allen Themen am offensichtlichsten und innerhalb von ITIL klar definiert. Allein die weitgehende Deckungsgleichheit des oben beschriebenen Vorgehens mit den Vorgaben des IT-Grundschutzhandbuches verdeutlicht dies.

In vielen Institutionen wird das Thema Wiederanlaufpläne, Sicherung der Hochverfügbarkeit etc. wie oben erwähnt grundsätzlich von der IT-Sicherheit mit behandelt. Hier gilt es in erster Linie, eine geeignete Rollenverteilung und Zusammenarbeit zwischen IT, IT-Sicherheit und dem operationalen Risikomanagement zu schaffen, um ein stimmiges Gesamtkonzept mit konsistenten Argumentationsketten vom Geschäftsprozess bis zum darauf abgestimmten IT-Service-Management zu erreichen.

Die Kombination der klassischen Schutzbedarfsfeststellung mit der Business Impact Analyse, die ja nach obiger Definition nur die konkrete Ausprägung einer Schutzbedarfsfeststellung für das Sicherheitsziel Verfügbarkeit ist, liegt nahe. Bei richtiger Durchführung der Analyse von Abhängigkeiten erreicht man hier die gewünschte Transparenz der Sicherheitsvorgaben anstelle der oft erforderlichen Pauschalierung.

4.2.5 Finanzmanagement (Financial Management)

Ziele und Aufgaben

Das Finanzmanagement für IT-Services unterstützt das Management in der Gewährleistung der Wirtschaftlichkeit von IT-Services. Es macht diese plan- und steuerbar und liefert hierfür die entsprechenden Verfahren.

Gestaltung

Je nach betriebswirtschaftlichem Status der IT-Service-Organisation als Cost oder Profit Center werden entwickelte Verfahren zur betriebswirtschaftlichen Steuerung der IT-Services benötigt. Die wesentlichen in ITIL empfohlenen Verfahren werden nachfolgend kurz zusammen gefasst:

- Die Finanz- und Budgetplanung (Budgeting): liefert Modelle und Verfahren zur Planung und von Service-Erlösen, Investitionen und Aufwenden und deren Verfolgung.
- Die Kostenrechnung und -analyse (Accounting): schafft Kostentransparenz aus verschiedenen Managementblickwinkeln. Sie soll die Verursachung von Aufwand nach Kostenarten und Kos-

tenstellen sichtbar machen wie auch die Verursacher (Kostenträger) in Form von Services und Projekten. Ein leistungsfähiges Accounting ist Voraussetzung für eine verursacher- und verursachungsgerechtere Kalkulation von IT-Services und Projekten.

- Die Serviceverrechnung (Charging): stellt die Abrechnungsprozesse für IT-Services sicher.

Daneben stellt das Finanzmanagement im Rahmen des Asset Managements in der CMDB auch betriebs-wirtschaftliche Informationen über IT-Komponenten bereit - z. B. Aktivwerte und Abschreibungsaufwand.

Synergien mit dem Sicherheitsmanagement

Sicherheit ist Nutzentreiber und Kostenfaktor in IT-Services. Zwei Beispiele sollen das Zusammenwirken von Finanz- und Sicherheitsmanagement veranschaulichen:

- **Wirtschaftlichkeitsbetrachtungen**: Das Finanzmanagement unterstützt in dem Fall, in dem alternative Sicherheitsmaßnahmen nach Wirtschaftlichkeitsgesichtspunkten zu analysieren und zu priorisieren sind. Die Herstellung von Nutzen-/Aufwand-Transparenz trägt wesentlich zur Akzeptanz bei Kunden und Management bei. Auch wenn der „Return on Security Investment“ oft schwer realistisch ermittelbar ist, kann er ein wesentliches Kriterium für die Lenkung der Sicherheitsmaßnahmen sein. Während das Finanzmanagement die Methoden liefert, muss das Sicherheitsmanagement die Angemessenheit der Investitionen mit Blick auf den Sicherheitswert beurteilen.
- **Sicherheitsservices**: SLM und Finanzmanagement können spürbar zur Akzeptanz der Leistungen des Sicherheitsmanagements beitragen, wenn sie verursacher- und verursachungsgerecht in den jeweiligen Services berücksichtigt werden. Mitunter ergeben sich hieraus auch eigene Sicherheits-Basisservices, die dem Kunden eine bessere Leistungstransparenz bieten und genau dort verrechnet werden, wo sie tatsächlich benötigt und erbracht werden. Das Servicemanagement unterstützt hier in der Servicedefinition und in der Gestaltung der Verrechnungsmodelle.

5 Gegenüberstellung ITIL und IT-Grundschutzhandbuch

Dieses Kapitel veranschaulicht als Abschluss noch einmal die Berührungspunkte zwischen ITIL und IT-Sicherheit. Die nachfolgende Tabelle enthält eine Übersicht, die aufzeigt, in welchen Kapiteln ("Bausteinen") des IT-Grundschutzhandbuchs Inhalte und Themen angesprochen werden, die auch in ITIL behandelt werden. Es zeigt sich sehr deutlich, wie groß die Schnittmenge ist, was die These, dass sich in der Praxis durch Zusammenspiel aus ITIL und IT-Grundschutz merkliche Synergieeffekte erzielen lassen können, verdeutlicht.

Jedes Feld mit einem **x** zeigt Übereinstimmungen von Inhalten des jeweiligen Grundschutzbausteins und Anforderungen aus dem zugeordneten ITIL-Prozess an. Ist die Tabellenzelle leer, beschreibt der Baustein keine Anforderung aus dem ITIL-Prozess. Es sind nur Bausteine aufgeführt, die mindestens Anforderungen aus einem ITIL-Prozess beschreiben.

Baustein	Konfigurations-management	Störungs-management	Service Desk	Problem-management	Änderungs-management	Versions-management	Service Level Management	Verfügbarkeits-management	Kapazitäts-management	IT-Service Continuity	Finanz-management
IT-Sicherheitsmanagement	x					x	x	x			
Organisation	x	x		x	x	x	x	x	x		
Notfallvorsorge-Konzept		x		x			x	x	x	x	
Datensicherungskonzept								x			
Computer-Virenschutzkonzept	x				x	x		x			
Behandlung von Sicherheitsvorfällen		x		x							
Hard- u. Software-Management	x	x	x	x	x	x	x	x	x	x	
Outsourcing	x				x	x	x	x	x	x	
Verkabelung								x	x	x	
Serverraum								x		x	
Heterogene Netze								x		x	
Datenträgeraustausch						x		x			
Standardsoftware	x				x	x					
Archivierung								x	x		
Schutzbedarfsfeststellung[1]	x							x			

Tabelle 1: ITIL-Prozesse und Bausteine des Grundschutzhandbuches mit übereinstimmenden Anforderungen

[1] Die Schutzbedarfsfeststellung ist kein eigener Baustein, sondern Teil der Risikobewertung der IT-Grundschutz-Vorgehensweise.

6 Fazit

Die genannten Beispiele zeigen deutlich, dass die frühzeitige Einbeziehung des Sicherheitsmanagements bei einer Implementierung von IT-Service-Management-Prozessen, sowohl in ökonomischer als auch sicherheitstechnischer Hinsicht mehr als sinnvoll ist. Umgekehrt kann IT-Sicherheit nur dann wirksam implementiert werden, wenn sich alle Sicherheitsmaßnahmen auf klar definierte Prozesse und Serviceanforderungen beziehen. Alle genannten ITIL-Themen sind ohnehin Aufgaben, die vom Sicherheitsmanagement mit betrachtet und bearbeitet werden sollten. ITIL bietet nun die Möglichkeit, diese Einzelaufgaben (die oft genug nur unregelmäßig als Ad-hoc-Tätigkeit betrieben werden) zu institutionalisieren und als unterstützende Prozesse für den Gesamtkomplex IT zu etablieren.

Ein weiterer nicht zu vernachlässigender Aspekt ist die gesteigerte Aufmerksamkeit des Managements für die IT-Sicherheit, die durch das Aufzeigen der hier genannten Berührungspunkte und Synergieeffekte entsteht. Gerade in Behörden und Unternehmen, die derzeit ITIL umsetzen oder damit liebäugeln, sollten sich Sicherheitsverantwortliche von Anfang an in diesen Gestaltungsprozess integrieren!

ITIL ermöglicht es, bei konsequenter Integration des Themas IT-Sicherheit in Geschäftsprozesse einerseits die sicherheitstechnischen Anforderungen transparenter zu machen und andererseits das Sicherheitsmanagement frühzeitiger und somit produktiver in Entscheidungsprozesse mit einzubinden.

Die Verinnerlichung des Servicegedankens auch im Sicherheitsmanagement kann dazu führen, auch die Sicherheit an sich als Service zu definieren. Damit würde sich der Kreis zum IT-Grundschutzhandbuch schließen. Denn die Umsetzung der Maßnahmen für den normalen Schutzbedarf sind nichts anderes als konkrete Vorschläge für einen speziellen Sicherheitsservice (und Service Level). Dieser Service Level kann dann gegebenenfalls um ergänzende Sicherheitsservice-Pakete für den hohen Schutzbedarf etc. ergänzt werden.

Die Maßnahmen des IT-Grundschutzhandbuches sind somit nichts anderes als einzelne Servicebausteine innerhalb eines Services. Die mit der Umsetzung entstehenden Sicherheitskosten werden somit finanziell quantifizierbar und könnten verursachergerecht umgelegt werden.

Wie zu erwarten, zeigen speziell die Grundschutzbausteine Organisation, Hard- und Software-Management, Notfallvorsorge-Konzept sowie Outsourcing große Übereinstimmungen mit den Anforderungen der ITIL-Prozesse. Weitere Anforderungen aus ITIL-Prozessen finden sich in den anderen, im Kapitel 5 dieses Dokumentes zugeordneten Bausteinen wieder.

7 Verweise

[1] IT Service Management, eine Einführung, van Haren Publishing, V1.0 März 2002, ISBN 9077212124

[2] http://www.sei.cmu.edu/cmm/

[3] Qualitätsmanagement nach ISO 9001:2000, Michael Cassel, Hanser Verlag, München

[4] http://www.itsmf.net

[5] http://www.bcs.org/BCS/Products/Qualifications/ISEB/

[6] http://www.exin.nl

[7] http://emea.bsi-global.com/IT+Service+Management/Overview/WhatisBS15000.xalter

[8] A Manager's Guide to Service Management, British Standards Institution, London, ISBN 0580427641

[9] IT Service Management. Self-assessment Workbook, British Standards Institution, London, ISBN 0580337125

[10] BS ISO/IEC 17799:2000, Informationstechnik - Leitfaden zum Management von Informationssicherheit, (Deutsche Übersetzung), British Standards Institution, London

[11] http://emea.bsi-global.com/InformationSecurity/Overview/WhatisBS7799.xalter

[12] IT-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, Köln, ISBN 3887849159

[13] http://www.bsi.de