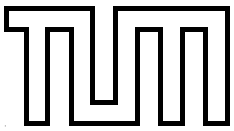
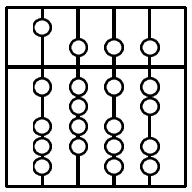


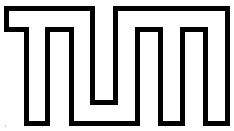
FAKULTÄT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit in Informatik

Managementsystem für das Intrusion Detection System im Bayerischen Behördennetz

Matthias Braun





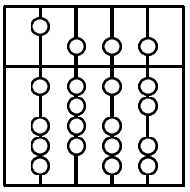
FAKULTÄT FÜR INFORMATIK

DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit in Informatik

Managementsystem für das Intrusion Detection System im Bayerischen Behördennetz

Bearbeiter:	Matthias Braun
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Dipl.-Inform. Nils O. v. d. gentschen Felde Dr. Helmut Reiser Dipl.-Inform. Bernhard Wager Dr. Thomas Peschel-Findeisen
Abgabedatum:	18. April 2006



Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 18. April 2006

. . . . . .

(Unterschrift des Kandidaten)

IT-Sicherheit und IT-Management – beides sind Themen, die in den vergangenen Jahren nicht zuletzt aufgrund der immer dichter werdenden Vernetzung von IT-Systemen an Bedeutung gewonnen haben.

Diese Arbeit schlägt quasi eine Brücke zwischen beiden Themengebieten. In ihr wird die Entwicklung eines Managementkonzepts zum Betrieb von Intrusion Detection Systemen beschrieben. Bei Intrusion Detection Systemen handelt es sich um Systeme zur Erkennung von Angriffen auf eine IT-Infrastruktur. Mit Hilfe eines effektiven und effizienten Managements kann der Einsatz der Systeme optimiert werden.

In der Arbeit wird die optimale Gestaltung der Infrastruktur von Intrusion Detection Systemen aus Managementsicht eingehend erörtert. Anschließend werden auf Basis des Service Support Managements der IT Infrastructure Library (ITIL) Prozessabläufe festgelegt, die eine strukturierte Bewältigung der im Betrieb anfallenden Aufgaben ermöglichen. Die IT Infrastructure Library ist eine Sammlung von Best-Practice-Ansätzen zur Unterstützung des IT Service Managements (ITSM). Als IT Service Management wird die Gesamtheit der Maßnahmen bezeichnet, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu ermöglichen.

Das vorgestellte Konzept zum Management eines Intrusion Detection Systems wird anschließend prototypisch im Bayerischen Behördennetz umgesetzt, um zu überprüfen, inwieweit es in der Praxis realisierbar ist.

Danksagung

Bei der Entstehung vorliegender Arbeit haben mich zahlreiche Leute mit ihrer Hilfe unterstützt, wofür ich hier allen meinen Dank aussprechen möchte.

Ganz besonderen Dank möchte ich an meine Betreuer am Lehrstuhl von Prof. Dr. Hegering, Nils gentschen Felde und Dr. Helmut Reiser, richten. Insbesondere Nils gentschen Felde stand mir in jeder Phase der Arbeit hilfreich zur Seite und hat mit Vorschlägen und konstruktiver Kritik wesentlich zu ihrem Gelingen beigetragen. Auch Michael Brenner und Dr. Markus Garschhammer – ebenfalls Mitarbeiter des Lehrstuhls – möchte ich für ihre Anregungen danken.

Herzlicher Dank gebührt außerdem Bernhard Wager und Dr. Thomas Peschel-Findeisen vom Landesamt für Statistik und Datenverarbeitung, bei denen ich jederzeit ein offenes Ohr gefunden habe. Mein Dank richtet sich aber auch an alle anderen Mitarbeiter des Landesamtes die mich mit ihren Ideen auf den richtigen Weg gebracht haben.

Nicht zuletzt möchte ich meiner Familie danken, die mich nicht nur während dieser Arbeit, sondern während des gesamten Studiums unterstützt hat. Ein herzliches Dankeschön an dieser Stelle noch an meine Großmutter, die sich mit der für sie fremden und trockenen Materie der vorliegenden Arbeit auseinandergesetzt hat, um dem Fehlerteufel den Garaus zu bereiten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

1.1 Motivation

In kaum einem anderen Bereich war der Fortschritt in den letzten beiden Jahrzehnten so groß wie im Bereich der Infomationstechnologie. Besonders die globale Vernetzung von IT-Systemen ist rasant vorangeschritten. Die meisten privaten Haushalte verfügen in Deutschland heutzutage über einen Internetanschluss, und im beruflichen Umfeld ist eine Arbeit ohne IT-Unterstützung in den meisten Branchen undenkbar. Von besonderer Bedeutung ist hier der Austausch von Informationen, sprich Kommunikation. Die Kommunikation ist zur Aufrechterhaltung geschäftlicher Beziehungen unverzichtbar. Mussten aber früher noch beschwerliche Wege in Kauf genommen werden, um miteinander in Kontakt treten zu können, so bestehen heutzutage dank technischer Errungenschaften vielfältige Möglichkeiten zum schnellen und unkomplizierten Informationsaustausch. Dabei hat in den vergangenen Jahren vor allem die Kommunikation mit Hilfe vernetzter Systeme immer mehr an Bedeutung gewonnen und gewinnt sie noch weiter. Was Ende der fünfziger Jahre mit der Entwicklung des ARPANETs begann und uns heute als Internet bekannt ist (siehe [Tane03]), ist aus unserem Alltag kaum noch wegzudenken. Neben der Kommunikation spielt heute zunehmend das Sammeln, Verarbeiten, Aufbereiten und Verteilen von Informationen eine bedeutendere Rolle (vgl. [Tane03]). Informationen sollen heute möglichst von jedem Ort aus zu jeder Zeit zugänglich sein. Es kann vom Zeitalter der Informations- und Kommunikationstechnologien gesprochen werden. Stichworte sind E-Mail, Videokonferenz, Data Warehouse und viele mehr.

So viele positive Eigenschaften die beschriebene Entwicklung bietet, bringt sie aber auch einige Probleme mit sich. Es wird zwar ein ungehinderter globaler Informationsfluss gewünscht, jedoch sollen dabei auf vertrauliche Informationen nur berechtigte Personen Zugriff haben. Gleiches gilt für die Datenspeicherung. Daten die von verschiedenen Orten aus abgerufen werden können, sollen nicht unbedingt in Jedermanns Hände gelangen. Ein weltweit tätiges Unternehmen möchte seinen Mitarbeitern in Deutschland beispielsweise Zugriff auf den Firmenserver in den USA gewähren. Sicherlich will das Unternehmen aber nicht, dass ein Konkurrenzunternehmen ebenfalls Zugriff auf dort gespeicherte Informationen bekommt. Leider ist aber das Risiko von Angriffen auf vernetzte Systeme, parallel zu ihrer schnellen Weiterentwicklung, stetig gewachsen. Es gilt also entsprechende Maßnahmen zu ergreifen, um die Informationssicherheit zu gewährleisten. Diese wird nach Eckert [Ecke03] folgendermaßen beschrieben:

> „Die Informationssicherheit (engl. security) ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen."

Um dies zu gewährleisten existieren bereits verschiedene Schutzvorrichtungen. Virenscanner

sollen Schadprogramme entdecken, die vorhandene Sicherheitslücken ausnutzen. Mit Hilfe von Firewalls kann ein lokales Netz von anderen Netzen abgeschirmt werden, sodass ein netzübergreifender Informationsaustausch nur nach definierten Regeln stattfinden kann. Sowohl Firewalls als auch Virenscanner stellen aber in erster Linie präventive Maßnahmen zum Schutz eines Rechnernetzes zur Verfügung. Zur weiteren Verbesserung der Informationssicherheit reicht Prävention alleine aber nicht mehr aus. Eine Möglichkeit zur Erweiterung einer bestehenden Sicherheitsstruktur liegt im Einsatz von Intrusion Detection Systemen.

Intrusion Detection Systeme sind in der Lage Angriffe oder Bedrohungen zu erkennen. d. h. sie dienen nicht alleine der Prävention, sondern auch der Detektion von Angriffen. Somit stellen sie neben den präventiven Vorkehrungen zum Schutz eines Rechnernetzes eine sinnvolle Ergänzung dar.

Der Fortschritt in der Entwicklung von Informations- und Kommunikationstechnologien bringt aber nicht nur Fragen im Bereich der Informationssicherheit mit sich. Die Komplexität bestehender Netzwerkstrukturen wird durch ihre ständige Erweiterung zunehmend höher. Die Tatsache, dass dabei stets die Sicherheit des Netzwerks gegen Angriffe gewährleistet sein soll, erhöht die Komplexität noch zusätzlich. Effektives und effizientes Management wird also zunehmend zu einem zentralen Thema der IuK-Technologie – auch im Bereich der IT-Sicherheit.

1.2 Idee

Der vorige Abschnitt hat die Herausforderungen gezeigt, denen sich eine moderne IuK-Gesellschaft stellen muss, und weshalb die Bereiche IT-Sicherheit und Mangament vernetzter IT-Systeme zunehmend an Bedeutung gewinnen. Neue Techniken, wie Intrusion Detection Systeme (IDS), können dazu beitragen die IT-Sicherheit zu erhöhen. Eine echte Hilfe stellen sie aber nur dann dar, wenn es gelingt, die Systeme derart effizient zu integrieren, dass die Komplexität bestehender Informationssysteme und Netzwerkstrukturen möglichst nicht weiter zunimmt.

Diese Erkenntnis führt direkt zur Aufgabenstellung für diese Diplomarbeit. Es soll ein Konzept entwickelt werden, auf dessen Basis sich ein IDS effizient verwalten lässt. Dieses Managementkonzept gilt es dabei so zu gestalten, dass eine flexible Anpassung an seine jeweilige Einsatzumgebung möglich ist. Das bedeutet, es soll sowohl hinsichtlich bestehender Netztopologien als auch bestehender organisatorischer Abläufe generisch gehalten sein. Zwei Punkte werden dabei besonders herausgestellt. Zum einen wird die optimale Gestaltung der Infrastruktur von Intrusion Detection Systemen eingehend erörtert. Zum anderen werden auf Basis des Service Support Managements der IT Infrastructure Library (ITIL) Prozessabläufe festgelegt, die eine strukturierte Bewältigung der im Betrieb anfallenden Aufgaben ermöglichen.

Die ITIL beschreibt ein Best Practice Framework zur Unterstützung des IT Service Managements (ITSM). Mit Hilfe des ITSM soll eine bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation ermöglcht werden. Die Herangehensweise an das Management vernetzter Systeme erfolgt in der ITIL dabei nicht aus rein technischer Sicht, sondern vor allem unter organisatorischen Aspekten. Im Vordergrund steht immer die Frage, wie ein Provider (Dienstleistungsanbieter) dem Kunden (Dienstleistungsempfänger) einen Service in möglichst

optimaler Qualität anbieten kann.

Das in der Arbeit entwickelte Managementkonzept wird anschließend auf seine Praxistauglichkeit getestet. Es wird versucht die Vorschläge im Bereich des Landesamtes für Statistik und Datenverarbeitung (LfStaD) umzusetzen. Das LfStaD ist der Betreiber des Bayerischen Behördennetzes (BYBN). Die Zusammenarbeit mit dem LfStaD bietet sich aufgrund des Vorhabens an, im Bayerischen Behördennetz ein Intrusion Detection System einzusetzen.

Da dort zum jetzigen Zeitpunkt noch kein Intrusion Detection System zum Einsatz kommt, steht auch noch nicht fest um welches Produkt es sich handeln wird. Für den Fall, dass die Komplettlösung eines Herstellers zum Einsatz kommt, die bereits Möglichkeiten zum Management beinhaltet, sollen sich diese leicht in das entwickelte Konzept integrieren lassen.

2 Grundlagen

Dieses Kapitel bespricht die Grundlagen für die vorliegende Arbeit. Abschnitt 2.1 gibt eine Einführung in das Themengebiet der Intrusion Detection Systeme – im weiteren auch als IDS bezeichnet – und deren unterschiedliche Ausprägungen. In Abschnitt 2.2 wird auf die Grundlagen des Managements vernetzter IT-Systeme eingegangen. Als Grundlage für Managementarchitekturen werden vier Teilmodelle eingeführt. Im Anschluss daran werden die Grundzüge des IT Service Managements (ITSM) auf Basis der IT Infrastucture Library (ITIL) erläutert, da sich das in Kapitel 3 zu entwickelnde Managementkonzept für IDS ebenfalls daran orientiert. Dieses wird exemplarisch am Bayerischen Landesamt für Statistik und Datenverarbeitung (LfStaD) umgesetzt. Deshalb erfolgt in Abschnitt 2.3 ein Einblick in den Aufgabenbereich und die Netzwerktopologie des Landesamtes. Darüber hinaus werden Kriterien für den Einsatz eines IDS am LfStaD genannt.

2.1 Intrusion Detection Systeme

Bevor mit weiteren Ausführungen zu Intrusion Detection Systemen begonnen werden kann, gilt es zuallererst zu klären, wie der Begriff eines „Intrusion Detection Systems“ überhaupt definiert werden kann. Es ergeben sich unterschiedliche Bedeutungen, je nachdem, ob man Intrusion aus dem Wörterbuch mit einem Begriff wie „Einbruch“, „Störung“ oder „Verletzung“ ins Deutsche übersetzt. Zumeist wird von einem „Einbruchs-“ beziehungsweise „Eindringlings-Erkennungs-System“ gesprochen. Diese Übersetzung beschreibt die Aufgabe eines IDS aber nur unvollständig, da der Begriff Einbruch oder Eindringling einen unerlaubten Netzwerkzugriff von außen suggeriert. Viele Angriffe finden aber innerhalb der jeweiligen Netzwerke statt, beispielsweise durch Mitarbeiter einer Firma die Zugang zum Firmennetz haben. Angesichts dieser Tatsache erweckt diese Definition also einen verkehrten oder zumindest unvollständigen Eindruck.

In Anlehnung an die Ausführungen von Spenneberg [Spen03] wird deshalb folgende Definition vorgenommen:

Definition 2.1 *Ein Intrusion Detection System ist ein System, welches in der Lage ist, nicht autorisierte Zugriffe oder Aufrufe auf einem Rechner oder in einem Rechnernetz zu erkennen und zu melden.*

Die Definition ist sehr allgemein gefasst, aber für die weiteren Ausführungen sinnvoll und ausreichend. „Nicht autorisierte Zugriffe oder Aufrufe“ werden im Folgenden auch als „Angriff“ oder „Einbruch“ bezeichnet. Hierzu ist anzumerken, dass sehr wohl auch durch autorisierte Zugriffe eine Verletzung der IT-Sicherheit verbunden sein kann, wenn eine unerlaubte Weitergabe

Aufgabe der Komponente:	Arbeitsschritt:
Informationsbeschaffung	Überwachung festgelegter Bereiche eines Informationssystems und Datensammlung. Beispiel: „Mitschneiden“ von Netzverkehr.
Informationsauswertung	Analyse der Daten (vgl. Abschnitt 2.1.2), die durch eine oder mehrere Komponenten zur Informationsbeschaffung gesammelt wurden. D. h. die Daten werden nach Auffälligkeiten, die auf einen Angriffsversuch hinweisen könnten, untersucht.
Signalisierung/Reaktion	Aufbereitung und Darstellung von Auffälligkeit bei der Datenanalyse. Evtl. Ergreifung automatischer Gegenmaßnahmen.
Management	Verwaltung der anderen Komponenten. Die Managementeinheit stellt sozusagen den zentralen Überbau zu den anderen Einheiten dar.
Datenspeicherung	Speicherung der Ereignisdaten zur späteren Rückverfolgung und Weiterverarbeitung.

Tabelle 2.1: Komponenten eines IDS und ihre Aufgabe

der Informationen erfolgt. Die Erkennung derartiger Sicherheitsverletzungen wird hier aber ausgeschlossen, da sie ohnehin – zumindest auf technischem Wege allein – nicht möglich ist. Um dies an einem kurzen Beispiel zu erläutern: Ein Benutzer hat beispielsweise Zugriff auf ein für den firmeninteren Gebrauch bestimmtes Dokument und besitzt darüber hinaus Druckrechte. Wenn er nun das firmeninterne Dokument zuerst aufruft und anschließend ausdruckt, stellen beide Vorgänge keinerlei Sicherheitsverletzung dar, der Administrator war schließlich dazu autorisiert. Eine Sicherheitsverletzung würde erst stattfinden, wenn das ausgedruckte Dokument beispielsweise an ein Konkurrenzunternehmen übermittelt würde. Solch eine Sicherheitsverletzung kann durch ein IDS nicht erkannt werden.

Zur übersichtlicheren Strukturierung wird ein IDS hier in verschiedenen Teilkomponenten aufgesplittet, denen jeweils ein bestimmter Arbeitsschritt zufällt (Tabelle 2.1). Die Gliederung der Arbeitsschritte ergibt sich aus den bei König [Koen03] oder gentschen Felde [Feld05] aufgeführten Ansätzen. Die jeweilige Zuordnung der Teilkomponenten erfolgt sinngemäß.

Die Aufteilung in die Teilkomponenten ist hier bewusst abstrahiert dargestellt, da Bezeichnungen wie Sensor oder Agent in der Literatur oftmals unterschiedlich gebraucht werden. Das Bundesamt für Sicherheit in der Informationstechnik spricht von „Sensoren, die [..] als eigenständiges System den Netzverkehr überwachen (Netzsensoren) oder als Agenten auf dem zu überwa-

chenden System betrieben werden (Hostsensoren)“ [BSI02a]. In diesem Sinne wird auch hier im Weiteren von Sensoren – als Oberbegriff – die Rede sein. Dabei kann ein Sensor einerseits reine Informationsbeschaffungseinheit sein, andererseits aber auch eine vorverarbeitende Auswertungslogik enthalten. In der Praxis hängt dies vom jeweils eingesetzten IDS ab, wobei der Übergang fließend ist. Zur späteren Beschreibung des Managements von IDS ist aber eine klare Unterscheidung, wie in Tabelle 2.1 vorgenommen, sinnvoll.

Das Management ist dabei der entscheidende Faktor für die effektive und effiziente Zusammenarbeit aller Teilkomponenten, um den Schutz eines – meist vernetzten – Systems zu gewährleisten. Dabei stellt die Implementierung eines IDS alleine aber lediglich eine von vielen in Frage kommenden Sicherheitsmaßnahmen dar. Je nachdem, wie wertvoll die zu schützenden Informationen sind, müssen zusätzliche Maßnahmen ergriffen werden.

Meist fallen dabei im Zusammenhang mit dem Thema Netzwerksicherheit die Schlagworte „Firewall“ oder „Proxy“. Würden diese nicht bereits ausreichend Schutz bieten? Um diese Frage zu klären ist es notwendig die grundlegenden Unterschiede zwischen einem IDS und einer Firewall beziehungsweise einem Proxy zu klären.

Im Bereich der Computernetze stellt eine Firewall eine Abschirmung zweier oder mehrerer Netze voneinander dar. Das bedeuted, dass lediglich bestimmte Informationen zwischen den einzelnen Netzen ausgetauscht werden dürfen und können. Es sollten keine weiteren Verbindungen zwischen den Netzen bestehen, die eine Umgehung der Firewall ermöglichen. Die geforderten Funktionen werden in einer Firewall mit Hilfe verschiedener Techniken implementiert. Beispielsweise kann eine Filterung von Datenpaketen anhand bestimmter Merkmale im Header vorgenommen werden oder die Filterung erfolgt auf Applikationsebene. Die Paketfilterung nach Header-Merkmalen findet auf den Schichten 3 und 4 des ISO-OSI-Referenzmodells statt. Dabei erfolgt kein Zugriff auf die Applikationsdaten. Es besteht aber auch die Möglichkeit eine Filterung auf Applikationsebene (Schicht 7) vorzunehmen. Dies kann entweder mit Hilfe eines Circuit- oder eines Application-Level-Proxys geschehen. Der Proxy ist hierbei vergleichbar mit einem Man-in-the-Middle [1]. Soll von einem Client auf einen Server zugegriffen werden, so analysiert der Proxy den übertragenen Datenstrom und leitet nur solche Anfragen an den Server weiter, die zuvor als „erlaubt“ definiert wurden. Eine Firewall oder ein Proxy ist also in der Lage, die Kommunikation einzuschränken oder zu untersagen.

Die Arbeitsweise einer Firewall zeigt aber gleichzeitig auch ihre Grenzen auf. Hier kommt nun das IDS in Spiel. Da eine Firewall lediglich in der Lage ist den Datenverkehr zwischen zwei Netzen zu kontrollieren, können durch ihren Einsatz keine Angriffe verhindert werden, die von innerhalb des zu schützenden Netzes durchgeführt werden. Anders gesagt: Befindet sich der Angreifer bereits innerhalb des Teilnetzes mit dem zu schützenden System, so wird der Datenverkehr zwischen ihm und diesem System nicht mehr durch eine Firewall oder einen Proxy gefiltert. Der Angreifer könnte zum Beispiel ein Wartungstechniker sein, aber auch ein Mitar-

[1] Als Man-in-the-Middle bezeichnet man eine Einheit, die in einem Netzwerk zwischen zwei Kommunikationspartnern steht und dabei die komplette Kontrolle über den Datenverkehr der Kommunikationspartner besitzt. (vgl. [Ecke03], [Wiki, Stichwort „Man-in-the-Middle-Angriff“])

beiter. Missbrauch durch Mitarbeiter stellt Schätzungen zufolge im Unternehmensumfeld ein sehr großes Gefahrenpotential dar.[2] Ein weiteres Sicherheitsproblem, welches durch Firewalls oder Proxys nicht verhindert werden kann, ist die Ausnutzung von fehlerhaften Implementierungen in Software. Erlaubt eine Firewall beipielsweise einen Zugriff auf den Webserver und es taucht eine Sicherheitslücke in der auf dem Webserver eingesetzten Software auf, so besteht die Gefahr, dass dieser Angriff zugelassen wird.

In den Ausführungen von Gerloni et al. [Gerl04] findet sich noch ein weiterer wichtiger Aspekt, weshalb IDS sinnvolle Ergänzungen zu anderen Schutzmaßnahmen sind. Ein IDS ist in der Lage alle von ihm detektierten Vorfälle zu protokollieren. Die Protokollierung erscheint deshalb so wertvoll, weil viele Angriffe auf ein System ansonsten unentdeckt bleiben würden, da ein geübter Angreifer ansonsten so gut wie keine Spuren hinterlassen würde. Die Protokolldaten des IDS leisten hier einen wesentlichen Beitrag dazu, das Vorgehen bei Angriffen zu rekonstruieren und somit eine Wiederholung zu vermeiden. Im Idealfall sind sogar Rückschlüsse auf den Angreifer möglich um diesen eventuell rechtlich zu belangen.

Es gibt jedoch auch zahlreiche Fälle, in denen ein IDS tatsächlich helfen kann, Angriffe von vorneherein zu verhindern. Ein Beispiel hierzu ist ebenfalls bei Gerloni et al. [Gerl04] zu finden: Versucht der Angreifer durch version.bind-Abfragen herauszufinden, welche IP-Adressen und Bind-Version die Nameserver haben und erhält von diesen eine Antwort, so hat er die Möglichkeit, Rückschlüsse auf Schwachstellen der jeweiligen Version zu ziehen und diese auszunutzen. Ist die verwendete Version eventuell durch eine Buffer-Overflow-Attacke kompromittierbar, so kann der Angreifer diese Schwachstelle später nutzen, indem er eine speziell präparierte DNS-Anfrage abschickt, um gewisse Rechte auf dem Server zu erlangen. Die Bind-Abfrage und der Angriff können zeitlich völlig getrennt erfolgen. Bei Verwendung eines gut konfigurierten IDS wäre in dem geschilderten Szenario die Systemadministration des IDS auf den Bind-Scan aufmerksam geworden und hätte die Sicherheitslücke möglicherweise schon vor Ausführung des eigentlichen Angriffs schließen können.

Dies zeigt, dass ein IDS eine sinnvolle Ergänzung zum Einsatz von Firewalls und Proxys darstellt. Um die Sicherheit eines Netzwerks weiter zu erhöhen sollten aber noch weitere Vorkehrungen getroffen werden, die beim Management einer Sicherheitsinfrastruktur berücksichtigt werden müssen (z. B. Authentifizierungsmechanismen, organisatorische Maßnahmen in Form von Sicherheitsrichtlinien, bauliche Maßnahmen, etc.)

2.1.1 Typen von IDS

In der Regel werden IDS in zwei Gruppen eingeteilt, wobei sich diese Einteilung auf den Einsatzort bezieht, an welchem das System in ein Netzwerk integriert wird. Man unterscheidet die Host Intrusion Detection Systeme (HIDS) von den Network Intrusion Detection Systemen (NIDS).

[2] Hierüber lassen sich kaum verlässliche Daten finden, da die Unternehmen bestrebt sind Angaben gegenüber der Öffentlichkeit zu vermeiden, um ihrem Image nicht zu schaden. Dennoch wird die Annahme einer hohen Zahl von Angriffen durch Mitarbeiter in unterschiedlichen Studien verdeutlicht (vgl. [Utim98] zitiert bei [Ecke03])

Host Intrusion Detection Systeme

Als HIDS wird ein System bezeichnet, dessen Sensor, in Form eines Agenten, auf dem zu überwachenden Rechner zum Einsatz kommt. Deshalb findet man in der Literatur manchmal auch den Begriff „Rechnerbasierte IDS“. Der Agent stellt dabei die Informationsbeschaffungseinheit dar (vgl. Tabelle 2.1).

Mit Hilfe eines HIDS ist es möglich Daten, welche auf einem Rechner zur Verfügung stehen, zu analysieren und auf Veränderungen oder Sicherheitsverletzungen hin zu untersuchen. Die untersuchten Daten werden vom Betriebsystem oder von einer Anwendung erzeugt.

Die verwendeten Techniken zur Analyse werden später in Abschnitt 2.1.2 näher erläutert. In Anlehnung an Gerloni et al. [Gerl04] werden hier noch einige Stärken und Schwächen von HIDS erläutert.

HIDS geben ein mächtiges Werkzeug zur Datenanalyse an die Hand. Durch eine entsprechende Konfiguration der Logging-Mechanismen ist eine exakte Rekonstruktion dessen möglich, was ein Angreifer getan hat. Dafür müssen Sensoren aber auf allen zu überwachenden Systemen installiert werden. Da sich die HIDS auf Betriebssystem-eigene Logging-Mechanismen verlassen müssen, kann es sein, dass hier auf unterschiedlichen Systemen unterschiedliche Voraussetzungen zur Verfügung stehen. Da nur Ereignisse erfasst werden, die sich auf dem überwachten Host selbst abspielen, ist eine Überwachung ganzer Teilnetze nur schwer oder gar nicht möglich. Angriffe auf einen Router können beispielsweise nicht erkannt werden, wenn für diesen Router keine Logging-Mechanismen vorgesehen sind. Ganze Netzabschnitte lassen sich nur mit den nachfolgend betrachteten NIDS überwachen. Gegenüber den NIDS bieten die HIDS jedoch den Vorteil das auch eine Überwachung verschlüsselter Kommunikation möglich ist, da die Verschlüsselung auf dem Zielsystem endet. Eine der größten Gefahren stellen grundsätzlich Angriffe mit Root-Rechten dar, weil auf diese Weise eine Manipulation oder Deaktivierung des IDS selbst möglich wird. Ein geschickter Angreifer wird das IDS nicht ausschalten, sondern lediglich versuchen seine Spuren zu verwischen, damit sein Eindringen unbemerkt bleibt.

Network Intrusion Detection Systeme

Ein NIDS bezieht seine Daten, die analysiert werden sollen, nicht von einem einzelnen Rechner, sondern von einem oder mehreren Sensoren, die im Netz verteilt installiert werden. Dabei hören die Sensoren laufend den Netzverkehr ab („sniffen“). Um möglichst den gesamten Datenverkehr zu erfassen, sollten die abhörenden Sensoren möglichst günstig platziert werden. Da die geeignete Positionierung auch ein wichtiges Kriterium für die Effizienz eines IDS ist, wird darauf im Kapitel 3 nochmals näher eingegangen. Das „sniffen“ selbst kann auf zwei unterschiedliche Weisen geschehen.

- Portspiegelung:

  Für die Portspiegelung nutzt man die Tatsache, dass es sich bei den meisten Netzwerken heutzutage um geswitchte Netzwerke handelt. Man verwendet Switches, auf welchen sich Mirrorports (auch SPAN-Ports genannt) definieren lassen, die den gesamten, über

den Switch laufenden, Datenverkehr am Mirrorport spiegeln. Somit kann ein am Mirrorport angeschlossener Sensor den Netzverkehr mitlesen. Man könnte das Mithören an einem Hub als Spezialfall der Portspiegelung betrachten, da der Hub bauartbedingt die Spiegelung implizit vornimmt, indem er den Netzverkehr an alle Komponenten, die an ihn angeschlossen sind, verteilt. In der Praxis nimmt die Bedeutung von Hubs aber stetig ab.

Portspiegelung hat aber im wesentlichen zwei Nachteile. Zum einen ist es möglich, dass bei hoher Last Daten verlorengehen und somit Angriffe nicht mehr zuverlässig erkannt werden können. Dies könnte z. B. dann der Fall sein, wenn die Daten eines 16-Port-Switches mit einem maximalen Datendurchsatz von 100 MBit auf einen Gigabit-SPAN-Port gespiegelt würden. Zum anderen könnte ein Angriff auf den Switch selbst darauf abzielen, dass der Sensor keine oder nicht mehr alle Daten erhält.

- Ethernet Tap:

  Die Nachteile der Portspiegelung lassen sich bei der Verwendung von Ethernet Taps (Test Access Ports) vermeiden. Ein Ethernet Tap wird direkt in den Datenstrom eingehängt. Er verfügt über einen Eingang und zwei Ausgänge. Jedes eingehende Paket wird an beide Ausgänge weitergeleitet. Einer der beiden Ausgänge, der Tap-Ausgang, kann nur Daten empfangen. An diesem wird der Sensor angeschlossen.

  Ein Ethernet Tap ist eine passive Komponente und somit im Netzwerk völlig transparent. Selbst wenn die Stromversorgung des Taps ausfällt, wird der Datenstrom korrekt weitergeleitet. Mit Hilfe eines Zwischenpuffers wird, selbst bei extrem hoher Last, einem Datenverlust am Tap-Ausgang vorgebeugt.

Auch in diesem Abschnitt soll wie bei den HIDS in Anlehnung an Gerloni et al. [Gerl04] noch auf die Stärken und Schwächen eines NIDS eingegangen werden.

Da die Sensoren lediglich in das Netzwerk integriert werden und nicht in den überwachten Systemen selbst, ist keine Modifikation an diesen Systemen notwendig. Im Gegensatz zu den HIDS ist eine Überwachung kompletter Teilnetze möglich, da die Analyse nicht auf die an einem Host anfallenden Daten eingeschränkt ist. Durch den Einsatz mehrerer Sensoren besteht auch die Möglichkeit verteilte Angriffe zu erkennen. Ein Nachteil von NIDS besteht darin, dass keine Angriffe innerhalb verschlüsselter Verbindungen erkannt werden können. Bei der Wahl der Sensorstandorte muss darüber hinaus sehr sorgfältig vorgegangen werden, da nur Angriffe entdeckt werden können, die innerhalb des jeweils überwachten Netzsegments stattfinden. Netzsegmente mit hohem Datendurchsatz stellen zudem auch hohe Anforderungen an die CPU-Leistung von NIDS. Es muss sichergestellt werden, dass alle Datenpakete in Echtzeit analysiert werden können, da die Gefahr besteht, dass ein Eindringling versucht, das System selbst durch gezielte Überlastung anzugreifen.

2.1.2 Analysearten

Die von der Informationsbeschaffungseinheit gelieferten Daten müssen von der Auswertungseinheit (vgl. Tabelle 2.1) in geeigneter Weise nach Auffälligkeiten untersucht werden. Auffällig-

keiten sind Merkmale, die auf einen Angriff hindeuten. Dafür gibt es unterschiedliche Herangehensweisen.

1. Logfile-Analyse:

   Die Logfile-Analyse wird bei Spenneberg [Spen03] als die – zeitlich gesehen – am längsten bekannte Form der Intrusion Detection beschrieben. Dabei werden von der Anwendung oder vom Betriebssystem erzeugte Logfiles überwacht (z. B. /var/log/messages auf einem Unix-System). Wenn bestimmte zuvor festgelegte Ereignisse bei der Analyse der Logfiles erkannt werden, schlägt das System Alarm. Dazu werden entweder sogenannte Positiv-Listen oder Negativ-Listen definiert. Wenn eine Positiv-Liste verwendet wird, führen sämtliche mit ihr übereinstimmenden Meldungen zu einer Alarmierung. Die Wirkungsweise einer Negativ-Liste ist genau umgekehrt. Eine Alarmierung findet dann statt, wenn eine Meldung nicht mit dieser Liste übereinstimmt. Die Verwendung einer Negativ-Liste bietet den Vorteil, dass wichtige Meldungen nicht übersehen werden können, wie es passieren würde, wenn man einen entsprechenden Eintrag in einer Positiv-Liste vergessen hätte. Allerdings sind bei der Verwendung von Negativ-Listen die Anforderungen an den Logfile-Analysator höher, da die Meldungen weiter aufbereitet werden müssen, um dem Administrator das Lesen von hunderten oder tausenden Protokollzeilen zu ersparen. Die Meldungen sollten idealerweise automatisch zu übersichtlichen Berichten zusammengefasst werden.

2. Integritätstests:

   Integritätstests dienen dazu unerlaubte Änderungen am System zu erkennen. Dazu werden ausgewählte Dateien nach Installation und Konfiguration des Systems festgelegt und ständig auf ihre Integrität hin überwacht. Meist werden zur Überwachung der ausgewählten Dateien deren Prüfsummen (Hash-Werte) ermittelt und mit einem zuvor hinterlegten Muster verglichen. „MD5“ und „SHA-1“ sind beispielsweise bekannte Algorithmen zur Erstellung solcher Prüfsummen.

   Problematisch kann ein IDS auf Basis von Integritätstests in der Praxis dann sein, wenn berechtigte Änderungen an den spezifizierten Dateien vorgenommen werden sollen, da sich damit die Prüfsumme der Datei ändert und somit ein Alarm ausgelöst würde. Diese Tatsache muss also im realen Betrieb immer berücksichtigt werden.

   Meldungen einer Angriffserkennung auf Basis von Integritätstest erfolgen immer erst nach Durchführung einer unberechtigten Änderung. Aus diesem Grund eignet sich ein solches System nicht zur Präventiverkennung.

3. Echtzeitanalyse:

   Bei einer ständigen Überwachung von System- und Dateizugriffen spricht man von einer sogenannten Echtzeitanalyse. Diese sehr aufwendige Variante eines HIDS wird meist auf Betriebssystemebene realisiert. Man kann diese Technologie auch präventiv einsetzen, da das System bereits einen Alarm auslöst, wenn lediglich der Versuch eines unberechtigen Zugriffs erfolgt. Eine eventuelle Modifikation am System kann somit entweder durch das System selbst oder durch Einschreiten des Administrators verhindert werden (vgl [Spen03]).

4. Signaturbasierte Analyse:

   Bei der signaturbasierten Analyse kommt ein von Virenscannern bekanntes Prinzip zum Einsatz. Die Erkennungsmethode basiert auf der Erkenntnis, dass jedem Angriff bestimmte Charakteristika zugewiesen werden können. Diese Charakteristika dienen als Grundlage für die Anfertigung von Signaturen, die in einer Datenbank gespeichert werden.

   Zur Angriffserkennung wird der Datenstrom mit Hilfe dieser Signaturen überprüft. Hierbei werden Pattern-Matching-Algorithmen verwendet, um ihn mit den Einträgen in der Datenbank zu vergleichen.

   Die Methode der signaturbasierten Analyse kann als relativ zuverlässig angesehen werden, solange es sich um eine bekannte Angriffsart handelt. Zuverlässig bedeutet hier aber lediglich, dass die Zahl der Fehlalarme (False-Positive-Rate[3]) sehr gering ist. Wird nämlich auf ein System, welches ausschließlich signaturbasierte Analyseverfahren einsetzt, ein Angriff durchgeführt, zu dem keine Signatur existiert, so kann dieser nicht erkannt werden. Da immer wieder neue Angriffsmethoden entwickelt werden, ist die False-Negative-Rate[4] eines solchen Systems in der Regel sehr groß. Das heißt, viele tatsächliche Einbruchsversuche bleiben unerkannt (siehe auch [Feld05]).

   Wie bei Virenscannern ist die rasche Entwicklung neuer Signaturen immer ein Wettlauf gegen die Zeit, da die Signaturen immer erst nach Bekanntwerden eines neuen Angriffs entwickelt werden können. Darüber hinaus hängt die Qualität einer signaturbasierten Analyse auch entscheidend davon ab, wie gut die Analyseeinheit des IDS mit variierten Angriffen – also Angriffen, bei denen Angriffssequenzen untereinander vertauscht werden – zurechtkommt.

5. Anomalieanalyse, Statistische Analyse:

   Die Bezeichnungen „Anomalieanalyse“ und „Statistische Analyse“ werden in der Literatur häufig gleichbedeutend verwendet (z. B. bei Gerloni et al. [Gerl04]). Da die signaturbasierte Analyse lediglich die Erkennung einer vergleichsweise geringen Zahl von schon bekannten Angriffen ermöglicht, wird bei der statistischen Analyse versucht, abnormales Systemverhalten zu erkennen. Dazu muss das IDS erst einmal lernen welches Verhalten als „normal“ angesehen werden kann und somit rechtmäßig ist. Nach dieser Lernphase sollte das System dann in der Lage sein Abweichungen vom Normalen zu erkennen. Der Adminstrator hat hierbei die Möglichkeit mit Hilfe von Regelsätzen festzulegen, was als Abweichung angesehen werden soll.

   Es ist wichtig, dass die Daten, aus denen das Normalverhalten abgeleitet werden soll keine Anomalien enthalten. Ansonsten besteht die Gefahr, dass später ein auffälliges Verhalten nicht als Anomalie gedeutet werden kann (vgl. [Feld05]). Ein weiteres Problem bei dieser Methode der Angriffserkennung ist die Tatsache, dass ein tatsächlich abweichendes Verhalten im Netzwerkverkehr nicht immer einen Angriff als Ursache haben muss. Es kann sich um ein durchaus legitimes Verhalten handeln, das in der Lernphase nur noch nicht

[3] Alarm wird nicht ausgelöst, obwohl ein Angriff stattfindet
[4] Alarm wird ausgelöst obwohl kein Angriff vorliegt

aufgetreten ist. Für diesen Fall besteht die Möglichkeit, dem System diese Abweichungen in neuen „Lernrunden“ beizubringen. Man spricht dann von adaptiver Anomalieerkennung, andernfalls von statischer. Bei dem adaptiven Verfahren besteht aber wiederum die Gefahr, dass sich das ausgangs erlernte Normalverhalten nach und nach an Anomalien anpasst. Dies könnte ein Angreifer nutzen und das IDS langsam an seinen Angriff gewöhnen, bevor er ihn durchführt (vgl. [Feld05]).

Die Herausforderung besteht darin, die Grenzwerte, ab denen ein Verhalten nicht mehr als normal angesehen wird, möglichst exakt zu formulieren. Um den Administrationsaufwand zu minimieren sollten möglichst wenige Fehlalarme ausgelöst werden. Die False-Positive-Rate sollte also möglichst gering sein. Dies erweist sich bei der Umsetzung in die Praxis als nicht ganz einfach. Auf der anderen Seite kann man mit der statistischen Analyse aber die False-Negative-Rate, also unerkannt gebliebene Angriffe, im Vergleich zur signaturbasierten Analyse beträchtlich reduzieren.

6. Erkennung von Protokollfehlern:

   Um Protokollfehler zu erkennen wird überprüft, ob die empfangenen Datenpakete der Protokollspezifikation entsprechen.[5] Ein Datenpaket, welches dies nicht tut, kann auf einen Einbruchversuch hinweisen. Da die Umsetzung der Protokollspezifikation von verschiedenen Softwareanbietern oft auch nicht hundertprozentig eingehalten wird, ist dieses Analysevorgehen kritisch zu betrachten. Schon die Verwendung einer nicht korrekt implementierten Software kann zu Alarmmeldungen führen. Darüber hinaus existieren viele Angriffe, die nicht auf einer Schwachstelle in der Umsetzung der Protokollspezifikation beruhen und somit auch nicht erkannt werden können, da die Datenpakete die Spezifikation erfüllen.

In der Praxis werden häufig Systeme eingesetzt, welche mehrere Analysearten kombinieren. Bei NIDS, mit denen sich die Arbeit im Weiteren hauptsächlich beschäftigt, sind dies häufig Missbrauchs- und Anomalieerkennung. Darüber hinaus hängt die Effektivität und Effizienz eines NIDS aber auch wesentlich davon ab, wie es konfiguriert wird. Mit diesen, das Management betreffende, Fragen setzt sich Kapitel 3 auseinander.

2.2 Management

Ursprünglich wurde der Begriff Management aus dem lateinischen (von manum agere = „an der Hand führen“) abgeleitet und zu Beginn des 20. Jahrhunderts von Mary Parker Follet (* 1868; †1933) mit den Worten „Management ist die Kunst, mit anderen Leuten zusammen Dinge zu erledigen“ [Wiki, Stichwort „Mary Parker Follet“] definiert. Aus heutiger Sicht ist diese Definition aber nicht mehr ausreichend. Es muss der Tatsache Rechnung getragen werden, dass Management nicht mehr allein menschliches Miteinander-handeln beschreibt. Der Fortschritt in technologischer Hinsicht erfordert eine Definition, die auch den Einsatz moderner Informations- und Kommunikationsmittel umfasst. In der Wikipedia [Wiki, Stichwort „Management“] findet sich hierzu unter anderem folgende Definition: Management ist „die Gesamtheit der üblichen

[5] Protokollfehler werden manchmal auch als Protokollanomalie bezeichnet.

Tätigkeiten zur Führung oder Verwaltung von Organisationen“. Diese Definition erscheint hier sinnvoll, da sie allgemein genug gehalten ist, um alle weiteren Ausführungen zum Thema Management einzuschliessen.

Diese Arbeit beschäftigt sich mit dem Management von Intrusion Detection Systemen, insbesondere von NIDS (vgl. Abschnitt 2.1.1). Allgemeiner formuliert lassen sich NIDS als ein Speziallfall eines vernetzten IT-Systems darstellen. Aus diesem Grund sollen hier einige Grundlagen des Managements vernetzter IT-Systeme erläutert werden, die im weiteren Verlauf von Belang sind.

Der Begriff Management kann auf dem Hintergrund vernetzter Systeme nach Hegering, Abeck und Neumair [HAN99] enger abgegrenzt werden:

Definition 2.2 *„Das Management vernetzter Systeme umfaßt in seiner allgemeinsten Definition alle Maßnahmen, die einen effektiven und effizienten, an den Zielen des Unternehmens ausgerichteten Betrieb der Systeme und ihrer Ressourcen sicherstellen.“*

Effektivität bezeichnet dabei die Wahl der richtigen Mittel um diese Ziele zu erreichen. In der Betriebswirtschaftslehre wird Effektivität auch mit den Worten „to do the right things“ beschrieben. Als effizient wird der Einsatz dieser Mittel dann betrachtet, wenn mit Ihrer Hilfe das maximal mögliche Ergebnis erzielt wird („to do things right“).

Je nachdem mit welchen Objekten und Ressourcen sich das Management eines vernetzten IT-Systems beschäftigt, werden Netz-, System- oder Anwendungsmanagement unterschieden. Wie in Abbildung 2.1 zu sehen, bauen diese Formen des Managements in Ebenen aufeinander auf, wobei die unteren Ebenen die „Enabler“ für die oberen Schichten darstellen, diesen also die Mittel zum Erfolg zur Verfügung stellen sollen (vgl. [HAN99]). Rechnergestützte Lösungen in Form von Managenmentanwendungen sind meist lediglich auf den unteren Ebenen der Pyramide angesiedelt. Je besser die Managementanwendungen ihre Arbeit verrichten, desto größer wird auch der Erfolg sein, der an den oberen Enden der Pyramide „abgegriffen“ werden kann.

Rechnergestützte Managementlösungen sind im Umfeld vernetzter Systeme und verteilter Anwendungen aus heutiger Sicht unverzichtbar, um das Ziel eines effektiven und effizienten Managements zu erreichen. Eine Basis für rechnergestützte Lösungen wird in Form von Managementplattformen geschaffen. Eine Managementplattform ist ein Trägersystem für Managementanwendungen (vgl. [HAN99]).

Voraussetzung für den Entwurf von Managementplattformen in heterogener Umgebung sind sogenannte Managementarchitekturen. Diese werden in Übereinstimmung mit Hegering, Abeck, Neumair [HAN99] und Langer [Lang01] folgendermaßen definiert:

Definition 2.3 *Managementarchitekturen sind ein Rahmenwerk für managementrelevante Standards in Bezug auf folgende Aspekte, die mittels entsprechender Modelle in herstellerübergreifender Weise spezifiziert werden müssen:*

- *Beschreibung von Managementobjekten (Informationsmodell)*
- *Beschreibung von Organisationsaspekten, involvierten Rollen und deren Kooperationsformen (Organisationsmodell)*

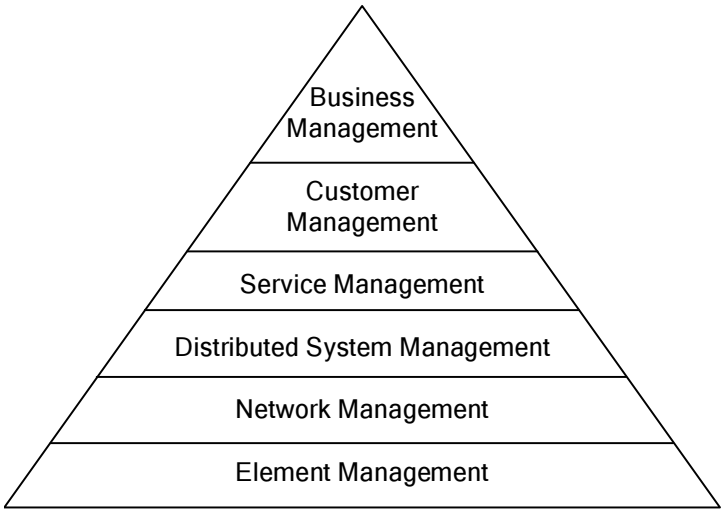


Abbildung 2.1: Managementpyramide [HAN99]

- *Beschreibung von Kommunikationsvorgängen (Kommunikationsmodell)*
- *Strukturierung der Managementfunktionalität (Funktionsmodell)*

In Abschnitt 2.2.1 werden die genannten Teilmodelle näher vorgestellt, bevor in Abschitt 2.2.2 eine Einführung in das IT Service Management (ITSM), welches von der IT Infrastructure Library (ITIL) unterstützt wird, erfolgt.

2.2.1 Teilmodelle einer Managementarchitektur

Wie gesagt setzen sich Managmentarchitekturen aus den oben genannten vier Teilmodellen – Informationsmodell, Organsisationsmodell, Kommunikationsmodell und Funktionsmodell – zusammen.

Es existieren verschiedene Standards für Architekturen, wobei die konzeptionelle Beschreibung der vier Teilmodelle im OSI-Management der ISO[6] bzw. ITU-T[7] am weitesten fortgeschritten ist. Das OSI-Management war die erste Architektur welche alle vier Teilmodelle beschrieben hat und kann damit als Referenzarchitektur angesehen werden. Darüber hinaus stellt es die Basis für das Telecommunications Management Network (TMN) dar und ist somit vor allem im Telekommunikationsumfeld verbreitet. Im Bereich der Datenkommunikation dagegen spielen andere Architekturen eine bedeutendere Rolle (vgl. [HAN99]).

Neben dem OSI-Modell existieren noch weitere Architekturstandards, wie z. B. der Internet-Managementarchitektur (nach dem Managementprotokoll auch als SNMP-Management be-

[6] International Organization for Standardization

[7] Die Telecommunication Standardization Bureau (ITU-T) ist innerhalb der International Telecommunication Union (ITU) für Fragen der Standardisierung bzw. der Verabschiedung von Empfehlungen zuständig.

zeichnet), der Common Object Request Broker Architecture (CORBA) oder dem Desktop Management Interface (DMI). Darüber hinaus gibt es auch Ansätze zum Web-basierten Management, die extra für die Nutzung von Web-Technologien ausgerichtet sind und viele mehr. Die Aufzählung soll hier lediglich einen Eindruck vermitteln, wie viele unterschiedliche Ansätze für Managementarchitekturen existieren. Sie haben aber alle gemeinsam, dass sie sich anhand der genannten Teilmodelle beschreiben lassen (vgl. [HAN99]).

Die vier Teilmodelle geben eine Systematik an die Hand, die es erleichtert, die zu managenden Aufgaben, Ressourcen, Organisationen und Tools überschaubar darzustellen. Abbildung 2.2 veranschaulicht den jeweiligen Aufgabenbereich der Teilmodelle. Die weitere Beschreibung der Teilmodelle erfolgt in Anlehnung an Hegering, Abeck und Neumair [HAN99]. Die Verwendung zusätzlicher Literaturquellen wird an entsprechender Stelle gesondert vermerkt.

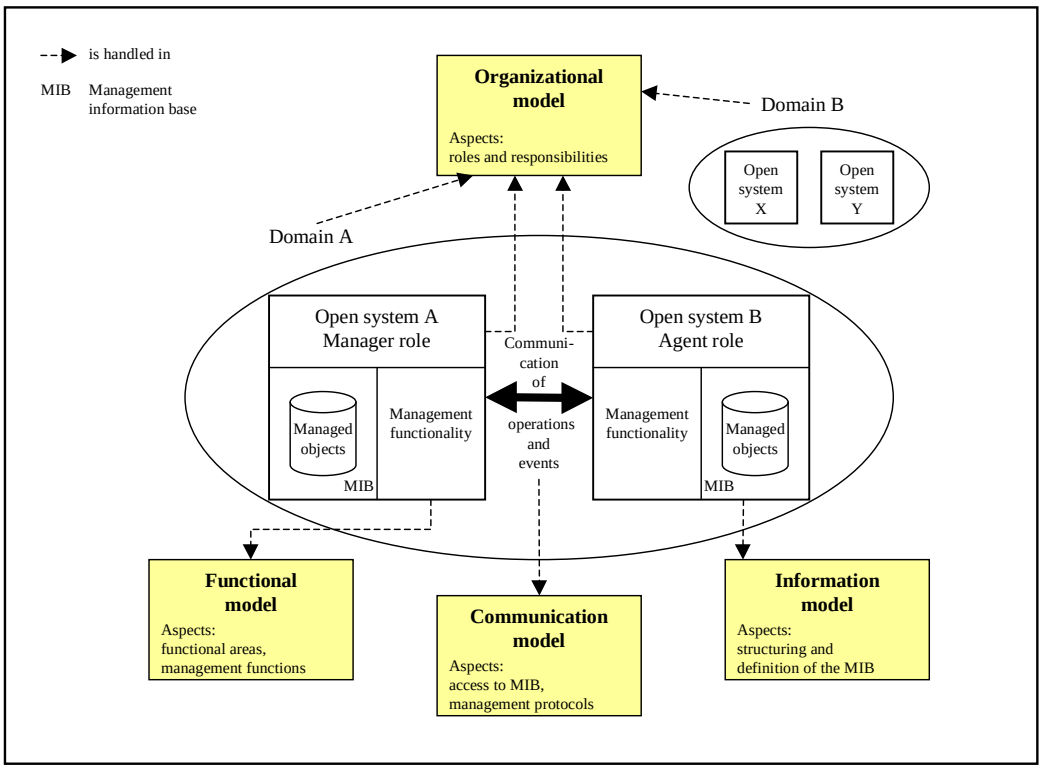


Abbildung 2.2: Teilmodelle einer Managementarchitektur [Krae03]

Informationsmodell

Das Informationsmodell kann als Herzstück jeder Managementarchitektur bezeichnet werden. Es führt die Idee von Managementobjekten (MOs) ein, indem es einen Beschreibungsrahmen für diese MOs spezifiziert (vgl. [HAN99]). MO sind die auf ihre für das Management relevanten Parameter reduzierten Modellierungen von Hard- und Softwareressourcen. Das heißt, es

findet eine Abstraktion der Charakteristika dieser Ressourcen statt [HAN99]. Managementrelevante Parameter wären zum Beispiel die Konfigurations- oder Tuningparameter von Switches oder Bridges, aber auch Managementfunktionen wie ‚Start' und ‚Stop' eines Fileservers. Das Informationsmodell dient dazu festzulegen, wie ein MO aus Sicht einer Managementarchitektur identifiziert, manipuliert, zusammengesetzt und angesprochen werden kann und regelt die Methoden zur Modellierung und Beschreibung [Lang01]. Nach Kraemer [Krae03] gehören damit zu einem Informationsmodell

- Objektidentifikation,
- Objektstruktur (Typen von Attributen),
- Objektverhalten (Semantik von Funktionen) und
- Objektrelationen zu anderen Objekten.

„Die Managementinformationsbasis kennzeichnet die von einem Manager bzw. von einem Agentensystem verwaltete Menge von Managementobjekten." ([HAN99] zitiert bei [Krae03])

In den verschiedenen Managementarchitekturen wurden unterschiedliche Modellierungsansätze (z. B. Entity Relationship, Datentypsatz, Objektorientierung) gewählt, um eine einheitliche Syntax zur Beschreibung von Managementinformationen festzulegen. Diese wird im Informationsmodell festgelegt. Im OSI-Management wurde ein objektorientierter Ansatz zugrundegelegt. Eine zu managende Ressource (MO), auf die ein Zugriff erfolgen soll, wird deshalb auch als Instanz einer Managementobjektklasse (MOC) bezeichnet, welche diese Ressource beschreibt (siehe han99).

Organisationsmodell

Das Organisationsmodell beschreibt den Teil einer Managementarchitektur, der die Akteure mit ihren Rollen festlegt sowie die Grundprinzipien ihrer Kooperation festlegt (siehe auch [Lang01]). Dabei wird eine flexible Anpassung an bestehende Aufbau- und Ablauforganisationen von Betreibern vernetzter Systeme gefordert. Die Managementarchitektur soll also nicht eine bestimmte Organisationsform vorgeben, sonder flexibel anpassbar sein. Bei der topologischen und funktionellen Anordnung existieren vielfältige Möglichkeiten, wie in Abbildung 2.3 leicht zu erkennen ist. Die Abbildung zeigt nur einige Beispiele und legt keinen Wert auf Vollständigkeit.

Kommunikationsmodell

Aufgabe des Kommunikationsmodells ist die Beschreibung der Kommunikationsvorgänge zum Austausch von Managementinformationen. Die zugrunde liegende Frage lautet: Wie wird der Informationsaustausch räumlich verteilter Ressourcen realisiert? Oder anders ausgedrückt: Wie werden die in den anderen drei Teilmodellen anfallenden Informationen untereinander ausgetauscht? Dabei werden die zur Kommunikation notwendigen Verbindungen zwischen den im Organisationsmodell definierten Rollen mittels Kommunikationsproktokollen beschrieben (vgl.

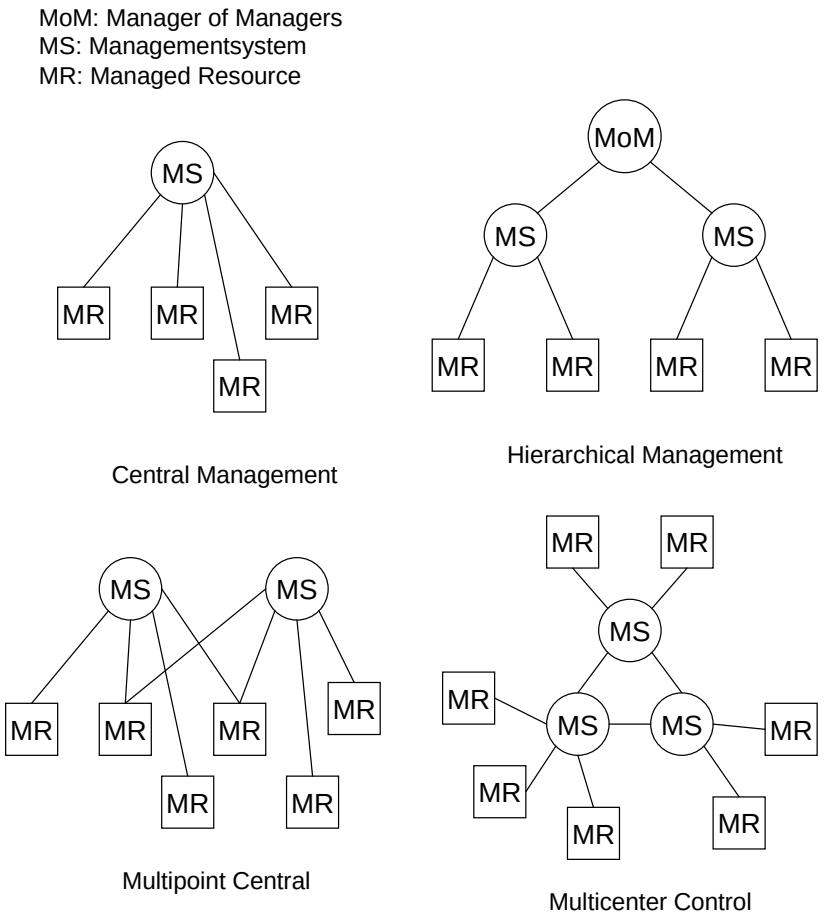


Abbildung 2.3: Anordnungsformen von Managementsystemen und überwachten Ressourcen [HAN99]

[Lang01]). Die Kommunikation geschieht dabei je nach Zielsetzung (vgl. auch [HAN99] und [Lang01]) durch

1. den Austausch von Steuerinformation, mit der auf eine Ressource bzw. auf das sie repräsentierende Objekt eingewirkt werden soll (Controlling). Die Initiative hat hierbei das Managementsystem.

2. Statusabfragen (Monitoring). Auch hier hat das Managementsystem die Initiative.

3. durch (asynchrone, spontane) Ereignismeldung. Die Initiative hat das gemanagte System.

Während die Initiative in den ersten beiden Fällen meist vom Manager ausgeht, geht sie bei Ereignismeldungen meist vom System aus, in dem die Ressource (das MO) liegt.

Das Kommunikationsmodell behandelt sowohl die Festlegung der kommunizierenden Partner, als auch der Kommunikationsmechanismen für die drei oben genannten Kommunikations-

zwecke. Darüber hinaus wird die Einbettung von Managementprotokollen in die Dienstarchitektur beziehungsweise Protokolhierarchie behandelt, nachdem zuvor Syntax und Semantik der Protokoll-Datenstrukturen festgelegt wurden.

Funktionsmodell

Im Funktionsmodell werden fünf Funktionsbereiche klassifiziert, die den Gesamtkomplex Management aufgliedern. Diese Funktionsbereiche werden im englischsprachigen Raum oft mit dem Akronym FCAPS bezeichnet, abgeleitet von ihren Anfangsbuchstaben. Es werden **F**ault, **C**onfiguration, **A**ccounting, **P**erformance und **S**ecurity Management (deutsch: Fehler-, Konfigurations-, Abbrechnungs-, Leistungs- und Sicherheitsmanagement) unterschieden. Diese Begriffswahl wurde dem OSI-Management entlehnt und wird heute oft verallgemeinert auch zur Beschreibung von Funktionsbereichen anderer Managementarchitekturen verwendet. In der Literatur werden darüber hinaus häufig weitere Bereiche beschrieben. Ein Lösungsansatz, bei dem eine weitere Untergliederung vorgenommen wird, ist zum Beispiel das in Abschnitt 2.2.2 vorgestellte IT Service Management. Die hier vorgestellten Funktionsbereiche finden sich aber auch in der dortigen prozessorientierten Strukturierung wieder. Die direkte Übertragung ist aber mit Vorsicht zu genießen, da das IT Service Management eine andere Sichtweise als Ansatzpunkt wählt. Mehr dazu in Abschnitt 2.2.2.

Auch die nachfolgende Beschreibung der Funktionsbereiche erfolgt in enger Anlehnung an Hegering, Abeck und Neumair [HAN99].

- Fehlermanagement (Fault Management):

  Fehlermanagement beschäftigt sich mit der Überwachung von Netz-, System- und Anwendungsverhalten. Darüber hinaus ist es eine wichtige Aufgabe die Verfügbarkeit eines verteilten Systems und seiner Dienste im Fehlerfalle zu gewährleisten beziehungsweise möglichst hoch zu halten. Einige Beispielaufgaben im Bereich des Fehlermanagements wären z. B. die Einleitung und Überprüfung von Fehlerbehebungsmaßnahmen, die Führung eines Trouble-Ticket-Systems oder auch die Hilfestellung bei Problemen für den Endanwender (Stichwort: User Help Desk).

- Konfigurationsmanagement (Configuration Management):

  Das Konfigurationsmanagement beschäftigt sich mit Fragen der Anpassung eines System an seine Betriebsumgebung. Beispielsweise Neuinstallation eines Systems, Neueinrichtung und Anpassung von Software, Änderungen der Netzwerktopologie oder der Einstellung von Systemparametern.

  Der Begriff Konfiguration kann dabei unterschiedlich verstanden werden. Die Bedeutung läßt sich aber im Allgemeinen aus dem verwendeten Kontext erschließen.

  - Unter Konfiguration kann die *Beschreibung* des Aufbaus eines verteilten Systems verstanden werden.
  - Es kann der *Vorgang* des Konfigurierens gemeint sein.

  - Und es kann mit dem Begriff Konfiguration das *Ergebnis* eines Konfigurationsvorgangs bezeichnet werden.

  Dem Konfigurationsmanagement wird in Kapitel 3 in Zusammenhang mit der ITIL noch einmal besondere Aufmerksamkeit zuteil.

- Abrechnungsmanagement (Accounting Management), Benutzerverwaltung:

  Zur Benutzerverwaltung gehört beispielsweise die Vergabe von Berechtigungen (Autorisierung) an Betriebsmitteln. Fallen durch das Anbieten verschiedener Dienste Kosten an, so ist es die Aufgabe des Abrechnungsmanagements diese Kosten den Verursachern zuzuordnen.

  Dieser Bereich des Managements ist für vorliegende Arbeit von nachrangiger Bedeutung.

- Leistungsmanagement (Performance Management):

  Wenn man will, kann man das Leistungsmanagement als eine Fortentwicklung des Fehlermanagements betrachten. Führt ein Fehler dazu, dass ein bestimmter Dienst nicht erbracht werden kann, so geht es beim Leistungsmanagement darum, Kriterien festzulegen, mit Hilfe derer festgestellt werden kann, wie gut ein Dienst erbracht werden kann. Diese Kriterien bezeichnet man als Dienstgüteparameter. Es gilt Leistungsengpässe zu vermeiden. Hierzu müssen ständig Messungen durchgeführt und ausgewertet werden. Die Dienstgüte ist ein wichtiger Faktor in der Beziehung zwischen Provider (Dienstleistungserbringer) und Kunden (Dienstleistungsempfänger).

  Das Leistungsmanagement stellt sicher, dass zwischen Kunden und Provider getroffene Dienstleistungsvereinbarungen (SLAs = Service Level Agreements) eingehalten werden.

- Sicherheitsmanagement (Security Management):

  Das Sicherheitsmanagement umfasst die gesamte Sicherheitspolitik einer vernetzten Umgebung. Es beschäftigt sich hingegen nicht mit der Sicherheit des Managements an sich. Hier muss eine klare Abgrenzung stattfinden. Die Sicherheit von vernetzten Systemen ist ein so komplexes Aufgabenfeld, dass man diesem Thema sicherlich eine eigene Arbeit widmen müsste. Hier wird darauf nicht näher eingegangen.[8]

Mithilfe der strukturierten Untergliederung in seine Funktionsbereiche wurde ein probates Mittel zur Überwachung und Steuerung vernetzter Systeme geschaffen. Die Funktionsbereiche führen dabei zu einer funktionalen Trennung der Aufgabeninhalte. Somit ist eine integrierte Managementlösung gut realisierbar, da alle Aspekte des Managements hinreichend gut erfasst werden (vgl. [HAN99]). Die Problematik dieses Ansatzes besteht jedoch darin, dass ein vernetztes System dabei lediglich aus der technischen Sicht betrachtet wird. Eine Untergliederung nach organisatorischen Gesichtspunkten findet praktisch nicht statt. Hier versucht das IT Service Management Abhilfe zu schaffen.

[8] Der Einsatz eines IDS ist natürlich Teil der Sicherheitspolitik eines Unternehmens. Hier geht es jedoch um die Frage, wie das Management eines solchen IDS auszusehen hat. Natürlich muss auch ein IDS adäquat gegen Angriffe geschützt werden, was in dieser Arbeit aber nicht von vorrangiger Bedeutung ist, da hierfür bewährte Strategien, die auch zum Schutz anderer Systeme (z. B. Datenbanken, Webserver, etc.) Anwendung finden, eingesetzt werden können.

2.2.2 IT Service Management

Das IT Service Management (ITSM) stellt streng genommen eigentlich keine Managementarchitektur dar, da der Begriff aus dem Gebiet des Systemmanagements stammt, in welchem eine technische Sichtweise im Vordergrund steht. Das Ziel, ein effektives und effizientes Management bei der Steuerung vernetzter Systeme zu gewährleisten, findet sich aber auch hier wieder. Der Unterschied besteht darin, dass das ITSM versucht einen Lösungsansatz für integriertes Management aus organisatorischer Sicht zu schaffen. Mit ITSM wird die Gesamtheit der Maßnahmen bezeichnet, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu ermöglichen ([Somm04] zitiert bei [Sage05]). Im Gegensatz zum Systemmanagement mit einer funktionalen Trennung der Aufgabeninhalte, schafft das ITSM eine wichtige Vorarbeit zur prozessorientierten Strukturierung von Betreiberorganisationen (vgl. [HAN99]). Das ITSM betrachtet die IT als Lieferant von Services oder Dienstleistungen[9]. Anwender- und Kundenzufriedenheit genießen oberste Priorität (vgl. [Elsa05]).

Die hierfür notwendige Strukturierung findet sich in der IT Infrastructure Library (ITIL) wieder. Die ITIL ist ein von der britischen Regierung in Auftrag gegebener Leitfaden, der von der Central Computer and Telecommunication Agency (CCTA)[10] Ende der Achtziger Jahre erarbeitet wurde. Er sollte dazu dienen, die Qualität von IT-Dienstleistungen zu verbessern und gleichzeitig die Kosten dafür zu reduzieren. Zum damaligen Zeitpunkt gab es noch keine umfassende Grundlage für die wirtschaftliche und zweckmäßige Erbringung von IT Services [itSMF]. Heute ist die ITIL nach eigener Aussage der de facto Standard für die Beschreibung des ITSM [Bitt05] und wird durch das IT Service Management Forum (itSMF) weiterentwickelt und gefördert. Sie stellt eine Sammlung von Best-Practice-Ansätzen dar, die in Zusammenarbeit mit Experten, Beratern und erfahrenen Berufsleuten entwickelt wurde. Ihre Veröffentlichungen können einzeln, aber auch gemeinsam als Empfehlung für die Gestaltung von Verfahrensregeln verwendet werden (siehe [ITSM00]). Die Veröffentlichungen der ITIL sind frei verfügbar.

Das ITIL Framework besteht aus mehreren Bänden, die themenspezifisch unterteilt sind. Einen Überblick gibt Abbildung 2.4. Für das Service Management wurden zehn ineinander greifende Kernprozesse zu den Bereichen Service Support und Service Delivery beschrieben. Diese können als das Herzstück der ITIL gesehen werden. Die Kernprozesse gliedern sich wie aus Tabelle 2.2 ersichtlich auf.

Der Inhalt der einzelnen Kernprozesse wird hier im Folgenden kurz beschrieben. Die Beschreibung erfolgt auf Grundlage der „Introduction to ITIL“ des OGC [OGC05], sowie dem Pocket Guide zur ITIL [ITSM00]. Andere verwendete Quellen werden an den entsprechenden Stellen gesondert benannt.

[9] Der englische Begriff Service und der deutsche Ausdruck Dienstleistungen werden in vorliegender Arbeit synonym verwendet

[10] Der Nachfolger der CCTA ist das Office of Government Commerce (OGC)

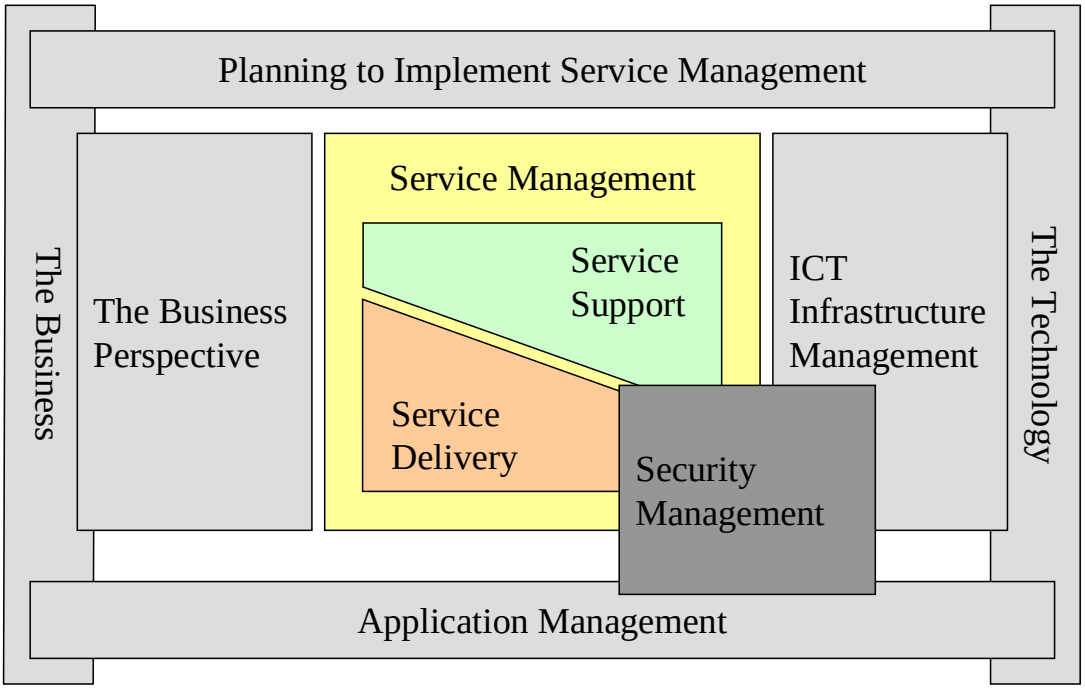


Abbildung 2.4: ITIL Publication Framework [OGC05]

Service Support	**Service Delivery**
Incident Management	Service Level Management
Problem Management	Financial Management for IT Services
Change Management	Capacity Management
Configuration Management	Availability Management
Release Management	IT Service Continuity Management

Tabelle 2.2: Kernfunktionen des ITSM (in Anlehnung an [ITSM00])

Service Support

Nach Victor und Günther [ViGu04] sollen die fünf Prozesse des Service Support sicherstellen, dass die Endanwender möglichst effizient mit den angebotenen Diensten arbeiten können. Sie spiegeln die tägliche Arbeit bei der Erbringung von Dienstleistungen wieder.

Das Zusammenspiel der fünf Prozesse lässt sich vereinfacht, wie in Abbildung 2.5 anhand des Deming-Cycles[11] dargestellt, beschreiben.[12]

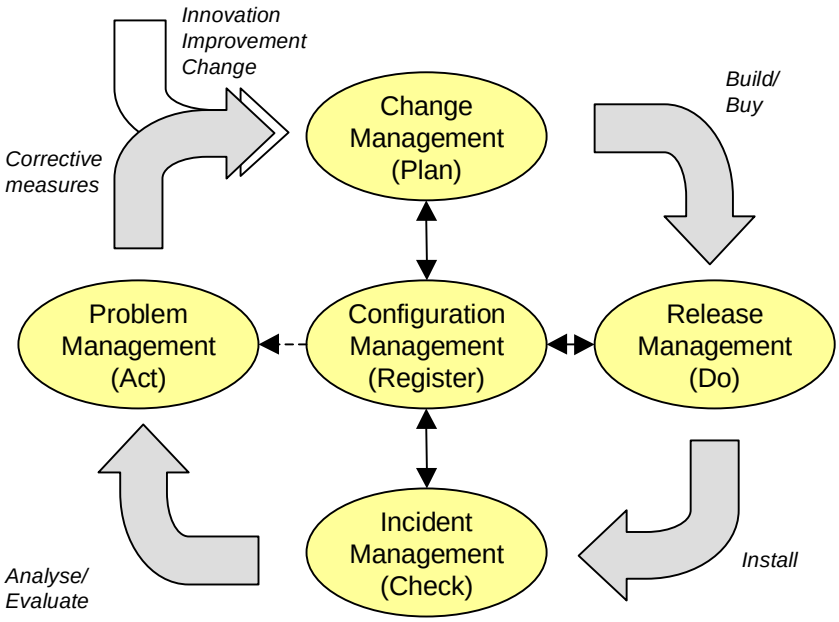


Abbildung 2.5: Service Support anhand des Deming-Cycles [OGC05]

- Incident Management

  Das Incident Management beschäftigt sich mit allen Anfragen, Kundenbedürfnissen oder Meldungen, die mit einer Einschränkung eines Dienstes zu tun haben und stellt somit einen integrierenden Bestandteil der kundenorientierten Serviceleistung dar. Es verfolgt das Ziel bei einer Störung (Incident) einen ausgefallenen Service so schnell wie möglich wieder verfügbar zu machen. Hierbei ist das Herausfinden der Ursache zweitrangig, auch eine Störungsumgehung wird als Lösung akzeptiert.Zur Unterstützung bei Störungsmel-

[11] Plan-Do-Check-Act (vgl. [Wiki, Stichwort „Qualitätsmanagementnorm“])

[12] Aus der Abbildung gehen nicht alle Schnittstellen zwischen den Prozessen untereinander hervor. Es existieren in Wahrheit Schnittstellen aller Prozesse untereinander.

dungen, wird das Incident Management häufig über einen Service Desk[13] gesteuert. Dieser beschreibt eine Kundenkontaktstelle (Initial point of contact), welche Anfragen kompetent und schnell beantwortet und Informationen für den Kunden bereitstellt.

- Problem Management

  Der Incident-Management-Prozess wird durch das Problem Management ergänzt. Da sich das Incident Management nur um die „Behandlung der Symptome“ kümmert, können unbekannte Ursachen aber immer wieder zu ähnlichen Störungen führen. Dies zu verhindern ist Aufgabe des Problem Managements. Ein Problem ist also eine unbekannte Ursache für eine mögliche Störung. Störungen und Probleme werden in der ITIL streng getrennt behandelt. Als Teil der Störungslenkung unterstützt das Problem Management den Service Desk bei der Analyse und Lösung schwieriger oder umfangreicher Störungen. Für Probleme deren Ursache ermittelt wurde (Known Errors) wird entschieden ob eine dauerhafte Behebung erarbeitet werden soll, um neue Störungen zu vermeiden. Der Vorschlag zur Behebung wird in Form eines RfC (Request for Change) an das Change Management weitergeleitet, welches für die Umsetzung verantwortlich ist. Erscheint eine dauerhafte Lösung aus geschäftlicher Sicht nicht gerechtfertigt und es existiert eine Umgehungslösung (Workaround) oder eine Altenative, bleibt die Klassifizierung des Problems als „Known Error“ bestehen.

- Change Management

  Aufgabe des Change Managements ist die Zustimmung und kontrollierte Implementierung von Änderungen an der IT-Infrastruktur. Die Durchführung von Änderungen ist eine alltägliche Anforderung beim Betrieb eines IT-Services. Änderungsanfragen werden als “Request for Change“ (RfC) bezeichnet. RfCs können sich beispielsweise aufgrund von Störungen oder Problemen (Incident oder Problem Management) ergeben.

  Einerseits soll durch den Change-Management-Prozess sichergestellt werden, dass die Durchführung einer Änderung mit minimalen Auswirkungen auf den laufenden Betrieb – und damit auf bestehende Services – erfolgt, andererseits sollen sich die Änderungen zurückverfolgen lassen. Dafür müssen die Änderungen entsprechend erfasst werden.

  Auf den Change-Management-Prozess wird in Kapitel 3.3.3 noch ausführlich eingegangen.

- Configuration Management

  Das Configuration Management hat die Aufgabe, Service Support und Service Delivery durch Bereitstellung eines detailierten Modells der IT-Infrastruktur zu unterstützen. Dafür wird das Modell in einer Configuration Management Database (CMDB) erfasst. Die CMDB erfasst die Meta-Daten aller servicerelevanten IT-Komponenten – auch als Configuration Items (CIs) bezeichnet – und deren Beziehungen untereinander. In Anlehnung an Jäger [Jaeg05] werden sie wie folgt definiert:

[13] Synonym werden in der Literatur auch die Begriffe Help Desk, Service Line oder First Level Support verwendet [ITSM00], wobei die Bezeichnung First Level Support genaugenommen irreführend ist, da dieser zwar Teil des Incident Managements ist und durch Mitarbeiter des Service Desks erledigt werden kann, aber nicht der Service Desk selbst ist.

Definition 2.4 *CIs sind die Betriebsmittel des Dienstleistungserbringers, welche für den Einsatz zugelassen sind. Über jedes Configuration Item müssen Angaben zu seiner Existenz und seinem aktuellen Zustand in der CMDB erfasst werden.*

Folgende Betriebsmittel fallen unter den Begriff des Configuration Items:

- *Computer, Hardwarekomponenten, andere IT-Geräte*
- *Software*
- *Dokumentation, Arbeitsanweisungen, Verträge*

Die CMDB – und damit das Configuration Management – ist, wie Abbildung 2.6 zeigt, eng mit den anderen Service Management Prozessen verknüpft.

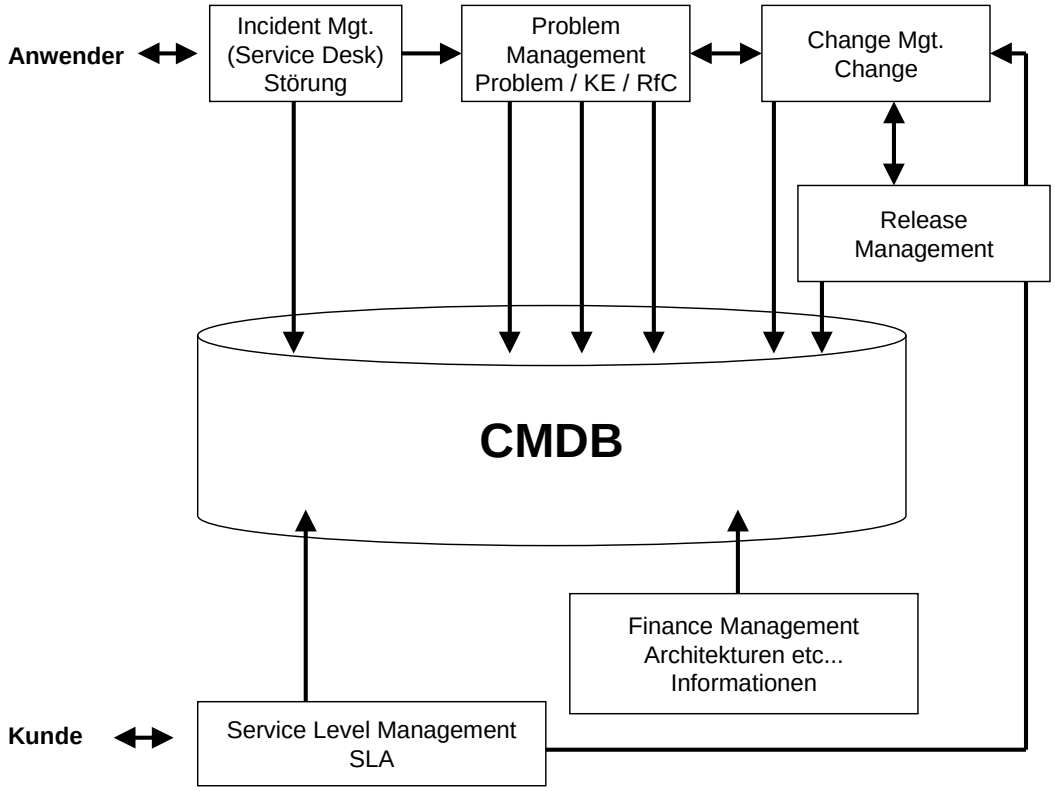


Abbildung 2.6: Die CMDB in Verbindung zu anderen Service Management Prozessen [ITSM00]

- Release Management

  Release Management – vormals auch als Software Control & Distribution bezeichnet – beschäftigt sich mit der koordinierten Einführung (Roll-Out) autorisierter Changes an IT-Services. Damit ist es dem Change Management beigeordnet. Es stellt die erforderliche Planung und Durchführung von Hardware- und Software-Installationen sicher. Zum

Schutz der produktiven Umgebung wird die Hardware beziehungsweise Software mithilfe formeller Verfahren und Checks vor der Einführung getestet. Die tatsächliche Einführung einer Änderung erfolgt oft durch das Release Management. Es bezieht sich darüber hinaus aber auch auf Änderungen an Installationsanweisungen, Dokumentationen und Benutzerhandbüchern.

Im Rahmen des Change Managements kann die Festlegung einer Release Strategie erfolgen. Es werden unterschieden:

Delta Release: Beinhaltet nur neue oder seit dem letzen Release veränderte Komponenten.

Package Release: Zusammenfassen mehrerer Änderungspakete. Dadurch Vergrößerung der Änderungsintervalle.

Notfall Release: Zur Lösung schwerer oder hoch priorisierter Probleme. Nur sparsamer Einsatz empfohlen, da der normale Release-Zyklus unterbrochen wird (Fehleranfälligkeit).

Service Delivery

Im Bereich Service Delivery werden nach Victor und Günther alle Prozesse zusammengefasst, die taktischer Natur sind. „Ziel dieser 5 Prozesse ist die Gewährleistung der Kontinuität und der Qualität der Dienstleistung zu vorab vereinbarten Kosten und Leistungen.“ [ViGu04]

- Service Level Management

  Aufgabe des Service Level Managements (SLM) ist es klare Vereinbarungen mit dem Kunden über den Typ und die Qualität von IT-Diensten zu schliessen und diese Vereinbarungen umzusetzen. Dabei wird eher versucht die Dienste nach den Anforderungen und Wünschen des Kunden auszurichten (demand pull), anstatt danach, was derzeit technisch umsetzbar ist (supply push).

  Eine der Hauptaufgaben des SLM besteht in der Aushandlung von Dienstleistungsvereinbarungen – in der ITIL als Service Level Agreements (SLA) bezeichnet – zwischen Dienstleistungserbringer (Provider) und Dienstleistungsempfänger (Kunde). Die Servicequalität gilt es zu überwachen und einzuhalten. Gegebenenfalls muss eine Anpassung erfolgen (vgl. auch [Sage05]).

- Financial Management for IT Services

  Dieser Prozess – früher unter dem Namen Cost Management bekannt – umfasst die Kostenermittlung und Leistungsverrechnung. Diese sind integrierende Bestandteile des IT Infrastructure Managements. Sie bilden die Grundlage um die tatsächlichen Kosten der erbrachten Dienstleistung zu ermittlen und somit diese Leistung transparent und nachvollziehbar zu berechnen. Außerdem fördern Sie das wirtschaftliche Denken und Handeln in den IT-Abteilungen.

Kostenermittlung ist die Feststellung, was die erbrachten Dienstleistungen kosten. Die Leistungsverrechnung ist die Weiterverrechnung der Kosten an den Kunden. Eine Leistungsverrechnung muss nicht zwangsläufig erfolgen, wenn sie aber erfolgt muss ihr immer eine Kostenermittlung vorausgehen.

- Capacity Management

  Wie der Name bereits vermuten lässt, beschäftigt sich das Capacity Management mit der Bereitstellung ausreichender Ressourcen (Kapazitäten). Das bedeutet, die Kundenanforderungen bezüglich Transaktionsvolumen, Durchlaufzeiten und Antwortzeiten müssen erfüllt werden (vgl. auch [Szak04]). Diese werden in SLAs (siehe oben: Service Level Management) vereinbart. Auf der einen Seite stellt das Capacity Management sicher, dass bei Änderung der Anforderungen die erforderlichen Kapazitäten (menschliche und technische Ressourcen) rechtzeitig und günstig zur Verfügung gestellt werden, andererseits sollen durch geschickte Auslastung der bestehenen Ressourcen Überkapazitäten vermieden werden.

- Availability Management

  Das Availability Management stellt sicher, dass aus den vorhandenen Ressourcen und Dienstleistungen ein maximaler Nutzen gezogen werden kann, um dadurch die Verfügbarkeit der mit dem Kunden vereinbarten Dienstleistungen zu gewährleisten. Hier werden die Hilfsmittel koordiniert, die benötigt werden, um Ausfälle möglichst schnell zu beheben. Dies kann zum Beispiel durch die Forderung von Monitoring oder Backups geschehen (vgl. [Sage05]). Das Availability Management ist verantwortlich für Zuverlässigkeit, Wartbarkeit und Servicefähigkeit.

- IT Service Continuity Management

  IT Service Continuity Management befasst sich mit der Ausarbeitung von Maßnahmen zur Weiterführung der Dienste, für den Fall, dass es zu einem Totalausfall des Systems oder dem Ausfall von Teilkomponenten kommt. Dies geschieht in Form eines Eventualfall-Plans. Das heißt, auch das IT Service Continuity Management beschäftigt sich, genau wie Availability Management, mit Fragen der Verfügbarkeit. Während aber im Availability Management Antworten auf die Frage „Was können wir jetzt tun?“ gesucht werden, sucht man hier Anworten auf die Frage „Was können wir tun, wenn...?“[14]. Der Eventualfall-Plan ist dem Change-Management unterstellt und wird regelmäßig auf seine Aktualität überprüft und getestet.

2.3 Das Landesamt für Statistik und Datenverarbeitung

Das im Rahmen dieser Arbeit vorgestellte Konzept zum Management eines IDS soll, wie schon in Kapitel 1.2 erwähnt, im Hinblick auf seine Anwendbarkeit prototypisch überprüft werden. Hierzu wird das generische Konzept in einer konkreten Ausprägung an die Bedürfnisse des Landesamtes für Statistik und Datenverarbeitung (LfStaD) angepasst. Dadurch ist es möglich

[14] Im deutschen Sprachgebrauch hat auch die Bezeichnung “Eventuallfall-Planung“ Einzug gehalten.

Rückschlüsse zu ziehen, inwieweit das Konzept praxistauglich ist. Das LfStaD und sein Aufgabenbereich werden hier kurz vorgestellt.

2.3.1 Aufgabenbereich des LfStaD

Das LfStaD ist Betreiber der zentralen Dienste des Bayerischen Behördennetzes (BYBN). Das bedeutet, es stellt den Internetzugang für alle bayerischen Behörden bereit und bietet darüber hinaus Netzdienste wie DNS und Email an. Außerdem regelt es den Betrieb von über 100 Hochleistungsservern.

Die Ausgangsbasis für das Netz wurde 1996 durch die bayerische Staatsregierung im Rahmen des Projekts „Bayern Online“ geschaffen. Aufgrund der immer größer werdenden Bedeutung von eGovernment – man denke hier an die schon eingeführte elektronische Steuererklärung (ELSTER) – kann davon ausgegangen werden, dass die Bedeutung des Bayerischen Behördennetzes in den nächsten Jahren weiter zunehmen wird. Dies betrifft insbesondere die Bereiche der staatlichen und kommunalen Verwaltung. Die Grundlage dafür wurde im Projekt „Bayern Online“ gelegt.

Eine der Herausforderungen für das Landesamt für Statistik und Datenverarbeitung besteht nun darin, innerhalb des Netzwerks ein ausreichendes Sicherheitsniveau zu gewährleisten. Neben Firewalls und VPN-Gateways soll ein IDS zum Einsatz kommen, welches in die bestehende Netzwerkstruktur des Landesamtes integriert wird.

2.3.2 Überblick über die Netzwerkstruktur

Als Netzbetreiber für das Behördennetz fungiert die British Telecom. Das Bayerische Behördennetz an sich ist unterteilt in verschieden Virtual Private Networks (VPNs), die wiederum verschiedenen Sicherheitsleveln unterliegen. Das Sicherheitsbedürfniss ergibt sich dabei aus dem Aufgabenbereich der Behörden die dem jeweiligen VPN angehören. Beispielsweise gelten für kritische Daten wie zum Beispiel Daten der Polizei strengere Zugriffsbeschränkungen als für die oftmals weniger sensiblen Daten einer kommunalen Behörde.

Die VPNs sind durch eine Firewall voneinander getrennt. Server auf die von den VPNs aus zugegriffen werden darf (z. B. Datenbankserver), befinden sich hinter der Firewall in einer demilitarisierten Zone (DMZ). Die VPNs bilden zusammen mit der Firewall und der demilitarisierten Zone den internen Bereich des Bayerischen Behördennetzes.

Zusätzlich besteht eine Anbindung an das Internet. Hierfür wird der interne Bereich durch eine zusätzliche Firewall mit einer eigenen demilitarisierten Zone geschützt. Diese zweite DMZ beherbergt jene Server, auf die auch aus dem Internet, also von außerhalb, zugegriffen werden darf. Dabei handelt es sich beispielsweise um Webserver. Den Servern in dieser zweiten DMZ wird vom LfStaD im Prinzip der gleiche Sicherheitslevel zugeordnet, wie dem Internet. Sie werden also im Gegensatz zu den Systemen im internen Bereich als nicht vertrauenswürdig eingestuft.

Dieser Aufbau wird in Abbildung 2.7 noch einmal verdeutlicht. Um Missverständnisse zu vermeiden, müssen die Begriffe „interner Bereich“ und „externer Bereich“ noch erläutert werden.

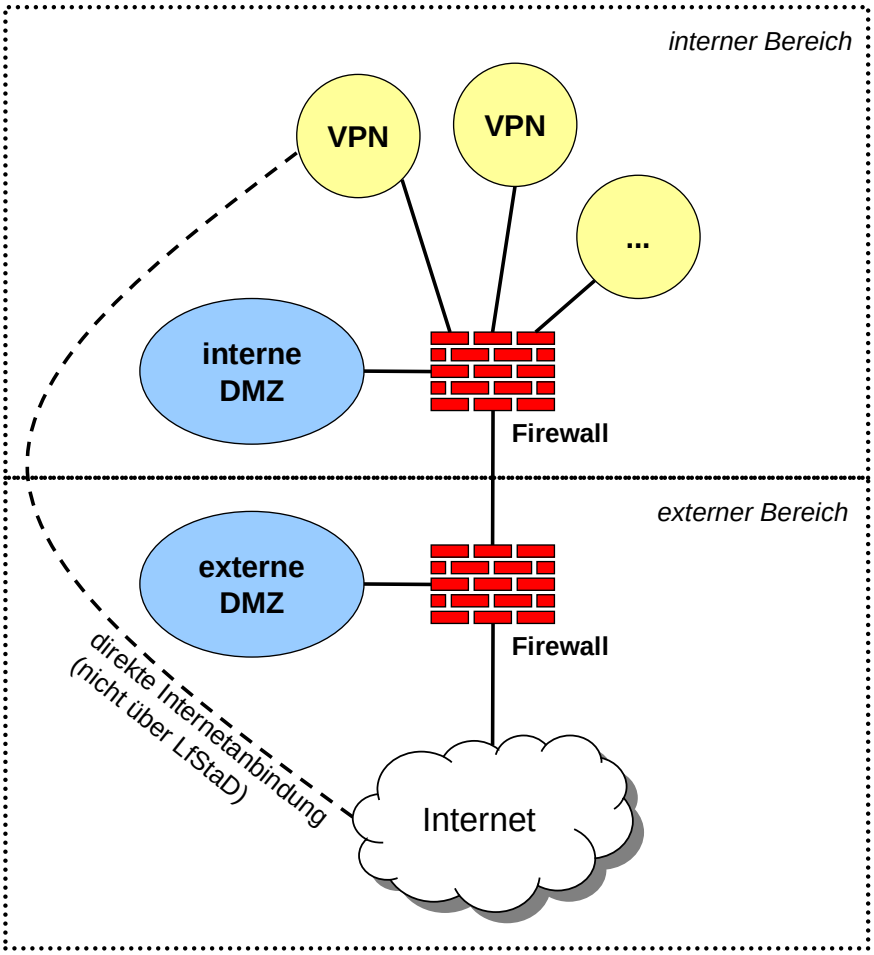


Abbildung 2.7: Schematischer Aufbau des Bayerischen Behördennetzes

„Intern“ bezieht sich auf den vom LfStaD als vertrauenswürdig eingestuften Bereich, während der nicht vertrauenswürdige Bereich als „extern“ eingestuft wird. Selbstverständlich ist die äußere Firewall und die dahinterliegende DMZ aber noch Teil des Bayerischen Behördennetzes. Außerdem muss noch erwähnt werden, dass einige VPNs mit einer eigenen Internetanbindung existieren. Diese Anbindungen unterliegen nicht der Kontrolle und Überwachung des LfStaD. Aus diesem Grund werden sie auch beim Einsatz des IDS nicht weiter berücksichtigt.

Um möglichen Systemausfällen vorzubeugen, existieren Backupleitungen und das gesamte Netzwerk ist weitgehend redundant ausgelegt. Zusätzlich wird die Netzlast immer auf mehrere Leitungen verteilt. Zusammen mit den verschiedenen Sicherheitsvorgaben der VPNs beziehungsweise der jeweiligen Behörden, und dem sehr großen Datenvolumen ergibt sich eine sehr komplexe Netzwerk-Infrastruktur. Die hier gezeigte Abbildung gibt also lediglich einen schematischen Überblick wieder.

2.3.3 Bedeutung des IDS-Managements im Bayerischen Behördennetz

Aufgrund der hohen Komplexität des Bayerischen Behördennetzes fällt dem effektiven und effizienten Management eines IDS hier eine besondere Rolle zu. Die Vorgaben, die eine solche Infrastruktur mit sich bringt, eignen sich gut, um zu überprüfen, inwieweit das in Kapitel 3 erarbeitete Managementkonzept universell einsetzbar ist und sich auf diese Anforderungen übertragen lässt.

Von großer Bedeutung ist es, die betrieblichen Strukturen des LfStaD zu berücksichtigen. Allein der Bereich, der sich mit IT im engeren oder weiteren Sinne beschäftigt, umfasst mehrere Abteilungen. Dies muss berücksichtigt werden, da aus dem Einsatz eines IDS zahlreiche Abhängigkeiten zu anderen Bereichen resultieren. Es ergeben sich Dienstleistungsbeziehungen zwischen dem IDS-Betreiber und dem Betreiber der überwachten Systeme. Eine klare Untergliederung der Aufgabenbereiche im LfStaD ist also notwendig. Die Aufgabenbereiche müssen verschiedenen Rollen zugeordnet werden. Damit wird eine Abstraktionsebene geschaffen, die die Umsetzung des Managementkonzepts erleichtert.

Das Managementkonzept soll sich in die organisatorischen Strukturen des Landesamtes integrieren lassen. Dabei kann davon profitiert werden, dass sich das LfStaD derzeit in einer Restrukturierungsphase befindet, in der die betrieblichen Abläufe im IT-Bereich nach und nach an die ITIL angepasst werden sollen. Dies hat den positiven Nebeneffekt, dass sich aus den hier gemachten Vorschlägen eventuell noch Erkenntnise für andere Bereiche gewinnen lassen.

3 Konzept zum Management eines netzbasierten IDS

In diesem Kapitel wird ein Konzept entwickelt, welches das Management netzwerkbasierter IDS auf generischer Ebene beschreibt. In diesem Zusammenhang bedeutet generisch, dass sich das Konzept möglichst einfach auf exitierende Lösungen von freien oder kommerziellen IDS-Produkten anwenden lassen soll. Hierfür wurde bereits in Kapitel 2.1 eine Abstraktion der Komponenten beschrieben.

Zuerst erfolgt in Abschnitt 3.1 die Beschreibung des Lebenszyklus eines IT-Systems, um den verschiedenen Phasen entsprechende Prozesse des ITSM zuordnen zu können. Abschnitt 3.2 diskutiert anschließend verschiedene Möglichkeiten, die Infrastruktur eines IDS zu gestalten, wobei darauf geachtet wird, den Bezug zum jeweiligen Einsatzzweck herzustellen. Im letzten Abschnitt dieses Kapitels (3.3) wird der Betrieb eines IDS anhand von Szenarien in die Prozessabläufe der ITIL eingegliedert, wobei die Prozesse des Service Support den Schwerpunkt bilden werden.

3.1 Lebenszyklus eines IDS

Als Grundlage für die weiteren Ausführungen wird hier eine Übertragung der zehn Kernprozesse der ITIL auf den Lebenszyklus eines IT-Systems vorgenommen. Dieser Lebenszyklus besitzt auch für IDS uneingeschränkte Gültigkeit.

Die Einordnung lässt sich wie in Abbildung 3.1 vornehmen. Das hier verwendete Prozessmodell stammt ursprünglich aus dem Microsoft Operations Framework (MOF). Das MOF ist zwar eigentlich eine Erweiterung und Anpassung der ITIL im Bezug auf Microsoft-Technologien, dennoch sind große Teile technologieunabhängig und können im Internet abgerufen werden [MSMOF]. Aus diesem Grund und da es eine sehr übersichtliche Einordnung bietet, wurde dieses Modell hier auch zur Darstellung der Prozesse im Lebenszyklus eines IT-Systems gewählt. Das Prozessmodell des MOF enthält neben einigen spezifischen Details alle Prozesse von Service Support und Service Delivery.

Im nachfolgenden Abschnitt werden die wichtigen Aspekte beim Aufbau einer IDS-Infrastruktur näher betrachtet. Im Vordergrund stehen die Besonderheiten, welche die Planung eines IDS mit sich bringt. Diese Thematik wäre im abgebildeten Prozessmodell (Abbildung 3.1) hauptsächlich dem Bereich des Infrastructure Engineering zuzuordnen.

Für den Betrieb eines IDS spielen aber besonders die Prozesse des Service Support eine wichtige Rolle. Entlang dieser Prozesse lassen sich verschiedene Szenarien angeben, die den Betriebsab-

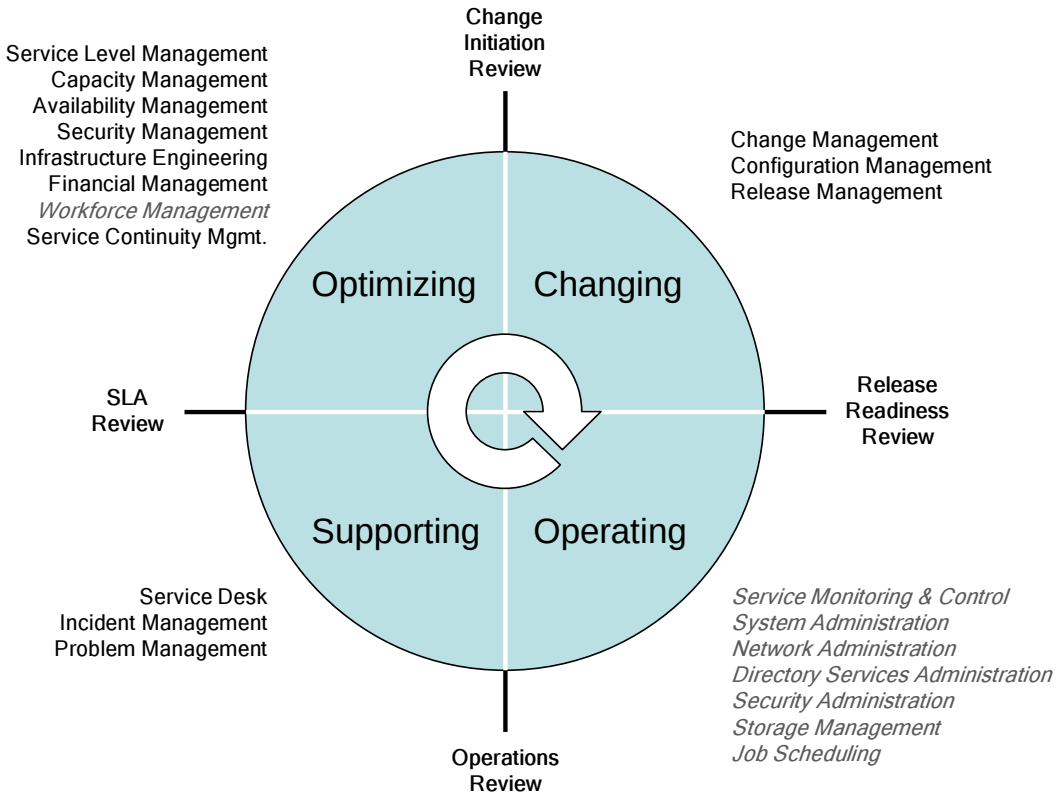


Abbildung 3.1: Prozessmodell nach MOF [Sage05]

lauf beschreiben. In Abschnitt 3.3 werden diejenigen Szenarien gesondert betrachtet, die für den Dienstleistungsaspekt von besonderer Bedeutung sind. Der Betreiber eines IDS übernimmt dabei die Rolle eines Dienstleistungserbringers. Die zu betrachtenden Szenarien spielen sich dabei zum einen im Bereich des Incident und Problem Management ab, zum anderen im Bereich des Change Managements und den damit eng verbunden Prozessen des Configuration und Release Managements. Hierbei ist zu beachten, dass im Falle von Alarmen durch das IDS Incident und Problem Management des Dienstleistungsempfängers betroffen sind, während sich Änderungsanforderungen – in Form von RfCs – in vorliegender Arbeit immer auf das IDS selbst beziehen. Die Unterscheidung dieser beiden Sichtweisen wird in Abschnitt 3.3.1 noch detailiert erläutert.

3.2 Infrastrukturaufbau eines IDS

Bei der Frage nach einem effizienten und effektiven Betrieb eines IDS stellt sich zuerst die Frage, welche Voraussetzungen dafür geschaffen werden müssen. Mit anderen Worten, es muss für den Betrieb zuallererst eine entsprechende Infrastruktur bereitgestellt werden. Dafür ist eine ge-

eignete Vernetzung der IDS-Komponenten selbst sowie eine strategisch geschickte Vorgehensweise bei der Anbindung an das zu überwachende Netzwerk notwendig. Kriterien, die hierbei hilfreich sind werden nachfolgend vorgestellt und erörtert.

3.2.1 Platzierung der Komponenten zur Informationsbeschaffung

Der Informationsbeschaffung gilt es beim Betrieb eines IDS besondere Aufmerksamkeit zu schenken. Von der Relevanz der erfassten Informationen hängt entscheidend die Effizienz des IDS ab. Auch wenn die Erkenntnis trivial klingen mag: Ohne oder mit schlechten Informationen sind keine sinnvollen Auswertungen möglich! Werden die Informationsbeschaffungseinheiten ungeschickt platziert, so kann es sein, dass bestimmte Angriffe von hoher Bedeutung unentdeckt bleiben. Andererseits kann auch der Fall eintreten, dass wichtige Meldungen nicht erfasst werden oder in einer großen Anzahl weniger wichtiger Alarme übersehen werden.

Hier sollen im Folgenden Richtlinien für die Platzierung der Informationsbeschaffungseinheiten diskutiert werden, die möglichst generisch gehalten sind, um die Anwendung in unterschiedlichen Umgebungen zu ermöglichen. Diese Verallgemeinerung ist aufgrund der vielen unterschiedlichen Ausprägungen von Netzwerken von Bedeutung. Als Grundlage der Diskussion werden zuerst die unterschiedlichen Ziele und Zwecke erörtert, zu denen ein IDS eingesetzt wird. Hieraus lassen sich anschließend unterschiedliche Vorgehensweisen zur Wahl der Standorte für die Informationsbeschaffungseinheiten ableiten.

Angemerkt sei noch, dass nachfolgend anstelle des Begriffs „Informationsbeschaffungseinheit“ der in der Literatur häufig anzutreffende Begriff „Sensor“ verwendet wird. Die Bezeichnungen lassen sich zwar nicht immer mit hundertprozentig identischer Bedeutung verwenden (siehe Kapitel 2.1), aber an dieser Stelle spielen die möglichen Unterschiede keine weitere Rolle.

Ziel und Zweck eines IDS

Ein IDS dient, wie der Name schon besagt, der Entdeckung von Angriffen. Diese Entdeckung kann unterschiedliche Zwecke verfolgen.

1. Durch das IDS sollen wichtige Systeme oder Komponenten einer IT-Infrastruktur überwacht werden. Ziel dabei ist es, diesen Systemen oder Komponenten einen zusätzlichen Schutz neben anderen Sicherheitsmaßnahmen zukommmen zu lassen. Der Schutz erfolgt dabei nicht durch das IDS selbst, sondern resultiert aus der Tatsache, dass nach erfolgreicher Identifizierung eines Angriffs entsprechende Gegenmaßnahmen ergriffen werden können.[1] Die Motivation für diese Gegenmaßnahmen kann unterschiedlicher Natur sein. Zum einen soll ein eventueller Schaden nach erfolgtem Angriff möglichst gering gehalten werden, zum anderen können Sicherheitslücken in der IT-Infrastruktur erkannt und behoben werden.

[1] Es existieren sogenannte Intrusion Response Systeme (IRS), die automatisch Abwehrmaßnahmen einleiten. Intrusion Response stellt eine Erweiterung von Intrusion Detection dar. Diese Arbeit beschäftigt sich aber lediglich mit Intrusion Detection.

2. Die Aufgabe eines IDS kann auch darin bestehen, möglichst alle Angriffsversuche und Angriffe, die gegen eine Netzwerk als Ganzes gerichtet werden, zu erkennen. Hierbei spielt der Schutzgedanke eine untergeordnete Rolle. Die Angriffserkennung dient lediglich dazu, sich durch statistische Auswertungen einen Gesamtüberblick über die Gefahrenlage zu verschaffen. So kann zum Beispiel die Häufigkeit von Angriffen auf bestimmte Systeme im Vergleich zu andern ermittelt werden oder Aussagen darüber getroffen werden, welche Arten von Angriffen besonders oft vorkommen. Daraus lassen sich wiederum Erkenntnisse gewinnen, welchen Schutzmaßnahmen für ein Netzwerk besondere Bedeutung zukommt.

Die eben beschriebenen Zwecke ergeben sich aus der Praxis. Der erste Punkt beschreibt eine Verwendung des IDS eher aus organisatorisch-betrieblicher Sicht, der zweite Punkt stellt eher die forschungstechnischen Ansätze in den Vordergrund. Je nachdem welche Organisation ein IDS betreibt, spielt der erste beziehungsweise der zweite Gesichtspunkt eine größere Rolle.

Diese Darstellung lässt sich am einfachsten an zwei Beispielen erläutern. Das LfStaD ist Betreiber mehrerer Hochsicherheitsanwendungen und möchte durch den Einsatz eines IDS die Sicherheit des Systems erhöhen. Aus betrieblicher Sicht stehen die schnelle Reaktion und die effektive und effiziente Administration im Vordergrund. Die Ziele orientieren sich also an den unter Punkt Eins genannten Gesichtspunkten. Im LfStaD ist aber auch das Bayern-CERT angesiedelt. Es ist als Sicherheits- und Computer-Notfallteam ein Teil des CERT-Verbunds. Der CERT-Verbund ist eine Allianz bestehend aus mehreren derartigen Teams (siehe auch [CERT]). Im Interesse des CERT-Verbunds steht in erster Linie, sich ein Bild der aktuellen Gefahrenlage zu verschaffen. Eine Reaktion auf die Angriffe erfolgt nicht, beziehungsweise nur in wirklichen Ausnahmefällen. In erster Linie dient der Einsatz eines IDS hier der Sicherheitsforschung.

Vorgehen bei der Sensorplatzierung

Als Grundlage und Beispielnetzwerk zur Diskussion möglicher Sensorplatzierungen wird hier der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene 3-stufige Internetübergang herangezogen (vgl. [BSI02a], Abbildung 3.2). Betont werden muss, dass die betrachtete Anordnung der verschiedenen Netzwerkkomponenten hier lediglich zur Veranschaulichung dienen soll. Die daraus gewonnenen Erkenntnisse sollen, wie erwähnt, generischen Charakter haben und sich somit auf andere Einsatzumgebungen ebenfalls umsetzten lassen. In Tabelle 3.1 ist aufgeführt für welchen Sensor welcher Verkehr sichtbar ist.

Aus Abbildung 3.2 lassen sich einige grundsätzliche Schlüsse ziehen:

- Die Wahrscheinlichkeit, dass die Einheit zur Informationsauswertung einen Angriff meldet, steigt, je weiter außen der Sensor platziert wird. Das heißt die Anzahl gemeldeter Angriffe nimmt nach innen hin ab. Die Begriffe „innen“ und „außen“ stehen hierbei in Zusammmenhang mit den anderen in einem Teilnetz auftretenden Schutzvorrichtungen. Hier wird von „weiter innen“ gesprochen, je mehr andere Schutzvorrichtungen sich zwischen Sensor und potentiellem Angreifer befinden. Zu beachten ist, dass der potentielle Angreifer sich auch im internen Netz befinden kann, welches dann im Vergleich zu einer DMZ als „außen“ betrachtet wird (vgl. Abbildung 3.2). Je weiter ein Sensor außen

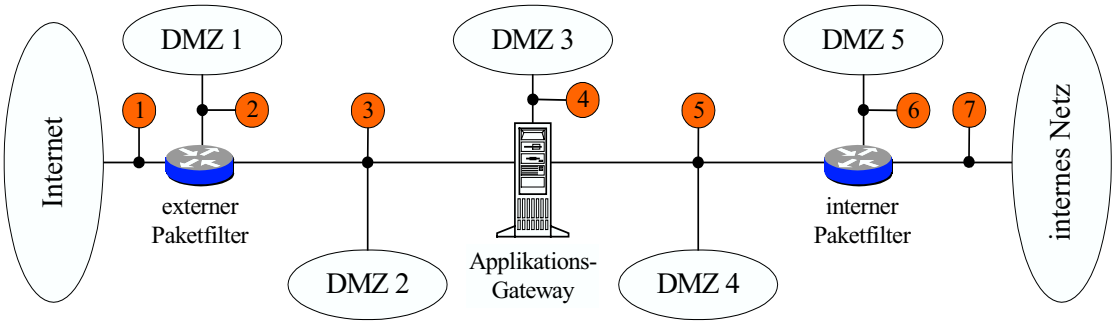


Abbildung 3.2: Möglichkeiten zur Sensorplatzierung am 3-stufigen Internetübergang [BSI02a]

platziert ist, desto weniger Angriffe werden durch zusätzliche Sicherheitseinrichtungen (Filter, Gateways, usw.) bereits geblockt, vorausgesetzt diese wurden richtig konfiguriert.

- Sensoren, die lediglich den Verkehr innerhalb einer DMZ – also hinter einer Firewall – erfassen, sind geeignet, einen ergänzenden Schutz von Systemen und Komponenten innerhalb dieser DMZ zu gewährleisten (z. B. Sensor 2, 4 und 6). Den Meldungen dieser Sensoren sollte grundsätzlich große Beachtung geschenkt werden, da sie bedeuten, dass bereits alle anderen Sicherheitsmaßnahmen versagt haben.
- Paarweise angeordnete Sensoren, die vor beziehungsweise hinter einer Firewall installiert sind, ermöglichen es, die Konfiguration der Firewall zu überwachen.

Unter Berücksichtigung der Einsatzzwecke (vgl. hierzu S. 36 im vorigen Abschnitt) können unterschieliche Vorgehensweisen für eine strukturierte Platzierung der Sensoren diskutiert werden. Vorgeschlagen wird hier ein stufenweises Vorgehen, d. h. der Aufbau des IDS erfolgt in mehreren Ausbaustufen. Dies hat aus Management-Gesichtspunkten den Vorteil, dass sich das Vorgehen zur Ermittlung geeigneter Sensorstandorte in Einzelschritte zerlegen läßt und ist auf der anderen Seite flexibel genug, bereits von Inbetriebnahme an oder später das gesamte Netz zu überwachen.

Das beschriebene Vorgehen legt als Einsatzzweck den im vorigen Abschnitt beschriebenen ersten Gesichtspunkt, nämlich die primäre Aufgabe der Intrusion Detection als zusätzliche Schutzfunktion, zugrunde (S. 36). Die Platzierung der Sensoren erfolgt dabei von innen nach außen. Im Anschluss an die Beschreibung werden die Vorteile und Einschränkungen eines solchen Vorgehens erläutert.

1. Weg:

1. Schritt Die im Netz zu überwachenden Systeme und Komponenten werden identifiziert und anschließend nach ihrer Schutzpriorität geordnet. Ein Sensor wird in dem Teilnetz installiert, welches das oder die höchstpriorisierten Systeme enthält.[2]

[2] Besonders in größeren Netzen werden sich die wichtigsten Systeme (z. B. Datenbankserver o. ä.) innerhalb von

Nr.	Position	Beobachtbarer Netzverkehr
1	Vor dem externen Paketfilter am Übergang zum Internet	Internet ↔ Netzverkehr
2	Zwischen externem Paketfilter und DMZ 1	Internet ↔ DMZ 1 DMZ 1 ↔ weiter innen platzierte Systeme
3	Am Knotenpunkt zur DMZ 2	externer Paketfilter ↔ DMZ 2 DMZ 2 ↔ Applikations-Gateway externer Paketfilter ↔ Applikations-Gateway
4	Zwischen Applikations-Gateway und DMZ 3	weiter außen platzierte Systeme ↔ DMZ 3 DMZ 3 ↔ weiter innen platzierte Systeme
5	Am Knotenpunkt zur DMZ 4	Applikations-Gateway ↔ DMZ 4 DMZ 4 ↔ interner Paketfilter Applikations-Gateway ↔ interner Paketfilter
6	Zwischen internem Paketfilter und DMZ 5	weiter außen platzierte Systeme ↔ DMZ 5 DMZ 5 ↔ internes Netz
7	Hinter dem internen Paketfilter am Übergang zum internen Netz	interner Paketfilter ↔ internes Netz

Tabelle 3.1: Beobachtbarer Netzverkehr [BSI02a]

2. Schritt Weitere Sensoren können in anderen Teilnetzen installiert werden, die Systeme oder Komponenten enthalten, deren Überwachung als relevant eingestuft wird.

Werden auf diese Weise alle wichtigen Systeme und Komponenten überwacht, kann das IDS in Betrieb gehen. Um die Wirksamkeit des IDS jedoch weiter zu verbessern, können jetzt weitere Sensoren installiert werden.

3. Schritt Wird das Teilnetz zusätzlich durch Firewall-Komponenten geschützt, so können weitere Sensoren vor der Firewall – also weiter außen – installiert werden, um deren Wirksamkeit zu überwachen. Das heißt, durch die Erkennung spezifischer Kommunikationsdienste, die von der Firewall eigentlich blockiert werden müssten, kann deren Konfiguration überwacht werden.

Es muss klar darauf hingewiesen werden, dass sich die beschriebene Vorgehensweise sehr stark an organisatorischen und betrieblichen Aspekten und Abläufen orientiert. Was heißt das konkret? Bei einem IDS, in dem die Sensorplatzierung nach vorstehendem Schema vorgenommen wird, steht die Effektivität und Effizienz im Vordergrund. Solange nicht die letzte Ausbaustufe – eine vollständige Überwachung des gesamten Netzes – erreicht ist, werden sicher nicht alle Angriffe erkannt. Indem Sensoren ausschließlich hinter anderen Schutzeinrichtungen, wie beispielsweise Firewalls, zum Einsatz kommen, bleiben alle Angriffsversuche verborgen, die bereits durch diese Schutzeinrichtung blockiert werden. Das bedeutet zwar, dass die anderen Schutzmaßnahmen greifen, und ein Angriff dadurch verhindert werden kann, es heißt aber auch, dass eventuelle Angriffsversuche gar nicht erfasst werden. Diese Nichterfassung kann absichtlich erfolgen, um den administrativen Aufwand zu reduzieren und die Anzahl an Alarmen zu

DMZs befinden

reduzieren. Wenn man sie aber in Kauf nimmt, muss man sich auch der beschriebenen Nachteile bewusst sein.

Für die Entdeckung von Angriffen aus forschungstechnischer Sicht erscheint diese Methode der Sensorplatzierung eher ungeeignet zu sein. Da, wie geschildert, in diesem Fall ein Gesamtüberblick über die Gefahrensituation erfolgen soll, ist hier eine Platzierung der Sensoren möglichst weit außen erwünscht. Die beschriebene Methode erfüllt diese Aufgabe zwar auch, aber lediglich, wenn das IDS voll ausgebaut wird. Aus strategischer Sicht ist für den Aufbau also ein stufenweiser Ausbau von außen nach innen sinnvoll.

2. Weg:

1. Schritt Die Sensoren werden an den Übergängen zum Internet, noch außerhalb eventueller Paketfilter installiert.

2. Schritt Zur Überprüfung der Schutzfunktion anderer Sicherheitskomponenten können weitere Sensoren weiter innen platziert werden.

Beide beschriebenen Wege zur Platzierung der Sensoren eines IDS kommen letztendlich zum gleichen Ziel, falls immer ein vollständiger Ausbau stattfindet, also wenn das gesamte Netzwerk und alle einzelnen Teilnetze überwacht werden. Da dies in der Praxis jedoch nicht immer der Fall ist, muss im Einzelfall entschieden werden, ob ein Ausbau von innen nach außen (1. Weg) oder ein Ausbau von außen nach innen (2. Weg) sinnvoller ist.

Wird ein Ausbau in mehreren Stufen vorgenommen, so ist darauf zu achten, dass sich bei der Platzierung neuer Sensoren möglicherweise Auswirkungen auf das bestehende System ergeben. Eventuell müssen die existierenden Korrelationen für Meldungen verschiedener Sensoren nach einem Ausbau neu angepasst werden. Dies hängt entscheidend von der jeweiligen Einsatzumgebung ab. Dadurch kann die Komplexität des Managements stark ansteigen.

Für den interessierten Leser sei noch erwähnt, dass die gewonnenen Erkenntnisse zur Thematik der Sensorplatzierung von denen im „Leitfaden zur Einführung von Intrusion Detection Systemen“ des BSI [BSI02a] in einigen Punkten abweichen, jedoch im Endeffekt zum gleichen Ergebnis führen. Die hier vorgestellten Verfahren für die Wahl geeigneter Standorte zur Sensorplatzierung bietet jedoch, bedingt durch ihren stufenweisen Aufbau, eine strukturiertere Vorgehensweise. Darüber hinaus tragen sie besser der Tatsache Rechnung, dass Angriffe vom internen Netz aus ebenfalls ein hohes Sicherheitsrisiko darstellen können. Die Studie des BSI stuft Datenverkehr aus dem internen Netz grundsätzlich als vertrauenwürdiger ein, als Datenverkehr von aussen. Diese Ansicht wird hier zumindest nicht grundsätzlich vertreten. Beispielsweise Angriffe, die mit böser Absicht durch Mitarbeiter eines Unternehmens durchgeführt werden, beherbergen ein erhebliches Risikopotential. Dieses wird noch durch das oftmals vorhandene Insiderwissen erhöht. Ein weiteres Risiko könnte auch durch Fremd- oder Wartungsfirmen ausgehen, die vorübergehenden Zugriff auf das interne Netz haben.

3.2.2 Platzierung der übrigen Komponenten eines IDS

Nachdem es gelungen ist, geeignete Standorte für die Sensorplatzierung zu identifizieren, muss nun entschieden werden, wie die übrigen Komponenten eines IDS angeordnet werden. Im Vordergrund steht hierbei bei den nachfolgenden Ausführungen die Sicherheit. Ein IDS soll dergestalt in eine bestehende IT-Infrastruktur integriert werden, dass durch seinen Betrieb nicht neue Sicherheitsrisiken für das Gesamtsystem entstehen. Aus diesem Grund ist eine eingehende Diskussion der verschiedenen Möglichkeiten zur Implementierung eines IDS notwendig.

Nach den Ausführungen im „BSI-Leitfaden für die Einführung von Intrusion-Detection-Systemen“ [BSI02a] können grundsätzlich drei verschiedene Möglichkeiten unterschieden werden, einen Informationsaustausch zwischen den Sensoren und den übrigen Komponenten sowie diesen Komponenten untereinander zu gewährleisten.

1. Die IDS-Komponenten nutzen das zu überwachende Netz für die Kommunikation untereinander. Dieser Fall ist in Abbildung 3.3 dargestellt.

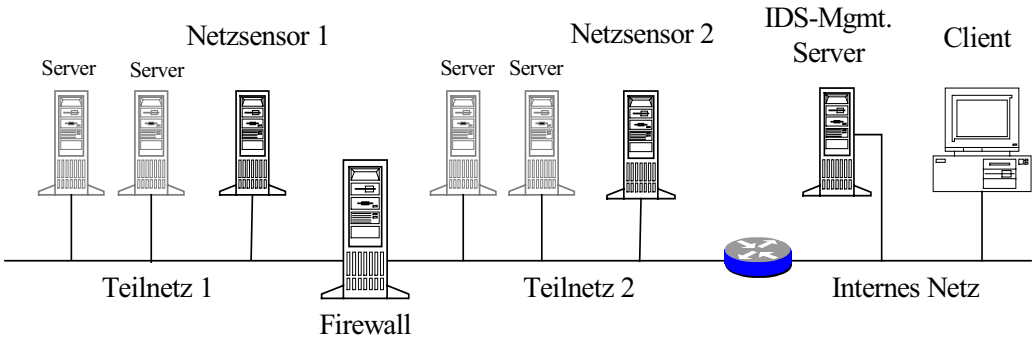


Abbildung 3.3: Kommunikation über das zu überwachende Netz [BSI02a]

2. Die IDS-Komponenten werden in einer eigenen DMZ betrieben. Sie werden damit durch eine Firewall vom zu überwachenden Netz getrennt. Abbildung 3.4 zeigt diesen Fall.

3. Die IDS-Komponenten werden in einem separaten Netz betrieben, welches zusätzlich zu dem zu überwachenden Netz aufgebaut wird. Diesen Fall zeigt Abbildung 3.5.

Unter dem Gesichtspunkt der Sicherheit lassen sich dem ersten Ansatz keinerlei Vorteile abgewinnen. Im Gegenteil! Durch die Integration der IDS-Komponenten in das zu überwachende Netz ergeben sich zusätzliche Sicherheitsrisiken. Es besteht die Gefahr durch falsch konfigurierte IDS-Komponenten Sicherheitslücken zu schaffen, die vorher nicht existiert haben. Darüber hinaus ist bei dieser Anordung das IDS selbst von eventuellen Angriffen bedroht. Eine eventuelle Manipulation am IDS kann zur Folge haben, dass man sich in einer trügerischen Sicherheit wiegt. Der erste Angriff auf das IDS kann dazu dienen, weitere Angriff auf das Betriebsnetz zu verschleiern, indem das IDS so manipuliert wird, dass es bestimmte Sicherheitsvorfälle nicht mehr meldet. Bis auf die Tatsache, dass eine derartige Implementierung einen sehr kostengünstigen Ansatz darstellt, ergeben sich keinerlei Vorteile gegenüber den anderen beiden Varianten.

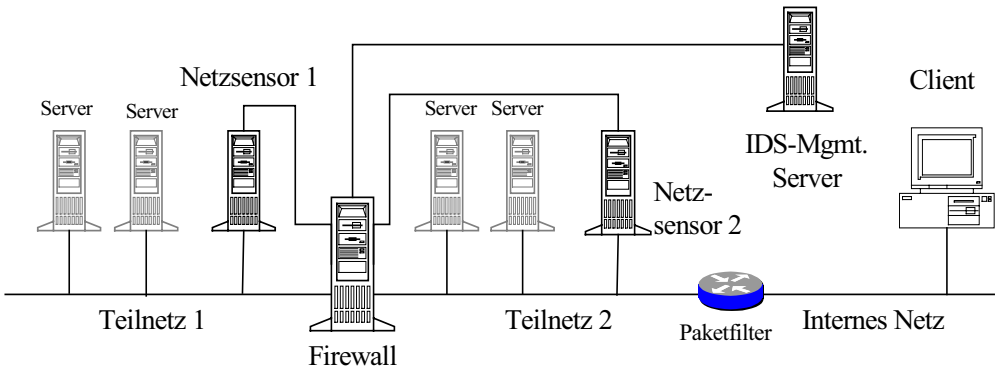


Abbildung 3.4: IDS-Komponenten in eigener DMZ [BSI02a]

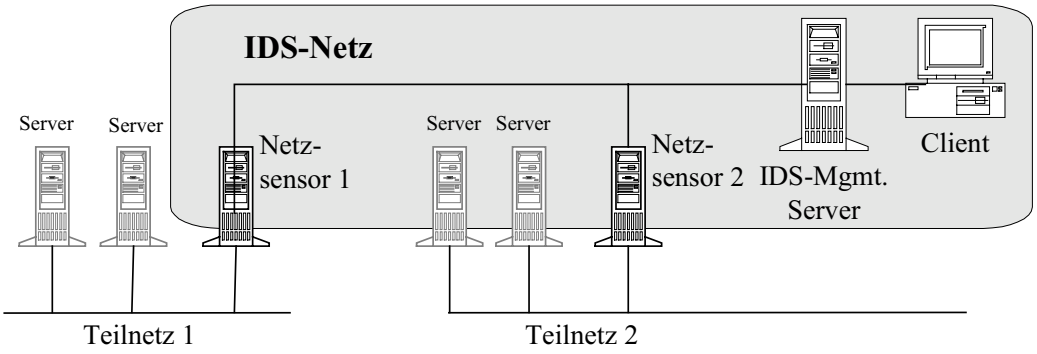


Abbildung 3.5: IDS-Komponenten im separaten Netz [BSI02a]

Es muss deshalb davon abgeraten werden, ein IDS direkt in das zu überwachende Netz zu integrieren.

Eine aus Sicht der Sicherheitspolitik bessere Lösung stellt die Platzierung der IDS-Komponenten in einer eigenen DMZ dar. Hierbei werden die erforderlichen Übergänge des Betriebsnetzes und des IDS-Netzes vollständig durch die Firewall überwacht. Somit lässt sich auch dem Problem vorbeugen, eventuelle versteckte Verbindungen der betrieblichen Teilnetze unter Umgehung der Firewall zu schaffen. Dieses Problem könnte nämlich entstehen, wenn der dritte Ansatz (eigenes IDS-Netz) zur Platzierung der IDS-Komponenten gewählt wird (vgl. hierzu Abbildung 3.6). Eine entsprechende Fehlkonfiguration der Netzsensoren 1 und 2 in der Abbildung würde dafür ausreichen. Die Einrichtung des IDS in einer eigenen DMZ ist mit relativ geringem Aufwand verbunden, da ein bereits vorhandenes Firewallsystem genutzt werden kann. Es muss lediglich entsprechend angepasst werden. Hieraus ergibt sich aber auch das größte Risiko, da bei dieser Anordnung die IDS-Kommunikation vollständig von der korrekten Konfiguration und Funktion der Firewall abhängig ist. Gelingt es einem Angreifer, die Firewall zu manipulieren, kann die korrekte Funktion des IDS nicht mehr gewährleistet werden.

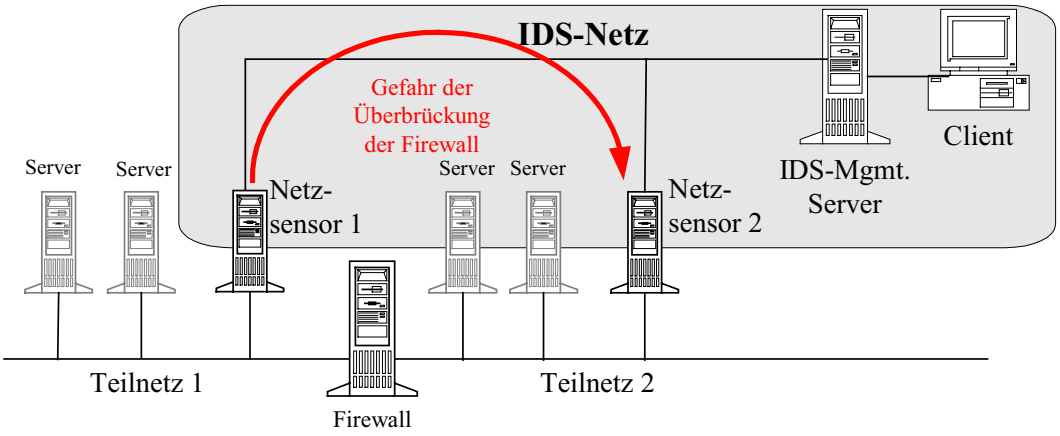


Abbildung 3.6: Umgehung der Firewall [BSI02a]

Genau an diesem Punkt liegen die Stärken des dritten Ansatzes – dem Aufbau eines separaten IDS-Netzes. Um das IDS selbst zu manipulieren muss es einem Angreifer gelingen in das separate Netz einzudringen. Demnach ist es notwendig, die Standorte, an denen die Sensoren installiert sind entsprechend zu schützen. Durch Verwendung von den bereits in Kapitel 2.1.1 vorgestellten Ethernet Taps existiert eine geeignete Lösung zur Anbindung der Sensoren an das Produktivnetz. Da der Tap selbst völlig transparent ist, wird er vom Angreifer nicht gesehen. Darüber hinaus löst der Tap das im vorigen Abschnitt (Abbildung 3.6) beschriebene Problem einer versteckten Verbindung. Er erlaubt nur ein Abhören des Netzverkehrs, kann aber nicht ins Produktivnetz senden. Eine Problemstelle bleiben weiterhin sämtliche Verbindungen vom Produktivnetz zum IDS-Netz, die nebenher noch existieren. Das sind zum Beispiele sämtliche Kommunikationswege zur Management- und Auswertungseinheit, die notwendig sind, um beispielsweise Alarme per E-Mail zu melden. Diese Übergänge müssen mit Hilfe einer eigenen Firewall abgesichert werden. Im Gegensatz zum Betrieb eines IDS in einer eigenen DMZ hat eine Fehlkonfiguration dieser Firewall jedoch keine Auswirkungen auf das Produktivnetz. Theoretisch bestünde auch die Möglichkeit keinerlei Übergänge zu einem anderen Netz zu schaffen. Diese Lösung ist aber in der Praxis nicht praktikabel, da dann weder Alarme geeignet gemeldet werden können, noch ist ein Signaturupdate über das Netz möglich. Alle Updates müssten per Hand eingespielt werden. Das gesamte Management könnte darüber hinaus nur von einer Station aus durchgeführt werden, die sich innerhalb des IDS-Netzes befindet.

Unter Berücksichtigung aller diskutierten Aspekte kann der Schluß gezogen werden, dass – zumindest unter dem Aspekt der Sicherheit – der Aufbau eines eigenen IDS-Netzes die geeignetste Lösung für die Platzierung der IDS-Komponenten ist. Aus den geschilderten Gründen empfiehlt sich dabei unbedingt der Einsatz von Ethernet Taps zur Anbindung der Sensoren sowie einer eigenen Firewall zur Überwachung der Netzübergänge.

3.2.3 Kalibrierung der Sensoren

Nachdem mit der Platzierung aller IDS-Komponenten die Infrastruktur des Systems weitestgehend festgelegt wurde – von der späteren Integration weiterer Sensoren einmal abgesehen – muss man sich nun Gedanken über die Kalibrierung der Sensoren machen.

Vorweg gilt es zu klären, was unter der Überschrift „Kalibrierung des Sensoren“ überhaupt zu verstehen ist. Oftmals wird in der Literatur, so auch vom Bundesamt für Sicherheit in der Informationstechnik [BSI02a], in diesem Zusammenhang davon gesprochen für jeden Sensor festzulegen, was dieser erkennen soll. Nach der strikten Trennung von Informationsbeschaffung und Informationsauswertung, die in Kapitel 2.1 in Tabelle 2.1 vorgenommen wurde, ist diese Auslegung jedoch höchst missverständlich, da die Aufgabe eines Sensors lediglich in der Beschaffung der Daten für die Auswertung liegt[3]. Deshalb erfolgt hier eine stringente Definition.

Definition 3.1 *Die Kalibrierung der Sensoren bezeichnet den Vorgang, in welchem festgelegt wird, auf welche Daten, die von einer Informationsbeschaffungseinheit gesendet werden, die Informationsauswertungseinheit in welcher Weise reagieren soll.*

Bei der signaturbasierten Analyse wird für die übermittelten Daten jedes Sensors individuell festgelegt, auf welche Meldungen die Auswertungseinheit für Daten dieses Sensors reagieren soll. Vereinfacht ausgedrückt bedeutet das nichts anderes, als festzulegen, welche Signaturen für den Sensor berücksichtigt werden sollen.

Für die Festlegung der Signaturen auf die ein IDS reagieren soll, existieren in der Fachwelt zwei gänzlich unterschiedliche Ansätze. Diese sollen hier diskutiert werden.

1. Je nachdem in welcher Umgebung ein Sensor betrieben wird, werden bei der Auswertung seiner Daten nur Signaturen berücksichtigt, die für die jeweilige Umgebung von Belang sind. Beispielsweise kann dies bedeuten, dass für einen Sensor, in einem Teilnetz mit ausschließlich Unix-Systemen, alle windows-spezifischen Signaturen deaktiviert werden. Auf gleiche Weise werden auch Signaturen für einen Microsoft Internet Information Server nicht berücksichtigt bleiben, wenn ausschließlich Apache Webserver eingesetzt werden. Dabei wird das System, ausgehend von einer Basiskalibrierung, durch Verfeinerung dieser Kalibrierung immer weiter an seine Einsatzumgebung angepasst. Bei diesem Vorgehen ist auch vorgesehen, festzulegen, wie auf ein Ereigniss reagiert werden soll (Alarmierung, Protokollierung, . . .). Es wird im Leitfaden des BSI näher beschrieben [BSI02a] und auch von Seiten einiger Anbieter von Intrusion Detection Systemen empfohlen (z. B. von der GeNUA mbH [GeNUA]).

2. Ein weiter Ansatz besteht darin, eine Überwachung der Sensoren mit allen für das IDS zur Verfügung stehenden Signaturen vorzunehmen. Es spielt dabei keine Rolle, ob die Signatur für das zu überwachende System von Relevanz ist oder nicht. Sobald neue Signaturen verfügbar sind, wird das System aktualisiert. Ein solches Vorgehen wird beispielsweise bei Gerloni et al. [Gerl04] beschrieben.

[3] Auch hier noch einmal der Hinweis, dass in der Praxis auch Sensoren existieren, die bereits eine Auswertungseinheit integriert haben

Es stellt sich nun die Frage, welcher dieser beiden Ansätze der bessere ist. Wie schon zuvor auf Seite 37 bei der Platzierung der Sensoren beschrieben, lassen sich auch diese beiden Ansätze auf die unterschiedlichen Einsatzzwecke zurückführen. Im betrieblichen Umfeld findet sich häufig eine Lösung, die sich am ersten Punkt orientiert, während im Forschungsumfeld die zweite Lösung häufig zu finden ist.

Dabei birgt die erste Lösung aber eine große Gefahr! Durch das absichtliche Deaktivieren bestimmter Signaturen, kann es vorkommen, dass mögliche Angriffsversuche auf eine bestehende IT-Infrastruktur nicht erkannt werden. Das wäre der Fall, wenn ein potentieller Angreifer über keine detailierten Kenntnisse des angegriffenen Netzes verfügt und möglicherweise auch Angriffsvarianten ausprobiert, die keine Aussicht auf Erfolg haben können. Dies ist der Fall, wenn der Angriff sich – aus Unkenntnis – gegen ein System richtet, welches in dem jeweiligen Netz gar nicht vorkommt. Sind beispielsweise die Signaturen für den IIS deaktiviert, weil lediglich Apache Webserver eingesetzt werden, so wird ein Angriffsversuch gegen einen von dem Eindringling vermuteten Internet Information Server (IIS) nicht registriert. Dies kann zu einem ernsthaften Sicherheitsproblem werden, da die Tatsache, dass ein Angriff nicht erkannt wird, eben nicht gleichbedeutent damit ist, dass er nicht stattfindet. Soll ein System gezielt kompromittiert werden, so wird es nicht bei diesem einen Versuch bleiben, sodass ein frühzeitiges Erkennen durchaus wünschenswert wäre. Außerdem besteht die Gefahr, versehentlich Signaturen zu deaktivieren, die durchaus relevant gewesen wären. Aus diesem Grund wird von einem derartigen Vorgehen bei der Sensorkalibrierung dringend abgeraten.

Warum dennoch häufig eine gezielten Deaktivierung vermeintlich „irrelevanter“ Signaturen vorgenommen wird dürfte vermutlich zwei Gründe haben. Zum einen wird dieses Vorgehen zum Teil von namhaften Entwicklern von IDS empfohlen, zum anderen erscheint diese Lösung gerade im organisatorischen und betrieblichen Umfeld aus Gründen der Effizienz sehr geeignet, da bei weniger aktiven Signaturen auch die Menge der Alarmmeldungen abnimmt, und somit eine leichtere Verwaltung möglich ist.

Für diese Arbeit ergibt sich aber aus den vorgenommenen Betrachtungen der Schluss, dass eine Kalbibrierung der Sensoren nach dem zweiten geschilderten Verfahren vorzunehmen ist, da nur so eine größtmöglicher Gewinn an zusätzlicher Sicherheit durch ein IDS gewährleistet ist. Ist aus betrieblichen Gründen dennoch eine Reduzierung möglicher IDS-Meldungen wünschenswert, so kann dies durch eine entsprechende Anordnung der Sensoren erreicht werden, wie bereits auf Seite 37 beschrieben wurde. Durch eine Platzierung der Sensoren möglichst weit innen, verringert sich die Anzahl von Meldungen, ohne dass das System nachhaltig eingeschränkt wäre, da ein weiterer Ausbau jederzeit vorgenommen werden kann. Eine Möglichkeit die betrieblich Effizienz eines IDS weiter zu steigern besteht darin, verschiedene Meldungen miteinander zu korrelieren. Das bedeutet, dass erst eine definierte Folge mehrerer Meldungen zum Auslösen eines Alarms führt. Die Festlegung von Korrelationskriterien ist aber in hohem Maße von der Umgebung abhängig in der das IDS zum Einsatz kommt, weshalb kaum allgemeingültige Aussagen zu einem möglichen Vorgehen gemacht werden können. Die Korrelationen müssen immer im Kontext ihrer Umgebung festgelegt werden. Darüber hinaus kann man für bestimmte Meldungen auch lediglich die Protokollierung vorsehen, ohne dass ein Alarm ausgelöst wird. Wenn das IDS aber zum zusätzlichen Schutz einer IT-Infrastruktur eingesetzt werden soll,so

ist dieses Verfahren mit äußerster Vorsicht anzuwenden, da die Gefahr besteht, dass auf diese Weise wichtige Meldungen zwar erfasst, aber übersehen werden.

3.3 Betrieb eines IDS auf Basis der ITIL

In Abschnitt 3.3.1 erfolgt eine Einordnung, die Aufschluss darüber gibt, welche Rollen ein NIDS im ITSM einehmen kann. Diese Einordnung dient dem besseren Verständnis der nachfolgenden Ausführungen. Um eine strukturierte Beschreibung der Vorgänge im laufenden Betrieb zu ermöglichen, erfolgt eine Einordnung in die Service-Support-Prozesse der ITIL anhand folgender Szenarien.

1. Alarmmeldungen (Abschnitt 3.3.2)
2. Änderungen am IDS (Abschnitt 3.3.3)

Die Umsetzung dieser Szenarien nach der ITIL mündet in der Beschreibung eines generischen Konzepts zum Management eines IDS. Priorität wird dabei auf die Allgemeingültigkeit gelegt, damit sich das Konzept produkt- und umgebungsunahängig einsetzen läßt. Die ITIL und die in ihr enthaltenen Prozesse des Service Supports (siehe Kapitel 2.2.2) wurden aufgrund der großen Praxisnähe und Anwenderorientierung als Grundlage herangezogen.

3.3.1 Einordnung eines IDS im Service Mangement

Da die ITIL das ITSM beschreibt, steht das Erbringen von Dienstleistungen im Vordergrund. Soll die ITIL als Ausgangsbasis für den Betrieb eines IDS herangezogen werden, gilt es vorab zu klären, welche Rolle ein IDS in der Dienstleistungsbeziehung spielt. Die Dienstleistungsbeziehung ist dabei die Beziehung zwischen einem Kunden – im Sinne von Dienstleistungsempfänger – und einem Anbieter – im Sinne eines Dienstleistungserbringers. Dabei kann man sich eine Art „Dienstleistunskette“ vorstellen, denn jeder Dienstleistungserbringer kann gleichzeitig auch Dienstleistungsnehmer sein (siehe Abbildung 3.7). Die erbrachte Dienstleistung wird als IT-Service bezeichnet. Nutznießer des angebotenen IT-Services ist dabei der Kunde. Für jeden IT-Service ergeben sich unterschiedliche Betrachtungswinkel. Diese unterschiedlichen Betrachtungswinkel werden für IDS nachfolgend beschrieben, wobei der IDS-Betrieb – wie zu sehen sein wird – eine Besonderheit mit sich bringt.

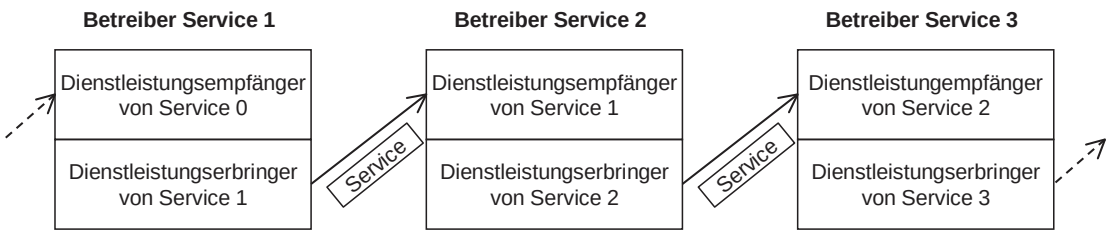


Abbildung 3.7: Dienstleistungskette

1. IDS-Betreiber als Dienstleistungserbringer

   Der Betreiber des IDS nimmt die Rolle des Erbringers einer Dienstleistung ein. Ein anderer IT-Service ist der Empfänger dieser Dienstleistung (Kunde). Die Dienstleistung selbst besteht in der Erkennung von Angriffen, die gegen das System des Dienstleistungsnehmers gerichtet sind. Ziel des Dienstleistungsnehmers ist eine Verbesserung seiner Sicherheitsstruktur, indem er mögliche Angriffe aufgrund der Meldungen des IDS entweder abwehren oder in Zukunft verhindern kann. Der Kunde könnte beispielsweise der Betreiber eines Datenbankservers sein, der das IDS dazu nutzen möchte mögliche Angriffe auf den Datenbankserver zu erkennen, um damit beispielsweise die Verfügbarkeit zu erhöhen, indem auf Angriffe schnell und gezielt reagiert werden kann. Dieses Szenario wird anhand der Abbildung 3.8 noch einmal verdeutlicht.

Abbildung 3.8: IDS-Betreiber als Dienstleistungserbringer

2. IDS-Betreiber als Dienstleistungsempfänger

   Als zweite Möglichkeit kann der Fall formuliert werden, dass der Betreiber des IDS selbst die Rolle des Dienstleistungsempfängers einnimmt. Dabei nimmt er selbst den Service eines Dienstleistungserbringers in Anspruch. Im Falle eines eigenen IDS-Netzes könnte man sich zum Beispiel vorstellen, dass dieses Netz durch eine eigene Firewall abgesichert wird. Dabei muss der Betreiber der Firewall nicht zwangsläufig gleichzeitig das IDS betreiben. Somit ist das IDS Nutzer des Services „Firewall“. Abbildung 3.9 zeigt dieses Szenario

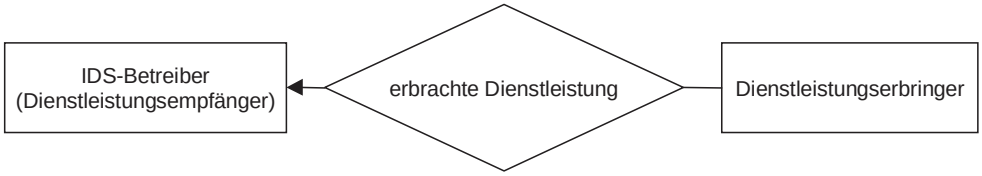


Abbildung 3.9: IDS-Betreiber als Dienstleistungsempfänger

3. IDS übernimmt die Rolle des „Kunden“

   Wie eingangs bereits erwähnt, ergibt sich für den Betrieb eines IDS eine Besonderheit in der Anbieter-Kunden-Beziehung. Und zwar dann, wenn das IDS einen Alarm ausgibt.

Dann tritt das IDS seinem Nutzer – also dem Dienstleistungsempfänger – gegenüber in der Rolle eines Störungsmelders auf. Die ITIL erlaubt diese Definition, da prinzipiell jeder berechtigt ist, Störungen zu melden. Häufig werden Störungen in der Praxis jedoch von den Kunden eines Serviceerbringers gemeldet. Deshalb kann man sich die Beziehung zwischen dem IDS und dessen Nutzer so veranschaulichen, dass das IDS kurzzeitig in die Kundenrolle schlüpft, um einen Alarm an den Serviceempfänger zu melden. Dieses Verhalten wird in Abbildung 3.10 veranschaulicht, wobei die Rolle des IDS als „Kunde“ lediglich die Situation veranschaulichen soll und nicht als Definition verstanden werden darf. Diese Rolle wird in Kapitel 3.3.2 bei der Beschreibung des Vorgehens im Alarmfall näher erläutert. Zur besseren thematischen Einordnung wird sie aber vorweggenommen und bereits hier beschrieben. Abschnitt 3.3.2 trägt nachfolgend dazu bei, mehr Klarheit im Hinblick auf die Bedeutung dieses Punktes zu schaffen.

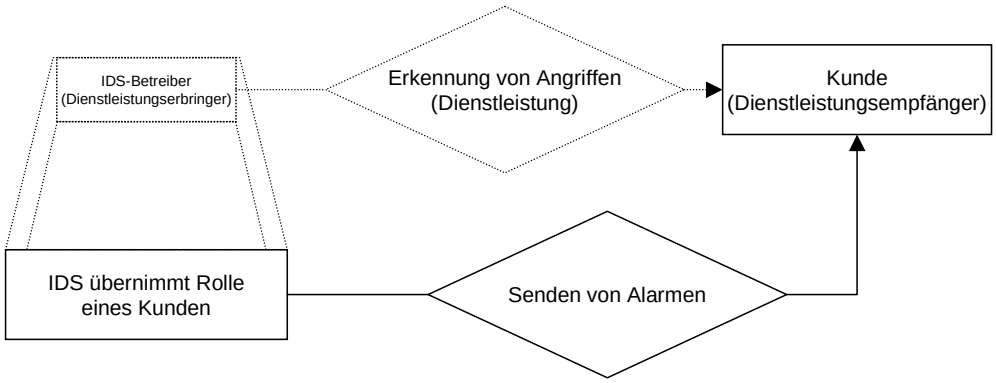


Abbildung 3.10: IDS in Kundenrolle

3.3.2 Alarmmeldungen

Beim Betrieb eines IDS dürfte wohl eines der wichtigsten Szenarien die Vorgehensweise im Falle von auftretenden Alarmmeldungen sein. Die Signalisierung sicherheitskritischer Ereignisse stellt einen der Hauptzwecke dar, ein IDS zu betreiben, insbesondere wenn die Erkennung von Angriffen als IT-Service zur Verfügung gestellt wird.[4].

Wie bereits im Abschnitt 3.3.1 festgelegt wurde, nimmt das IDS nach der ITIL gegenüber dem Dienstempfänger die Rolle des Störungsmelders ein. Wenn man sich vorstellt, dass der Dienstempfänger seinerseits auch wieder Diensterbringer für einen Dritten ist, liegt eine Störung dann vor, wenn dieser zu erbringende Dienst in irgend einer Weise beeinträchtigt wird. Ein Beispiel verdeutlicht dies: Der Betreiber eines Webservers stellt diesen als Dienst zur Verfügung. Gleichzeitig nimmt er zur Verbesserung seines Schutzpotentials die Dienste eines IDS-Betreibers in

[4]Es existieren auch Systeme, die sicherheitskritische Ereignisse lediglich protokollieren. Sie dienen meist Forschungszwecken und werden beispielsweise vom CERT eingesetzt [CERT]

Anspruch. Kommt es nun zu einem Serverausfall, werden sich die Kunden des Webserver-Betreibers an diesen wenden, um diese Störung zu melden. Liegt dem Serverausfall aber beispielsweise ein Denial-of-Service-Angriff zugrunde, erfolgt die Meldung bereits durch das IDS.

Unter Annahme dieser Rollenverteilung soll nun ein Eskalationsplan auf Basis der ITIL festgelegt werden, der das Verhalten im Alarmfall beschreibt. Dies hat den Vorteil, dass sich auf diese Weise ein strukturiertes Vorgehen ergibt. Der Umgang mit Störungen erfolgt in der ITIL mit Hilfe des Incident-Management-Prozesses (vgl. Kapitel 2.2.2). Unterstützung bietet hierbei das Problem Management (ebenfalls Kapitel 2.2.2).

Eskalationsplan auf Basis des Incident Managements

Der Vorteil einer Behandlung von Alarmen als Störung liegt auf der Hand. Genau wie eine Störung lassen sich Alarme zentral erfassen. Die zentrale Erfassung ist Aufgabe des Service Desks. Das Incident Management der ITIL beschreibt einen Umgang mit Störungen wie in Abbildung 3.11 dargestellt.

Dieses Vorgehen lässt sich auch auf einen Eskalationsplan für das IDS übertragen. Die oberste Zielsetzung besteht darin, auf eine Alarmmeldung möglichst schnell zu reagieren, um die Beeinträchtigung eines Services durch einen Angriff so gering wie möglich zu halten. Im besten Fall wird bereits der Angriffsversuch erkannt und es kommt zu keinerlei Einschränkungen des Services, im schlechtesten Falle gilt es nach einem erfolgreichen Angriff den Service so schnell wie möglich wieder verfügbar zu machen.

Die folgenden Schritte beschreiben einen Eskalationsplan auf Basis des Incident Managements:

1. Die Auswertungseinheit des IDS registriert einen potentiellen Angriff
2. Eine Alarmmeldung wird an den Service Desk des Dienstleistungsempfängers weitergeleitet. Dem Dienstleistungsempfänger obliegt die Verantwortung (Incident Ownership).[5]
3. Dies führt zum Öffnen eines Incident Records und zur Erstellung eines Incident Tickets, welches die wichtigen Daten des Alarms enthält (Art des Angriffs, betroffenes System, Datum, Zeit, etc.). Gleichzeitig wird der Vorfall in einer Datenbank erfasst.
4. Auf Basis des Incident Tickets erfolgt eine Erstbewertung und Klassifizierung, die eine möglichst schnelle Beseitigung des Incidents zum Ziel hat. Hier besteht im Falle von Security Incidents – also Incidents deren Auslöser eine Sicherheitslücke ist – eine Besonderheit, die zwei Vorgehensweisen erlaubt:
5. Das Incident Management des Dienstleistungsempfängers versucht die durch den Angriff aufgetretene Störung seines Services möglichst schnell zu beseitigen.
    a) Es wird auf eine bekannte Lösung zur Beseitigung der Störung zurückgegriffen, damit der Service aufrecht erhalten werden kann.

[5] Es spielt keine Rolle, ob der Service Desk zentral oder dezentral verwaltet wird.

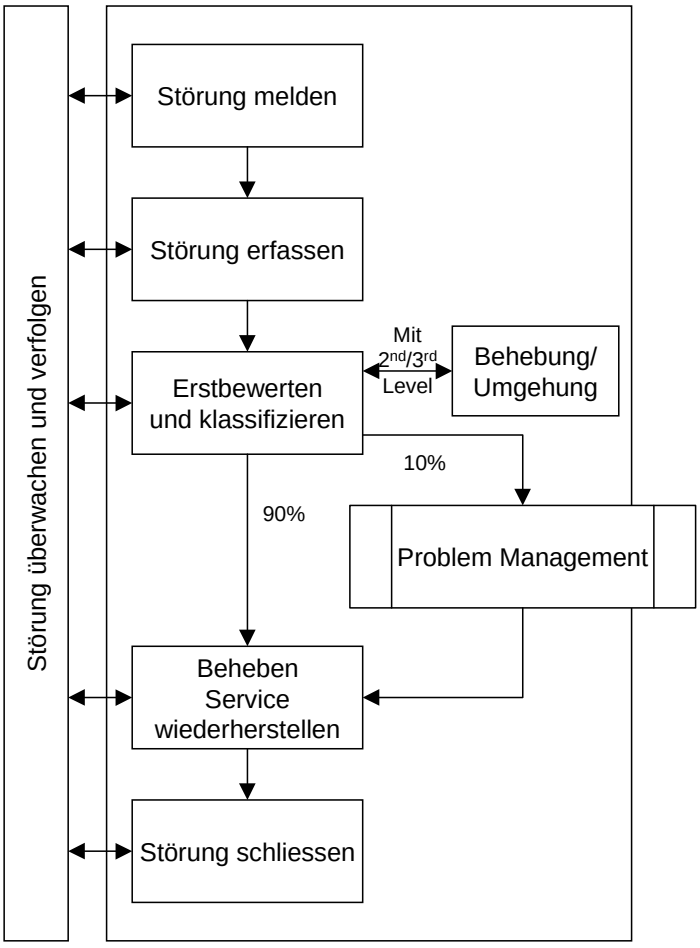


Abbildung 3.11: Incident Management nach ITIL [ITSM00]

b) Im Falle einer schwerwiegenden Sicherheitsverletzung kann die Entscheidung getroffen werden, den Service vorübergehend vom Netz zu nehmen, um zuerst ein Lösung (evtl. nur ein Work-around) zur Schließung der Sicherheitslücke zu finden.[6]

6. Die Störung wird behoben und der Service wiederhergestellt.

7. Nach erfolgreicher Behebung wird der Incident Record geschlossen.

Abbildung 3.12 veranschaulicht die beschriebene Vorgehensweise bei der Eskalation noch einmal grafisch.

[6] Die Entscheidung einen Service vorübergehend einzustellen widerspricht dem ersten Anschein nach der Idee des Incident Managements, kann jedoch sinnvoll sein, wenn dadurch eine weitergehende Einschränkung des Service verhindert werden kann. Beispiel: Die Aufgabe eines Datenbankservices besteht unter anderem darin, Datenintegrität zu gewährleisten. Zielt ein Angriff auf die Verletzung der Datenintegrität ab, so kann eine vorübergehende Deaktivierung des Services sinnvoll sein, auch wenn dadurch natürlich die Verfügbarkeit betroffen ist.

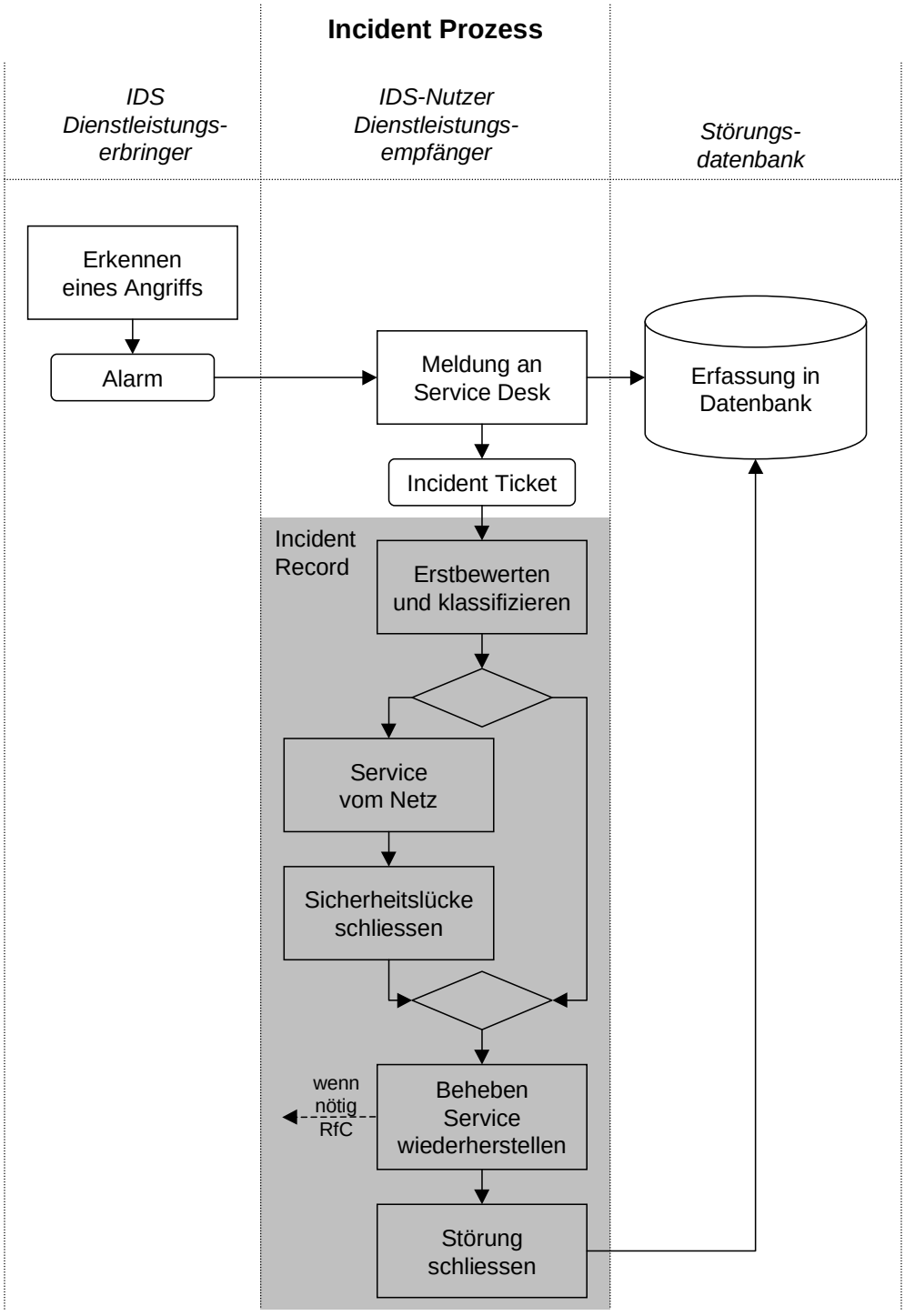


Abbildung 3.12: Eskalationsplan auf Basis des Incident Managements

Eskalationsplan auf Basis des Problem Managements

Nach ITIL definiert ein Problem eine noch nicht bekannte Ursache für eine Störung. Während das Incident Management lediglich versucht eine Störung schnellstmöglich zu beseitigen, beschäftigt sich das Problem Management mit der Ursachenforschung (vgl. [Elsa05]). Treten Störungen häufiger auf oder können Servicebeeinträchtigungen lediglich durch Behandlung der Symptome behoben werden, ist es die Aufgabe des Problem Managements, den Ursachen auf den Grund zu gehen und Lösungen zu erarbeiten. Ähnlich wie beim Incident Management, existiert auch für das Problem Management ein Ablaufplan, der ein strukturiertes Vorgehen beschreibt. Wie die Abarbeitung von Problemen in der ITIL vonstatten geht, zeigt Abbildung 3.13.

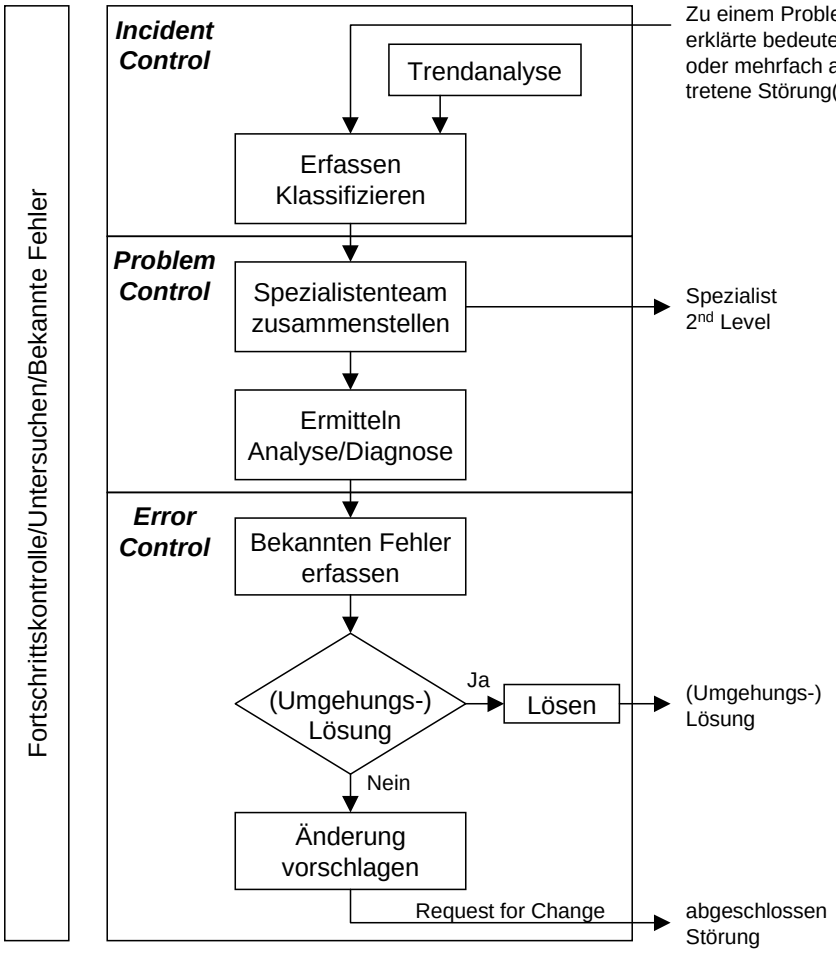


Abbildung 3.13: Problem Management nach ITIL [ITSM00]

Der anhand des Incident Management erarbeitete Eskalationsplan lässt sich auf den Bereich des Problem Managements erweitern. Für IDS-Alarme bedeutet dies, Servicebeeinträchtigungen

nachhaltig zu vermeiden, indem bestehende Sicherheitslücken geschlossen werden. Zur Veranschaulichung der Problematik folgende Beispiele: Es könnte sich herausstellen, dass ein Service wegen einer Sicherheitslücke der Firewall beeinträchtigt ist, die durch eine entsprechende Konfigurationsänderung behoben werden kann. Eine andere Möglichkeit wäre, dass sich fehlerhaft implementierte Anwendungen als Problem erweisen, sodass das Einspielen eines Patches notwendig wird.

Die Erweiterung des Eskalationsplans für IDS-Alarme, die das Problem Management integriert, lässt sich wie folgt beschreiben:

1. Das Problem Management greift auf die gemeinsame Datenbank zu, in der die an das Incident Management weitergereichten Alarmmeldungen (als Störungen) gespeichert sind.[7]
2. Alarme unbekannter Ursache werden erfasst und klassifiziert. Es wird ein Problem Record eröffnet.
3. Ein Spezialistenteam zur Bearbeitung des Problems Records wird zusammengestellt.
4. Das Spezialistenteam hat die Aufgabe den Grund für die Alarmmeldung zu identifizieren. Anschließend hat eine Analyse/Diagnose des Problems zu erfolgen, um wiederholtes Auftreten zu verhindern.
5. Ist die Ursache für die Alarmmeldung gefunden, wird kontrolliert, ob es sich um einen bereits bekannten Fehler (Known Error) handelt, der so oder in ähnlicher Form schon einmal aufgetreten ist.
6. Nun gibt es zwei Möglichkeiten:
   a) Handelt es sich um einen bekannten Fehler, lässt sich durch eine (Umgehungs-)Lösung rasch Abhilfe schaffen. Dann wird das Problem gelöst und die erfolgreiche Lösung an das Incident Management gemeldet (Second-Level-Support).
   b) Ist eine (Umgehungs-)Lösung nicht bekannt und es sind tiefgreifendere Änderungen an Hard- und Software nötig, wird ein Änderungsvorschlag (Request for Change, RfC) an das Change Management herangetragen (Third-Level-Support).
7. Nach Beheben des Problems (der Sicherheitslücke), wird die Lösung dem Incident Management mitgeteilt (in der Support Datenbank des Service Desk hinterlegt) und der Problem Record geschlossen.

Eine grafische Veranschaulichung der beschriebenen Schritte ist in Abbildung 3.14 noch einmal dargestellt.

An dieser Stelle noch ein wichtiger Hinweis, da in diesem Zusammenhang bei der Erstellung des Eskalationsplans wiederholt Schwierigkeiten aufgetreten sind. Incident Management und Problem Management werden in der ITIL in getrennten Prozessen beschrieben. Das bedeutet, dass ein „Incident“ niemals zum „Problem“ wird und umgekehrt. Die beiden Records werden

[7] Ob die Informierung des Problem Managements bei Auftreten eines Incidents ohne bekannte Ursache eine Hol- oder eine Bringschuld ist, wird in der ITIL nicht explizit festgelegt. Das gleiche gilt bei wiederholt auftretenden Störungen (vgl. [ViGu04]

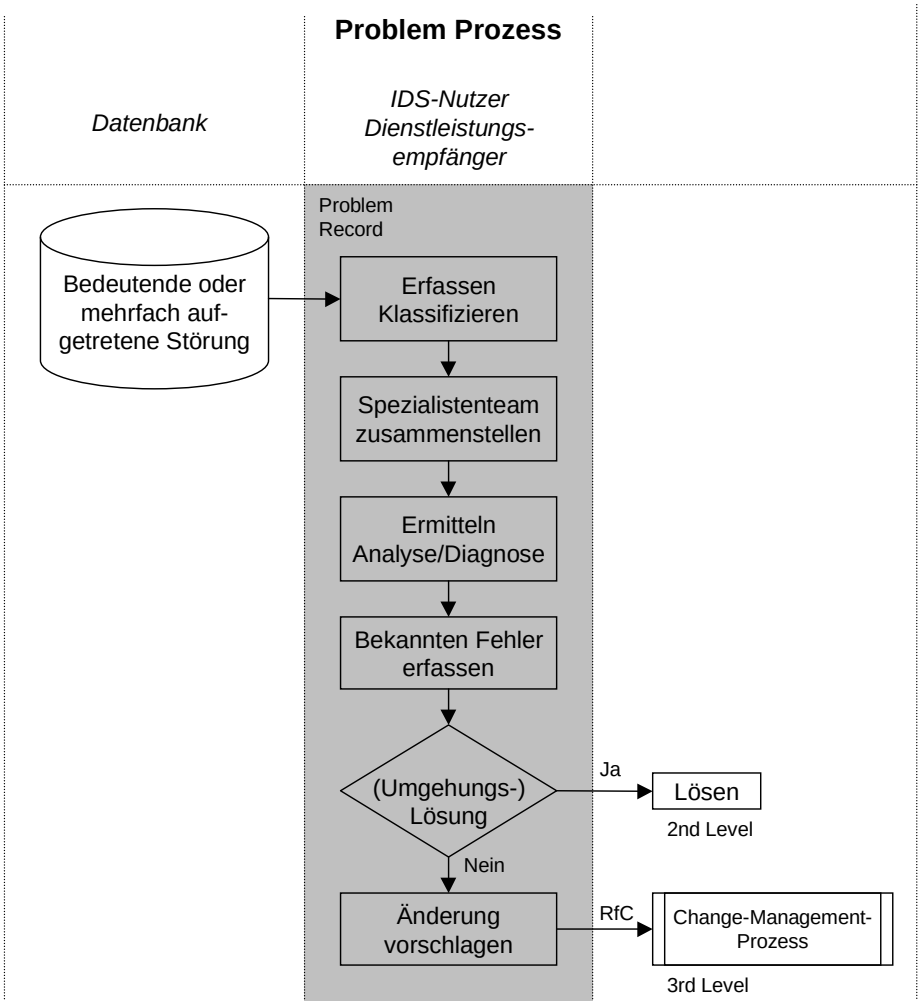


Abbildung 3.14: Eskalationsplan auf Basis des Problem Managements

völlig unabhängig voneinander verwaltet. Trotzdem sei hier auf die Notwendigkeit einer engen Kooperation zwischen Incident Management und Problem Management hingewiesen.

Es besteht die Möglichkeit, dass die Lösung für einen Sicherheitsvorfall eine dauerhafte Beeinträchtigung des angebotenen Services zur Folge hat. In einem solchen Fall müssen bestehende Service Level Agreements entsprechend angepasst werden. Dies ist Aufgabe des Service Level Managements.

3.3.3 Änderungen am IDS

Einen besonderen Stellenwert bei der Erstellung eines Konzepts zum Management von IDS nimmt die Behandlung von Änderungen ein. Schön wäre die Theorie eines Systems, welches einmal in Betrieb genommen, ohne weiteres Zutun seine Arbeit verrichtet. Doch der häufig zu hörende Ratschlag „Never touch a running system!“ lässt sich in der Praxis leider nicht umsetzen. Zustande gekommen ist dieser Ausspruch, da häufig die Erfahrung gemacht wurde, dass durch Änderungen in einem zuvor gut funktionierendes System oft Fehler aufgetreten sind. Da sich Änderungen aber wie gesagt nicht vermeiden lassen, gilt es ein Vorgehen zu entwickeln, wie diese am günstigsten abgewickelt werden können.

Hauptverantwortlich für Änderungen an einem IDS sind vor allem zwei Punkte. Der erste Punkt nimmt dabei besonders aus Sicht des Dienstleisters eine wichtige Rolle ein. Nämlich wenn aufgrund neuer Dienstleistungsvereinbarungen Erweiterungen an dem bestehenden System notwendig werden. Entweder ein neuer Kunde will den Dienst in Anspruch nehmen, oder ein bereits bestehender Kunde möchte die Inanspruchnahme des Dienstes ausweiten. In beiden Fällen wird die Installation neuer beziehungsweise zusätzlicher Sensoren notwendig. Der umgekehrte Fall, also die Auflösung von Dienstleistungsvereinbarungen mit der damit verbundenen Entfernung von Sensoren, lässt sich genauso beschreiben. Der zweite Punkt der zu Änderungen an einem IDS führen kann, ist die Notwendigkeit einer ständigen Aktualität des Systems, da nur so eine möglichst gute Erkennung von Angriffen sichergestellt werden kann. Zum einen muss eine ständige Aktualisierung des Systems selbst durch Einspielen von Patches und Softwareupdates durchgeführt werden, zum anderen gilt es ein signaturbasiertes IDS – wie das hier betrachtete – laufend mit den neuesten Signaturen zu versorgen. Diese beiden Anwendungsfälle für das hier betrachtete Szenario werden in Kapitel 4, wenn es um die prototypische Umsetzung geht noch ausführlich behandelt (Abschnitt 4.3.2 und 4.3.3).

Der praktische Einsatz macht selbstverständlich zahlreiche weitere Möglichkeiten denkbar, die zu einer Veränderung an dem IDS führen können. Diese lassen sich hier nicht alle einzeln darstellen, weshalb der Prozessablauf bei der Durchführung eines „Changes“ hier generisch beschrieben wird. Dieser bildet auch die Grundlage für die in Kapitel 4 beschriebenen Anwendungsfälle. Auf diese Weise lassen sich auch andere als die beschriebenen Anwendungsfälle, die sich aus der Praxis ergeben, leicht einordnen.

Die ITIL fordert auch bei der Durchführung von Changes ein strukturiertes Vorgehen. In diesem Punkt hat die ITIL sogar einen Vorzug gegenüber dem OSI-Management. Während im OSI-Management Änderungen Teil des Configuration Managements sind, wird im ITSM unterschieden zwischen Configuration Management und Change Management. Das Change Management beschreibt den Ablauf des Änderungsvorgangs selbst. Das Configuration Management schafft hierfür die Grundlage, indem es alle notwendigen Informationen über eine IT-Infrastruktur und ihre Konfiguration liefert und alle Änderungen erfasst. Es ist also für die Bereitstellung einer Informationsbasis verantwortlich, die den anderen ITIL-Prozessen zur Verfügung gestellt wird. Die hier zusammengetragenen Informationen über die Infrastuktur werden den anderen ITIL-Prozessen zur Verfügung gestellt. Wie bereits in Kapitel 2.2.2 beschrieben, werden sie in eine Datenbank, die CMDB, eingetragen. Die eingetragenen Daten müssen dabei jeweils den aktuellen Stand der tatsächlichen Gegebenheiten widerspiegeln. Das heißt, die Daten müssen sich

stets in einem aktuellen und konsistenten Zustand befinden. Aufgabe des Change Managements ist es nun, genau dies zu gewährleisten. Es dient der Steuerung und Kontrolle von Änderungen an den CIs [ViGu04].

Die Erstellung eines Datenbankschemas zur Erfassung der CIs eines IDS würde den Rahmen der Arbeit sprengen und hier auch von der Thematik abweichen. Für das Management von Änderungsvorgängen ist der Zusammenhang zwischen Configuration Management und Change Management aber dennoch wichtig. Deshalb an dieser Stelle ein kurzer Exkurs, um einige wichtige Punkte zu erläutern, die bei der Erstellung einer CMDB für IDS wichtig sind.

Die Beschreibung in einem Datenbankschema erlaubt eine Zerlegung des IDS in einzelne zu managende Einheiten, wobei diese logisch voneinander abhängig sind. Auch diese Abhängigkeiten lassen sich in Form von Beziehungen in einem Datenbankschema klar wiedergeben. Für die Unterteilung in einzelne Einheiten wurde die Grundlage bereits in Kapitel 2.1 geschaffen. Tabelle 2.1 gliedert ein IDS in verschiedene Teilkomponenten, die sich an den Arbeitsschritten orientieren. Warum diese Unterteilung sinnvoll ist, wurde bereits diskutiert. Eine Orientierung an dieser Untergliederung bei der Definition der CIs bietet sich somit natürlich an und erscheint sinnvoll.

Grundsätzlich ist anzumerken, dass die CIs eines IDS nicht nur die Hardware und deren Beziehung beschreibt, sondern dass auch Software, Dokumentationen, Arbeitsanweisungen und Verträge erfasst werden müssen, wodurch die Komplexität natürlich erheblich steigt. Diese Notwendigkeit ergibt sich durch die vielen Schnittstellen des Configuration Managements, welche die Unterstützung sämtlicher anderen Service Management Prozesse gewährleisten sollen. Hervorzuheben sind hier natürlich die anderen Prozesse des Service Support.

Das Datenbankschema sollte so generisch gehalten sein, dass in der Praxis die Daten jedes tatsächlich existierenden IDS-Produkts – wie z. B. Snort – in die CMDB übertragen werden können. Ansätze hierfür finden sich beispielsweise bei Jäger [Jaeg05].

Nun zurück zum Prozessablauf im Change Management, mit dessen Hilfe das Vorgehen bei Änderungen am IDS beschrieben werden können. Das Vorgehen orientiert sich an den Publikationen des itSMF [ITSM02] und OGC [OGC05]. Auslöser für eine Änderung ist immer ein formaler RfC. Der RfC kann durch den Kunden direkt erfolgen oder vom Service Desk oder Service Level Management weitergeleitet werden. Vom OGC heißt es hierzu:

> „Customers - may request more, fewer or other services. These requests may be submitted directly as RFC's, or channeled through the Service Desk, Service Level Management or IT Customer Relations Management." [OGC05]

Die nachfolgende Beschreibung der Änderungsvorgänge orientiert sich an Abbildung 3.15.

1. Der Change Manager, der für Änderungen zuständig ist, muss den RfC protokollieren.
2. Es muss entschieden werden ob der Änderungsantrag akzeptiert wird, d. h. ob überhaupt eine weiter Bearbeitung erfolgt. Dabei wird aber lediglich eine grobe Vorauswahl getroffen. Gründe für eine Nichtakzeptanz könnten beispielsweise doppelte, überflüssige oder nicht umsetzbare RfCs sein. Eine Ablehnung ist dem Antragssteller mitzuteilen. Dieser hat dann die Möglichkeit einen neuformulierten RfC einzureichen.

3. Der Change Manager nimmt eine Klassifizierung des Änderungsantrags vor. Die Klassifizierung erfolgt nach zwei Kriterien: Priorität und Kategorie. Die Priorität gibt an wie wichtig ein Change im Vergleich zu anderen Changes ist, die Kategorie richtet sich nach den Auswirkungen.[8]

4. Abhängig von der Klassifizierung entscheidet der Change Manager über die Dringlichkeit der Änderung. Bei Notfällen erfolgt eine gesonderte Behandlung durch das Change Advisory Board Emergency Committee (CAB/EC). Es ist autorisiert Notfallentscheidungen zu treffen. Lange Genehmigungswege entfallen. Notfälle unterliegen aber im wesentlichen den gleichen weiteren Schritten, wie alle anderen Änderungen.

5. Für Änderungen die keine Notfälle sind wird entschieden ob das Change Advisory Board (CAB) eingeschaltet wird. Die Entscheidung darüber kann von der Klassifizierung der Änderung abhängig gemacht werden. Kommt das CAB nicht zum Einsatz erfolgen alle weiteren Entscheidungen durch den Change Manager. Der Change Manager übernimmt auch bei Einsatz eines CAB dessen Vorsitz. Die Mitgliedschaft im Change Advisory Board kann je nach anfallenden Änderungen flexibel gestaltet werden. Normalerweise sind in ihm das Change Management, das Service Level Management sowie weitere Prozess-Manager vertreten. Dazu kommen noch Spezialisten, wie Kunden, Berater und Zulieferer (vgl. [ViGu04]).

6. Für die vorgesehenen Änderungen erfolgt eine Zeitplanung. Die Realisierung einzelner Änderungen wird terminiert. Das CAB hat bei der Planung wichtiger Changes eine beratende Funktion. Gleichzeitig ist es dafür verantwortlich, dass der Kunde in den Planungsprozess mit eingebunden wird.

7. Das CAB beziehungsweise der Change Manager muss Änderungen genehmigen. Das Change Management koordiniert die Weiterleitung genehmigter Änderungen an die entsprechenden Spezialisten (Administratoren, Techniker, etc.). Die Realisierung des Changes erfolgt in einem Entwicklungszyklus. Es sollte stets eine enge Zusammenarbeit zwischen dem Change Management und den Spezialisten bestehen. Nach erfolgreicher Entwurfs- und Testphase kann eine Implementierung in das laufende System erfolgen.

8. Der Abschluss des Change Prozesses bildet die Evaluation.[9] Es wird überprüft, ob die Änderung das gewünschte Ergebnis erbracht hat, und welche Aus- beziehungsweise Nebenwirkungen die Änderung hatte. Wenn die Änderung erfolgreich war, kann der RfC geschlossen werden, ansonsten kann er am Punkt des Scheiterns neu aufgenommen werden. In der Praxis ist es meist sinnvoll die Änderungen rückgängig zu machen und einen neuen RfC einzureichen.

[8] Die ITIL schreibt kein verbindliches System für die Klassifizierung vor, was eine flexible Anpassung an verschiedene Betriebsumgebungen erlaubt.

[9] In Ausnahmefällen, z. B. bei Standard-Changes, kann die Evaluation entfallen.

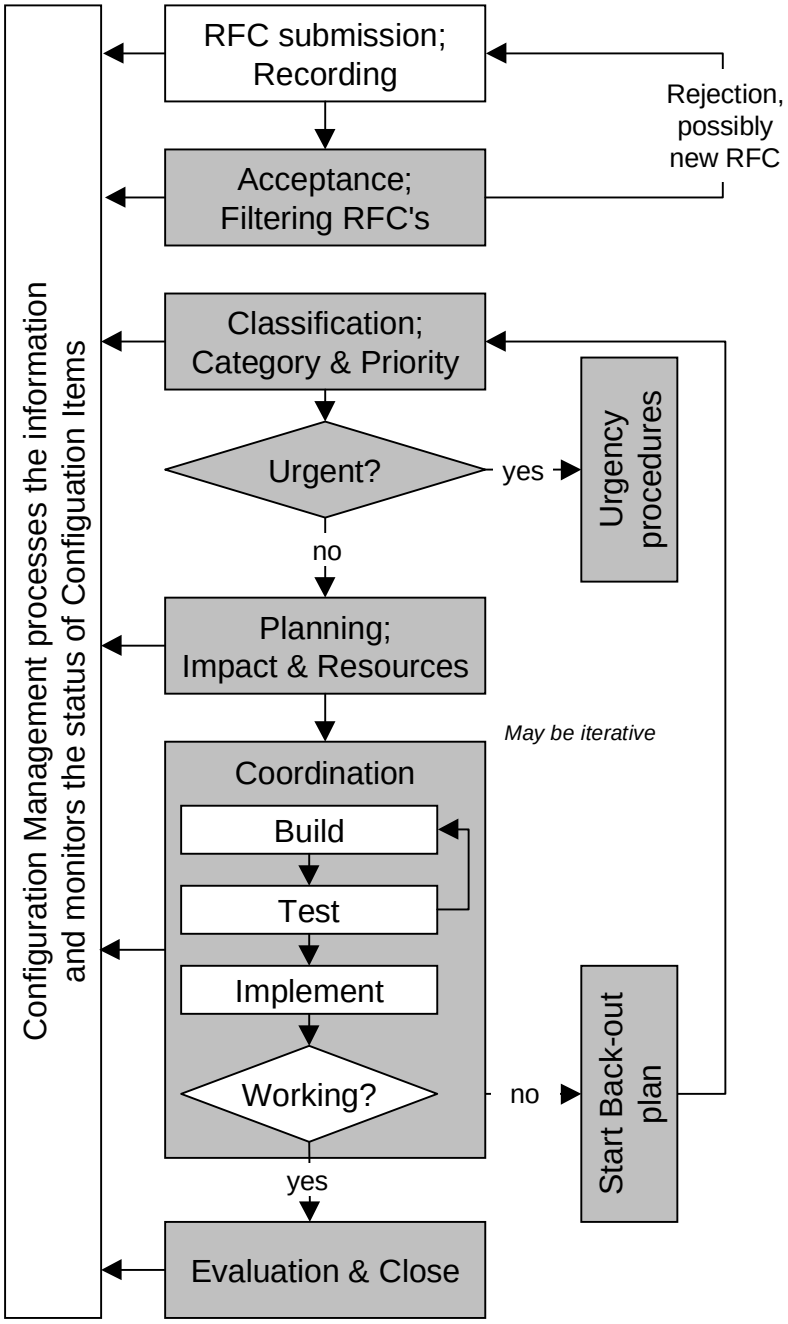


Abbildung 3.15: Change Management activities [ITSM02]

Der gesamte beschriebene Prozessablauf kann im ITSM nicht isoliert betrachtet werden. Zu einigen Service Prozessen besteht eine enge Verbindung (vgl. auch Abbildung 2.6).

Auslöser für Requests for Change

Eine der Verbindungen zu anderen Prozessen schafft der oben bereits angeführte RfC. Wenn in den weiteren Ausführungen davon ausgegangen wird, dass ein RfC vom Kunden ausgelöst wird, so ist dies nicht als Verallgemeinerung zu verstehen. Es wird deutlich darauf hingewiesen, dass dies nicht zwangsläufig der Fall sein muss. Wie bereits erwähnt, können auch andere Prozessabläufe zu einem RfC führen. An erster Stelle sind hier das Incident Management und das Problem Management zu nennen. In beiden Prozessen ist ein möglicher RfC an das Change Management vorgesehen. Gerade was das Incident Management anbelangt, muss einem RfC nicht in jedem Fall eine Störung zugrunde liegen. Denkbar für einen RfC sind auch sogenannte Service Requests, also normalen Kundenanfragen, deren Grund nicht eine Störung der angebotenen Dienstleistung ist. Auslöser von RfCs können weiterhin auch neue SLAs sein, die zwischen Kunden und Serviceanbieter durch das Service Level Management vereinbart wurden.

Die hier aufgezeigten Möglichkeiten einen RfC auszulösen sind bei weitem nicht vollständig. Sie sollen lediglich ein Grundverständnis für die Problematik schaffen, wie viele Möglichkeiten bestehen, eine Änderung anzustoßen. Der RfC selbst definiert dabei eine Schnittstelle des Change Managements zu den anderen Prozessen. Ob ein RfC direkt durch eine Person oder indirekt durch einen anderen Prozess angestoßen wird, hängt vom Einzelfall ab. Letztendlich ist dafür auch entscheidend inwieweit die verschiedenen ITIL-Prozesse in einem Unternehmen umgesetzt sind. Das ITSM erlaubt auch eine schrittweise Einführung mit der Umsetzung einzelner Prozesse.

Beziehung zum Release Management

Die Beziehungen zwischen Change und Release Management kommen besonders bei der Realisierung der Änderungen zum Tragen. Die Realisierung ist in Abbildung 3.15 Teil des Punktes „Coordination“. Das Change Management legt fest, welche Maßnahmen für die Änderung erforderlich sind und stellt sicher, dass die Änderungen autorisiert sind. Das Release Management kümmert sich dagegen darum, wie die Änderungen durchgeführt werden sollen. Es entwickelt effiziente Prozeduren für die Verteilung und Installation von Veränderungen (vgl. [ViGu04]). Darüber hinaus werden im Release Management auch mehrere Änderungen die denselben Bereich eines IT-Systems betreffen zu Paketen zusammengestellt. Diese Pakete werden als Releases zusammen implementiert. Der Release Manager ist für gewöhnlich auch Mitglied des CAB (vgl. [OGC05]). In Zusammenarbeit mit dem Release Management erstellt das Change Management auch Back-out-Prozeduren, die eine Wiederherstellung des alten Systemzustandes ermöglichen, falls eine Änderung fehl schlägt.

Beziehung zum Configuration Management

Während des gesamten Change Prozesses erfolgt eine enge Zusammenarbeit mit dem Configuration Management. Jeder Schritt des Change Prozesses erfolgt auf Basis der Daten die über alle von der Änderung betroffenen CIs in der CMDB erfasst sind. Bei jeder Implementierung einer Änderung wird diese durch das Change Management autorisiert. Gleichzeitig sorgt es dafür, dass die Änderungen vom Configuration Management erfasst werden. Damit ist die ständige Aktualität der Datenbank gewährleistet. Für die Erfassung selbst ist das Configuration Management zuständig

4 Prototypische Umsetzung des Konzepts

In diesem Kapitel wird eine konkrete Instantiierung des Managementkonzepts für IDS aus Kapitel 3 im Umfeld des Landesamtes für Statistik und Datenverarbeitung (LfStaD) vorgenommen. In Abschnitt 4.1 erfolgt eine Beschreibung der Einsatzumgebung, in der die prototypische Umsetzung erfolgen soll. Anschließend wird in Abschnitt 4.2 eine Lösung zum Aufbau der IDS-Infrastruktur für das Bayerische Behördennetz vorgeschlagen. Danach wird in Abschnitt 4.3 die Realisierung der verschiedenen ITIL-Prozesse für den IDS-Betrieb diskutiert. Zum Abschluss wird in Abschnitt 4.4 eine Bewertung vorgenommen, inwieweit sich das Managementkonzept – auf Basis der ITIL – zum Betrieb eines IDS in der Praxis umsetzen lässt.

4.1 Einsatzumgebung

In Kapitel 2.3 wurde das LfStaD bereits vorgestellt und der Aufbau des Bayerischen Behördennetzes skizziert. Zum momentanen Zeitpunkt befindet sich im Bayerischen Behördennetz noch kein IDS im Einsatz beziehungsweise finden lediglich Pilotversuche statt. Es wurde aber bereits eine Evalutation verschiedener IDS für das LfStaD vorgenommen. Die Evalutation wurde im Rahmen einer Diplomarbeit von Iliopoulos [Ilio05] durchgeführt. Bei den getesteten System handelt es sich ausschließlich um NIDS. Die beiden in der Diplomarbeit behandelten Systeme werden beide durch einen kommerziellen Anbieter vertrieben.[1] Die Entscheidung zur Evaluation kommerzieller Produkte wurde aufgrund der Möglichkeit von Wartungsverträgen mit den Anbietern der IDS-Produkte getroffen.[2]

Momentaner Stand ist, dass ein NIDS am Landesamt zum Einsatz kommen soll, jedoch wurde noch keine Entscheidung zugunsten eines bestimmten Systems getroffen. Zum jetzigen Zeitpunkt steht auch noch nicht fest, ob eines der getesteten Systeme oder ein anderes Produkt zum Einsatz kommen soll. Unabhängig von einem eventuellen Supportvertrag mit dem Hersteller des IDS, ist das LfStaD aus Managementsicht der Betreiber. Die Beziehungen zwischen Landesamt und Produkthersteller spielen hier keine Rolle.

In Absprache mit dem LfStaD wurde eine mögliche Einsatzumgebung für ein IDS festgelegt, um auf Basis dieser Informationen eine Umsetzung des beschriebenen Managementkonzepts vornehmen zu können. Dabei war darauf zu achten, dass die Einsatzumgebung für den prototypischen Zweck nicht zu komplex ausfällt.

Die Wahl der Einsatzumgebung wurde von verschiedenen Faktoren beeinflusst:

[1] Es handelt sich jeweils um ein Produkt der Firma GeNUA mbH und ein Produkt von Symantec.

[2] Ursprünglich war die Evaluation von Open Source Produkten vorgesehen

Rolle (Aufgabenbereich)	**Zuständige Abteilung im Landesamt**
Betreiber der Exchange-Umgebung	Zentrale Dienste
Betreiber der Firewall	Security Dienste
Betreiber des IDS	Security Dienste
Netzbetreiber	Tk- und Netzdienste
Verkabelung	RZ Technik

Tabelle 4.1: Rollenaufteilung im LfStaD

- Das IDS sollte in einer Umgebung zum Einsatz kommen, in der ein Betrieb aufgrund hoher Sicherheitsanforderungen sinnvoll ist.
- Der zu überwachende Netzwerkbereich sollte nicht zu groß und komplex gewählt sein.
- Um im Rahmen dieser Arbeit eine gute Abgrenzung vornehmen zu können soll die Anzahl betroffener Organisationseinheiten am LfStaD überschaubar bleiben.

Als Einsatzumgebung wurde ein Teilnetz des Bayerischen Behördennetzes ausgewählt, in welchem sich ein Microsoft Exchange Server befindet, der für den gesamten internen Mailverkehr zuständig ist. Für diesen Bereich sind alle oben genannten Faktoren erfüllt. Der Betrieb des Exchange Servers im Bayerischen Behördennetz stellt hohe Anforderungen in puncto Sicherheit. Dabei steht hier in erster Linie die Gewährleistung der Dienstverfügbarkeit im Vordergrund, da bei einem Ausfall der komplette Email-Verkehr im Bayerischen Behördennetz zum Erliegen kommen würde. Der Bereich in dem der Exchange Server betrieben wird ist überschaubar, weil er in einem eigenen Teilnetz betrieben wird. Die Anzahl der betroffenen Organisationseinheiten lässt sich, wie nachfolgend zu sehen, gut abgrenzen.

Zur Abgrenzung der Organisationseinheiten soll vorweg das zu überwachende Teilnetz beschrieben werden.

Im Prinzip kann man sich das Teilnetz wie eine DMZ im internen Bereich des Bayerischen Behördennetzes vorstellen (vgl. Abbildung 2.7).[3] Der Exchange Server wird innerhalb des Teilnetzes betrieben und gegenüber den anderen Teilnetzen durch einen Microsoft Internet Security and Acceleration Server, der die Funktion einer Firewall übernimmt, geschützt. Im folgenden wird der Einfachkeit halber von der ISA-Firewall gesprochen. Die Einsatzumgebung wird in Abbildung 4.1 noch einmal skizziert.

Damit ergibt sich die in Tabelle 4.1 vorgenommene Aufgabenverteilung auf verschiedene Organisationseinheiten. Wie aus der Tabelle hervorgeht, ist die Abteilung „Security Dienste“ für den Betrieb des IDS verantwortlich. In der Tabelle werden entsprechend der Aufgabenbereiche bereits die Rollen vergeben, die später aus Sicht des Managements zu unterscheiden sind. Hierbei ist festzuhalten, dass zwar im speziellen Fall des Landesamtes der Aufgabenbereich „Betreiber der Firewall-Einrichtung“ und „Betreiber des IDS“ von einer Abteilung betreut werden, hier aber aus Managementsicht zwei verschiedene Rollen definiert werden.

[3] Im LfStaD findet die Bezeichnung DMZ für diesen Bereich keine Verwendung.

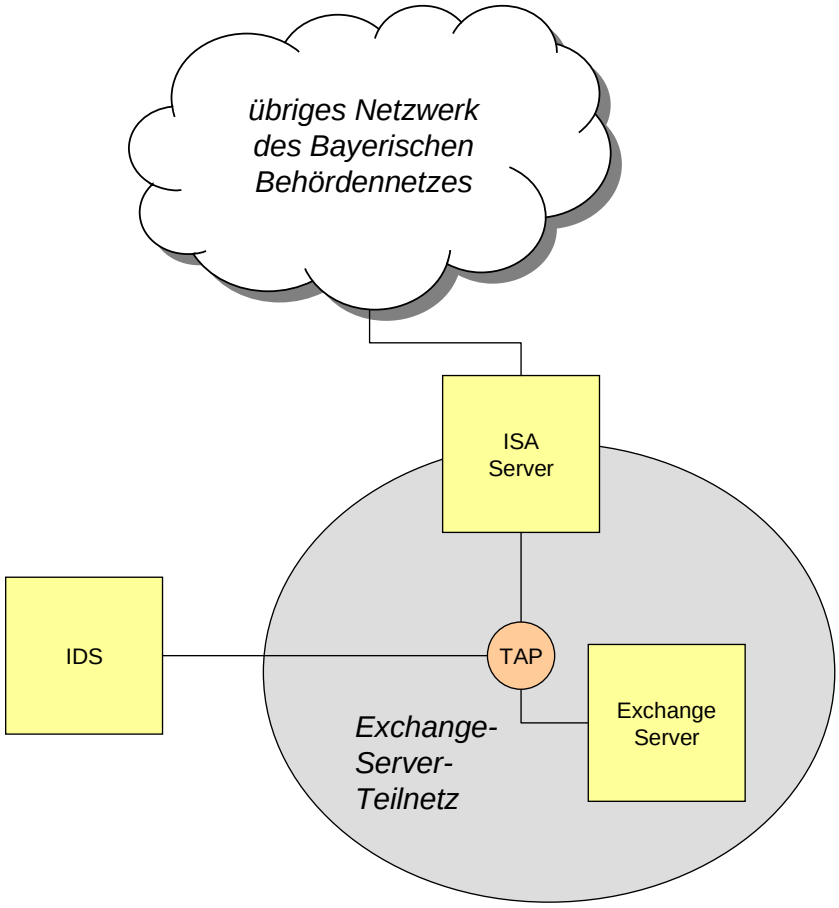


Abbildung 4.1: Einsatzumgebung für das IDS im Bayerischen Behördennetz

4.2 Vorschlag für den Aufbau einer Infrastruktur

Im folgenden soll ein Vorschlag zum Aufbau einer IDS-Infrastruktur für die in Abschnitt 4.1 vorgestellte Einsatzumgebung erfolgen. Das Vorgehen erfolgt dabei in enger Anlehnung an die in Kapitel 3.2 gemachten Ausführungen.

4.2.1 Platzierung der Sensoren

Auch wenn eine umgekehrte Vorgehensweise möglich wäre, wird hier – wie bereits in Kapitel 3.2 – mit der Platzierung der Sensoren[4] begonnen und anschließend die Platzierung der anderen IDS-Komponenten besprochen.

[4] Der Einfachheit halber, wird hier anstelle von „Informationsbeschaffungseinheiten“ der Begriff „Sensoren“ verwendet. Die Unterschiede wurden bereits in Kapitel 2.1 erläutert, können hier aber vernachlässigt werden.

Im konkreten Fall wird durch das IDS der Zweck verfolgt, dass ein „wichtiges System“ der IT-Umgebung überwacht werden soll. Bei dem System handelt es sich um den Exchange Server und eventuell zugehörige Komponenten. In diesem Fall ist es möglich den Exchange Server und die zugehörigen Komponenten als eine Einheit zu betrachten, da sie alle im gleichen Teilnetz betrieben werden und ein NIDS zum Einsatz kommt. Das NIDS ermöglicht aufgrund seiner Beschaffenheit, bei entsprechender Platzierung der Sensoren, den gesamten Datenverkehr eines Netzes abzuhören.

Da der Exchange Server in den Produktivbetrieb des LfStaD eingebunden ist, kann die Schlussfolgerung gezogen werden, dass der Einsatz des IDS aus organisatorisch-betrieblicher Sicht betrachtet werden muss. Das IDS hat also primär die Aufgabe eine zusätzliche Schutzfunktion zur Verfügung zu stellen (vgl. Kapitel 3.2.1. Für die Sensorplatzierung ist also der auf S. 38 beschriebene 1. Weg (von innen nach außen) anzuwenden.

Bei der prototypischen Umsetzung wird im folgenden ohne Beschränkung der Allgemeinheit davon ausgegangen, dass lediglich ein Sensor, der das entsprechende Teilnetz überwacht, zum Einsatz kommt. Da das Exchange-Server-Netz am LfStaD redundant ausgelegt ist, ist in der Praxis davon auszugehen, dass mehrere Sensoren zum Einsatz kommen werden. An Stellen wo dies von Bedeutung ist, wird gesondert darauf hingewiesen.

Die Entscheidung, zu Beginn lediglich das Teilnetz selbst zu überwachen und eine Platzierung weiter außen liegender Sensoren vorerst nicht vorzunehmen, rührt auch daher, dass sich damit die Anzahl an Alarmmeldungen wirksam reduzieren lässt, und somit der betriebliche Ablauf weniger beeinflusst wird. Eine zu große Anzahl an auflaufenden Alarmmeldungen kann derzeit im LfStaD nicht bewältigt werden, da hierfür die personellen Voraussetzungen fehlen. Daher ist der forschungstechnisch interessante Aspekt, einen Gesamtüberblick über die Gefahrenlage zu bekommen, aus betrieblicher Sicht nicht realisierbar. Trotzdem wird durch dieses Vorgehen nicht von vorneherein die Wirksamkeit des IDS eingeschränkt, da ein späterer Ausbau jederzeit möglich ist.

4.2.2 Platzierung der übrigen Komponenten

Der Wahl geeigneter Sensorstandorte folgt die Entscheidung darüber, wie die Anordnung der übrigen IDS-Einheiten vorzunehmen ist. Diese Einheiten sind, wie in Kapitel 2.1 vorgestellt, die Komponenten zur Informationsauswertung, zur Signalisierung/Reaktion, zum Management und zur Datenspeicherung.

In Kapitel 3.2.2 wurden für die Anordnung dieser Komponenten drei verschiedene Möglichkeiten genannt und diskutiert. Dabei wurde der Schluss gezogen, dass aus sicherheitstechnischer Sicht eindeutig der Lösung eines eigenen IDS-Netzes der Vorzug zu geben ist. Da im LfStaD Systeme mit höchsten Sicherheitsanforderungen betrieben werden, liegt der Schluss nahe, genau diese Lösung anzuwenden.

Der Betrieb eines eigenen Netzes für das IDS bringt aber das Problem mit sich, dass eventuell versteckte Kanäle entstehen können, indem zwei Teilnetze des Produktivnetzes überbrückt werden. In dem hier vorgestellten Szenario wird diese Möglichkeit aber bereits aufgrund der

Beschränkung auf ein Teilnetz (das Exchange-Server-Netz) ausgeschlossen. Im Hinblick auf eine spätere Erweiterung des IDS auf andere Teilnetze ist das Problem auf diese Weise aber noch nicht zufriedenstellend gelöst. Es sollten unbedingt Ethernet Taps als Informationsbeschaffungseinheit zum Einsatz kommen, die als passive Komponenten vollständig transparent im Produktivnetz eingehängt werden. Dabei sollten unbedingt Modelle zum Einsatz kommen, die auch im Falle einer Unterbrechung der Stromzufuhr die Weiterleitung der Daten im Produktivnetz sicherstellen. Eine Spiegelung der Daten auf den Tap-Ausgang findet in diesem Fall natürlich nicht mehr statt.[5]

Die Entscheidung für ein eigenständiges IDS-Netz zieht die Installation eigener Schutzeinrichtungen nach sich, da ein isolierter Betrieb des IDS als unrealistisch betrachtet werden darf. Auch wenn auf Seiten der Ethernet Taps keine direkte Übertragung vom IDS-Netz in das Produktivnetz existiert, bestehen Schnittstellen zu anderen Netzen (evtl. auch dem Produktivnetz). Diese ergeben sich beispielsweise durch die Notwendigkeit einer ständigen Aktualisierung der Signaturen, die normalerweise über das Internet erfolgt. Es muss darüber hinaus auch die Möglichkeit geben, im Alarmfall Meldungen an andere Systeme zu schicken. Auch die Administration erfolgt möglicherweise von entfernten Clients aus. Das letzte Beispiel kann aber auch verhindert werden, indem eine Administration nur aus dem IDS-Netz heraus erlaubt wird. Als explizite Schutzmaßnahmen kommen beispielsweise Firewalls in Frage. Diese dienen dann lediglich dem Schutz des IDS und sind somit einfacher administrierbar als Firewalls die dem Schutz mehrerer Systeme dienen. Somit sinkt die Wahrscheinlichkeit einer Fehlkonfiguration.

Auch wenn eine andere Aufteilung möglich ist, erscheint es sinnvoll, die Verwaltung des IDS-Netzes (inkl. aller Schutzeinrichtungen) am Landesamt vollständig durch den IDS-Betreiber vornehmen zu lassen. Somit existieren aus Sicht des Managements weniger Schnittstellen zu anderen Rollen, was wiederum einen effektiveren und effizienteren Betrieb des IDS ermöglicht. Diese Annahme wird auch den späteren Ausführungen in Abschnitt 4.3 implizit zugrunde gelegt.

4.2.3 Sensorkalibrierung

Die Thematik der Sensorkalibrierung wurde bereits ausführlich in Kapitel 3.2.3 erörtert. Es wurden zwei unterschiedliche Ansätze vorgestellt, wie die Kalibrierung erfolgen kann.

- Die eine Möglichkeit besteht darin, die Auswertung der Sensordaten nur auf Basis der in der jeweiligen Betriebsumgebung relevanten Signaturen vorzunehmen.
- Eine andere Möglichkeit ist es, die Überwachung eines Sensors mit allen Signaturen vorzunehmen.

Wie als Ergebnis der Diskussion in Kapitel 3.2.3 bereits gezeigt, eignet sich für den sinnvollen Betrieb eines NIDS lediglich die zweite Variante.[6] Somit gilt es die ständige Aktualisierung der IDS-Signaturen sicherzustellen. Näheres hierzu wird in Abschnitt 4.3 beschrieben

[5] Anmerkung: Die Unterbrechung der Stromzufuhr kann somit auch als Angriffsmöglichkeit gegen das IDS selbst genutzt werden.

[6] Auch am LfStaD herrschte zu dieser Thematik anfangs eine unterschiedliche Auffassung

Inwieweit Meldungen im Falle des Landesamtes lediglich protokolliert werden, und wann eine Alarmierung stattfinden soll, kann hier nicht abschließend festgelegt werden. Aufgrund der zuvor gewählten Sensorplatzierung wird hier aber vorgeschlagen zu Beginn alle Meldungen als Alarme weiterzugeben und später gegebenenfalls eine Anpassung vorzunehmen.[7]

4.3 Realisierung der ITIL-Prozesse

In diesem Abschnitt wird gezeigt, wie eine Umsetzung der Szenarien aus Kapitel 3.3 in der Umgebung des LfStaD ausschauen kann. Dabei werden besonders die Unterschiede oder Ergänzungen, die sich im Vergleich zum generischen Konzept ergeben, erläutert. Die Veranschaulichung des Change Management Prozesses erfolgt an einigen beispielhaften Anwendungsfällen, die praxisnah ausgewählt wurden (Abschnitt 4.3.2 und 4.3.3).

4.3.1 Alarmmeldungen in der Einsatzumgebung des Landesamtes für Statistik und Datenverarbeitung

Das Vorgehen im Falle von Alarmmeldungen ist sicherlich eines der wichtigsten Szenarien, die beim Einsatz eines IDS auftreten können. Wie schon mehrfach erwähnt, übernimmt das IDS aus Sicht des Service Managements gegenüber seinen Nutzern die Rolle des Dienstleistungserbringers. Der IDS-Nutzer ist damit der Dienstleistungsempfänger. Kapitel 3.3.1 beschreibt die Besonderheit der IDS-Rolle im Falle von Alarmen. Hier „schlüpft“ das IDS quasi in die Kundenrolle.

Um nun im Bayerischen Behördennetz eine Zuordnung der Rollen hinsichtlich ihrer Dienstleistungsfunktion vornehmen zu können, muss man sich vorab noch einmal die Aufgabenteilung in dieser Einsatzumgebung ins Gedächtnis rufen (siehe Abschnitt 4.1, Tabelle 4.1).

Von der Thematik der Alarmmeldungen und dem damit verbundenen Incident Prozess sind erst einmal nur zwei Rollen betroffen, nämlich der Betreiber des IDS als Dienstleistungserbringer und der Betreiber der Exchange-Umgebung als Dienstleistungsempfänger. Somit wäre eine Prozessdurchlauf streng entlang des in Kapitel 3.3.2 beschriebenen Eskalationsplans möglich. In der Praxis gestaltet sich dieser Fall jedoch etwas komplexer, da nicht zwangsläufig jede Alarmmeldung den Exchange-Server betreffen muss, auch wenn dessen Betreiber der Nutzer des IDS ist. Denkbar wäre auch, dass eine Alarmmeldung auf eine Schwachstelle in der Firewall zurückzuführen ist. Natürlich wäre eine einfache Dienstleistungsbeziehung zwischen IDS-Betreiber und Exchange-Server-Betreiber möglich, da der Exchange-Server-Betreiber die Störung gegebenenfalls an den Firewall-Betreiber weiterleiten kann. Da die Betreiber der einzelnen Systeme aber alle unter dem Dach einer einzigen Organisation – dem LfStaD – vereint sind, ist auch eine weitere Lösung möglich. Diese kann durch eine einfache Anpassung des in Abbildung

[7] Innerhalb des Exchange-Server-Netzes ist die Zahl der Alarmmeldungen wegen der bereits vorgeschalteten Schutzeinrichtungen von Haus aus geringer als außerhalb. Trotzdem anfallende Meldungen sollten somit grundsätzlich mit höherer Priorität behandelt werden, da sie bedeuten, dass die anderen Schutzvorkehrungen nicht die gewünschte Wirkung hatten.

3.12 skizzierten Prozessablaufs beschrieben werden. Dafür ist eine zusätzliche Dienstleistungsvereinbarung notwendig. Diese zusätzliche Dienstleistunsvereinbarung wird zwischen den Betreibern des IDS und dem Betreiber der Firewall geschlossen.[8] Damit existieren formell gesehen zwei Nutzer des IDS. Somit ist eine Weiterleitung von Alarmmeldungen jeweils an den betroffenen Nutzer möglich. Im Landesamt soll diese Weiterleitung, wie im Eskalationsplan vorgeschlagen, durch einen Service Desk erfolgen. Dieser ist zentral organisiert und kann eine Zuordnung auf Basis der vom IDS bereitgestellten Informationen vornehmen.

Abbildung 4.2 verdeutlicht noch einmal die für das Bayerische Behördennetz vorgenommene Anpassung beziehungsweise Erweiterung des Incident-Eskalationsplans.[9]

Es bleibt noch zu klären, was mit den Störungen - resultierend aus Alarmen - passiert, die wiederholt oder mehrfach auftreten, für die also möglicherweise ein eigenes Problem Record eröffnet wird und eine Bearbeitung durch das Problem Management erfolgt. Hier kann ein Prozessablauf in Anlehnung an den Eskalationsplan aus Kapitel 3.3.2 (Abbildung 3.14) ohne große Änderungen übernommen werden, da durch die Zurordnung der Störungen an die Inhaber einer Rolle implizit bereits die Zuordnung des Problems erfolgt ist.

[8] Beim LfStaD soll die Zuständigkeit für den IDS-Betrieb bei der gleichen Abteilung liegen, wie die Zuständigkeit für den Firewall-Betrieb (Abt. Security Dienste), trotzdem müssen zwei verschiedene Rollen unterschieden werden.

[9] Zu der Abbildung ist anzumerken, dass der Service Desk nicht vom IDS-Betreiber geführt wird, sondern wie erwähnt zentral organisiert ist. Hier soll lediglich die Weiterleitung der Alarme an den Service Desk verdeutlicht werden.

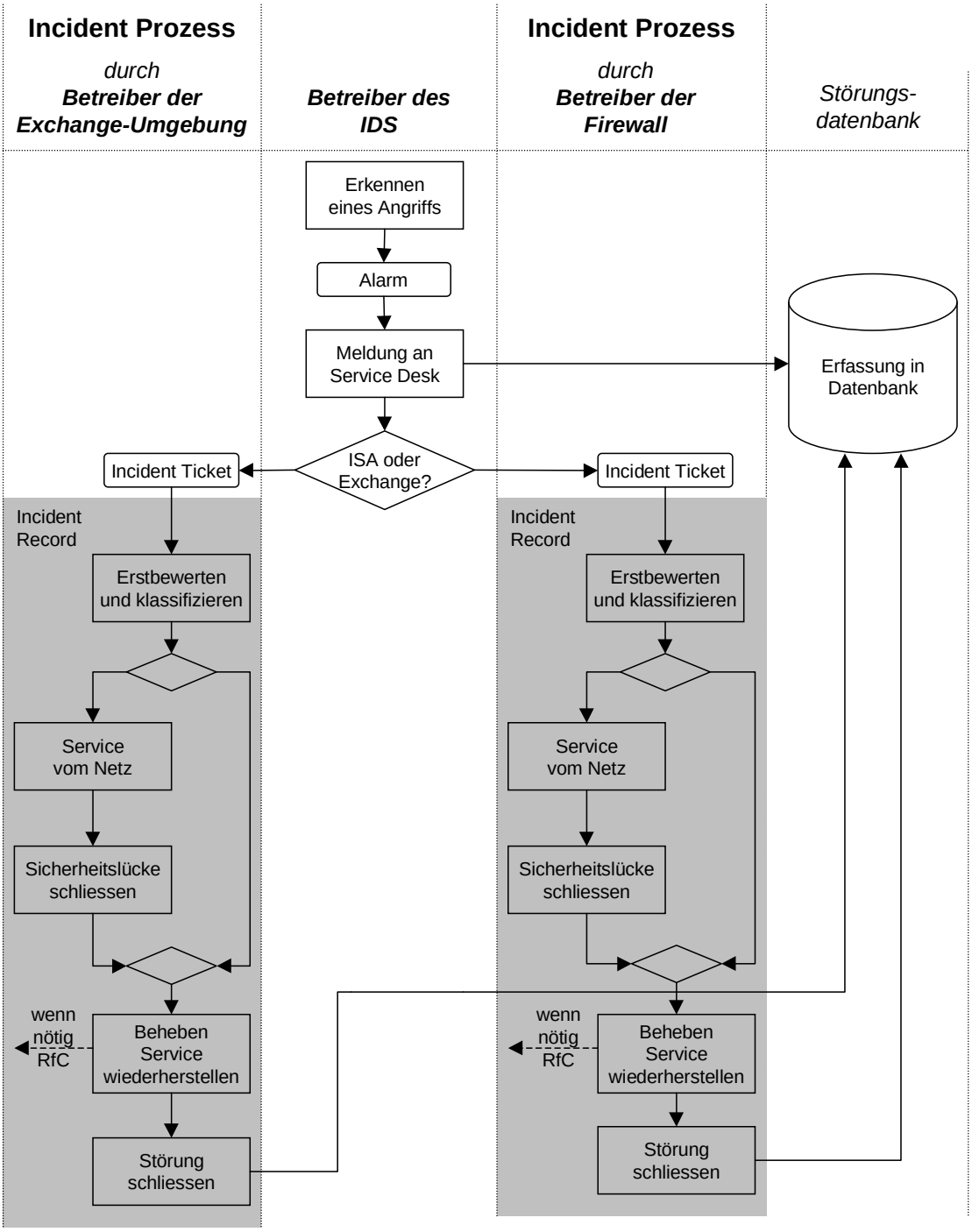


Abbildung 4.2: Alarmplan im LfStaD

4.3.2 Hinzufügen und Entfernen von Sensoren

Auf der Grundlage des in Kapitel 3.3.3 beschriebenen Änderunsprozesses kann nun eine Vorgehensempfehlung für das Hinzufügen beziehungsweise Entfernen von Sensoren gegeben werden.

Als Prämisse wird bei der Beschreibung angenommen, dass der entsprechende RfC durch das Service Level Management erfolgt. Ein Hinzufügen oder Entfernen von Sensoren könnte aufgrund der Vereinbarung neuer oder der Abänderung bestehender SLAs notwendig werden. Der RfC erfolgt dann auf Basis der vereinbarten SLAs. Natürlich können auch Störungen (Incidents) oder Probleme (Problems) dazu führen, dass ein entsprechender RfC gestellt wird. Der Kreis schließt sich hier aber wieder, da auch die Nichterfüllung von SLAs Störungen im Sinne des Incident Managements darstellen.

Eine Prozesskette zum Hinzufügen von Sensoren unter der Voraussetzung, dass ein RfC durch das Service Level Management ausgelöst wurde, lässt sich wie folgt beschreiben[10] (siehe auch Abbildung 4.3):

1. Der Change Manager muss den RfC zum Hinzufügen eines Sensors protokollieren.

2. Es wird eine erste Entscheidung getroffen, ob der RfC sich verwirklichen lässt oder nicht. Auch gegebenenfalls doppelte RfCs werden abgelehnt. Im Falle einer Ablehnung wird das Service Level Management als Antragssteller darüber informiert (inkl. kurzer schriftlicher Begründung)

3. Wird der Wunsch nach einem neuen Sensor akzeptiert, muss der Change klassifiziert werden. Da das Hinzufügen eines Sensors Auswirkungen auf mehrer Bereiche hat (siehe nächster Punkt), wird hier empfohlen eine Einstufung als normalen Change vorzunehmen, was die Einbindung des CAB zur Folge hat.[11]

4. Das CAB wird entsprechend des Änderungswunsches organisiert. In diesem Szenario empfiehlt sich mindestens eine Zusammensetzung aus Vertretern von Change Management, Service Level Management, Netzbetreiber und Kunden. Weitere Prozess-Manager, Spezialisten und Berater können nach Bedarf dazugenommen werden. Der Netzbetreiber des zu überwachenden Systems muss eingebunden werden, da die Integration der Sensoren einen Eingriff in seinen Bereich darstellt.

5. Es erfolgt eine Planung und Bewertung der anstehenden Änderung durch das CAB. Die Einbindung des Service Level Managements (und des Kunden) ist hierbei besonders wichtig, damit der Kunde später das gewünschte Ergebnis erhält.

6. Nach dem Planungsvorgang muss die Freigabe (Autorisierung) der Änderung durch das CAB erfolgen. Bei Nichtfreigabe wird dies dem Service Level Management – als Auslöser des RfC – mitgeteilt.

[10] Das Entfernen eines Sensors geschieht analog

[11] Die Einstufung wurde in Anlehnung an Victor und Günther [ViGu04] vorgenommen. Es werden Routine Change, Normaler Change und Dringender Change unterschieden. Die Einstufung ist nicht verbindlich, die Einbindung des CAB aber in jedem Fall anzuraten

7. Die Freigabe erlaubt die Implementierung des neuen Sensors, nachdem die Einbindung vorher in einem Entwicklungszyklus getestet wurde. In der Entwurfs- und Testphase müssen die Auswirkungen der neuen Sensoren auf den laufenden Betrieb des IDS geprüft werden. Gegebenenfalls müssen Auswirkungen auf bestehende Korrelationen berücksichtigt werden. Die neuen Sensoren müssen als CIs mitsamt ihren Abhängigkeiten von anderen CIs in der CMDB erfasst werden.
8. Nach der Evalution durch das Change Management wird der RfC geschlossen

An dieser Stelle noch einmal der Hinweis, dass alle Entscheidungen im Change Prozess immer auf Grundlage der Informationen in der CMDB erfolgen. Diese Beziehung ist in Abbildung 4.3 als gestrichelte Linie veranschaulicht.

Bei der Realisierung dieses Vorgangs im Bereich der beschriebenen Einsatzumgebung am LfStaD sollten Mitglieder aller in Tabelle 4.1 aufgeführten Rollen in das CAB integriert werden. Dabei wird unterstellt, dass eine Änderung oder Erneuerung der Dienstleistungsvereinbarung[12] jeweils sowohl mit dem Betreiber des Exchange-Servers als auch mit dem Betreiber der ISA-Firewall erfolgt. Dies erscheint in der Praxis sinnvoll, da beide Bereiche vom Einsatz des IDS profitieren können.

[12] Dienstleistungen, die hausintern erfolgen, werden als Operational Level Agreements (OLAs) bezeichnet, im Wesentlichen aber genauso wie SLAs behandelt.

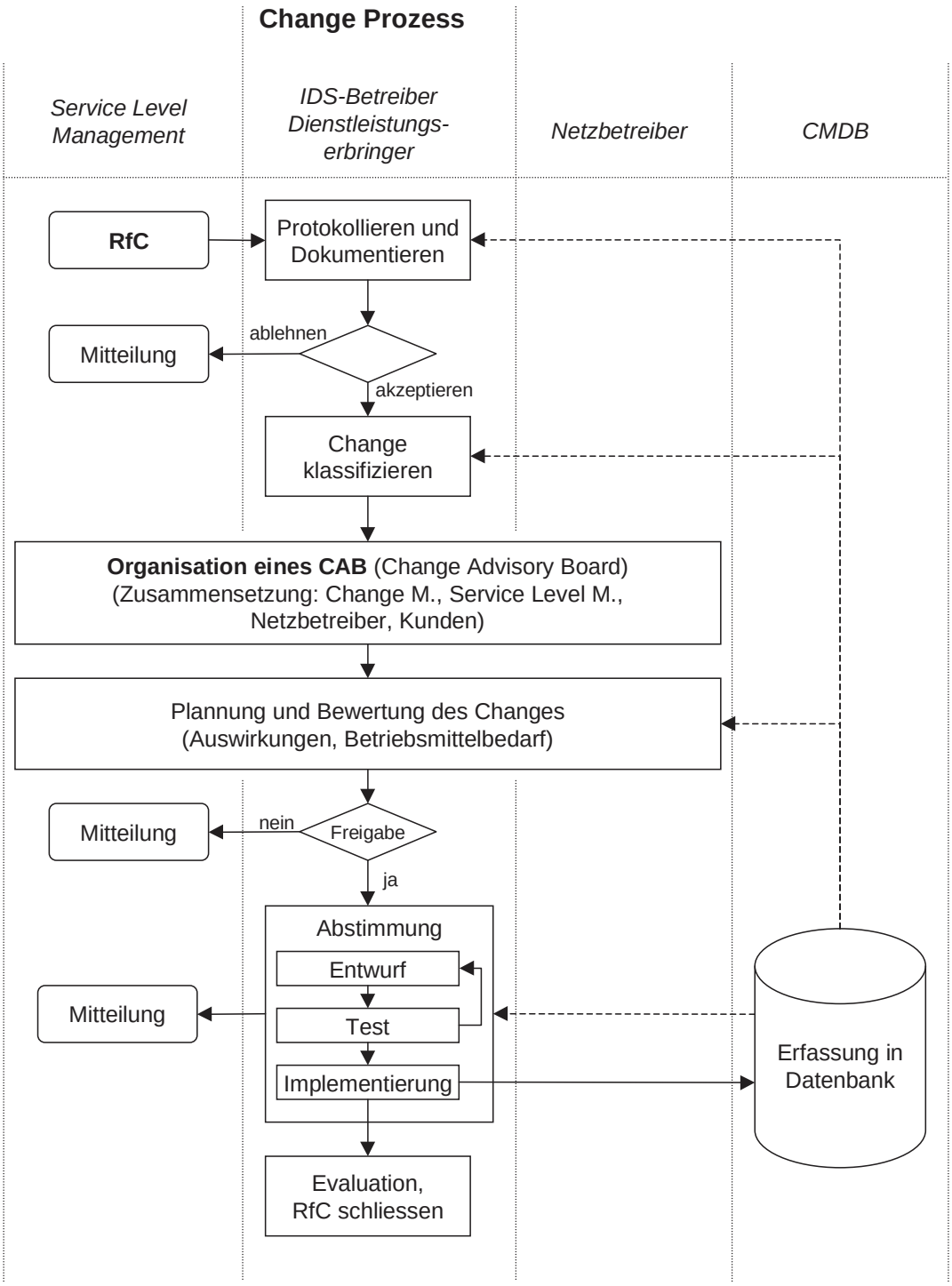


Abbildung 4.3: Hinzufügen und Entfernen von Sensoren basierend auf dem Change Prozess

4.3.3 Einspielen von Signatur- und Softwareupdates

Als Betreiber eines IDS muss das LfStaD sicherstellen, dass sein Service möglichst mit ständig gleichbleibender Güte erbracht wird. Bei der signaturbasierten Analyse heißt das, es muss dafür sorgen, ständig die aktuellsten Signaturen in das System einzuspielen, damit die False-negative-Rate der Alarme nicht wegen veralteter Signaturen ansteigt. Das Einspielen ist dabei vergleichbar mit Signaturupdates bei Virenscannern. Ähnliches gilt für die Einspielung aktueller Sicherheitspatches beziehungsweise Softwareupdates für das IDS selbst.

Damit bei diesem ständig wiederkehrenden Vorgang, der letzlich eine Änderung am System bedeutet, nicht jedesmal der gesamte Change Prozess durchlaufen werden muss, empfiehlt es sich, diesen Vorgang zu standardisieren. Das Change Management bietet hierfür die Möglichkeit sogenannte Standard Changes zu definieren. Standard Changes, die einmal definiert wurden, müssen nicht mehr jedesmal durch das Change Management kontrolliert werden. Sie können als Service Requests im Incident Management klassifiziert werden. Das Anlegen eines neuen Benutzers auf einem System wäre ein Beispiel für einen solchen Standard Change. Einmal als Standard Change definiert, kann mit Hilfe des Incident Prozesses jederzeit ein neuer Benutzer eingerichtet werden.

Im Falle von Signaturupdates kann man sogar noch einen Schritt weiter gehen, indem man den Vorgang automatisiert und beispielsweise stündlich eine Überprüfung auf das Vorhandensein von Updates vornimmt. Welche Zeitspanne zwischen den jeweiligen Updates gewählt werden sollte, hängt vom Hersteller des IDS ab. Er kann Auskunft darüber erteilen in welchen Abständen Signatur- und Softwareupdates herausgegeben werden. Je kürzer die Zeitspanne für Signaturupdates ist, desto besser. Softwareupdates erfolgen in der Regel nur wenn der IDS-Hersteller Fehler in seiner Software beheben will, sodass eine Überprüfung weniger häufig nötig ist.

In einem wichtigen Punkt muss bei der Definition der Prozessabläufe von Signaturupdates und Softwareupdates unterschieden werden. Dies betrifft das Einspielen eventuell fehlerhafter Updates, da die Auswirkungen in einem solchen Fall unterschiedlich sind.

In der betrieblichen Praxis wird ein Signaturupdate (meist automatisch) immer dann in das System eingespielt, wenn neue Signaturen herausgebracht werden. Dabei wird normalerweise keine Überprüfung durchgeführt ob das Update eventuell fehlerhafte Signaturen enthält. Ähnlich wie bei Virenscannern kann auch hier im Einzelfall eine Signatur eingespielt werden, die zu Fehlalarmen führt. Es wäre aber in einem solchen Fall nicht sinnvoll, das gesamte Update rückgängig zu machen, zumal es sich meist um ein Paket von Signaturen handelt, in dem die anderen Signaturen einwandfrei funktionieren. Derartige Fehler werden meist durch den Hersteller der IDS innerhalb kurzer Zeit gelöst, sodass eines der nächsten Signaturupdates das Problem behebt. Es ist also in einem solchen Fall nicht notwendig eine Back-out-Prozedur für den Fall des Scheiterns festzulegen. Dadurch ergibt sich für die Durchführung eines Signaturupdates der in Abbildung 4.4 geschilderte Prozessablauf.

Anders verhält es sich bei Software-Updates. Da hier das Einspielen eines fehlerhaften Updates möglicherweise eine Beeinträchtigung der Dienstqualität (bis hin zum Totalausfall) zur Folge haben kann, sollte eine Back-out-Prozedur festgelegt werden, die im Falle eines Misslingens durchgeführt wird. Das Vorgehen für den Standard Change „Softwareupdate“ wird in Abbildung 4.5 noch einmal veranschaulicht.

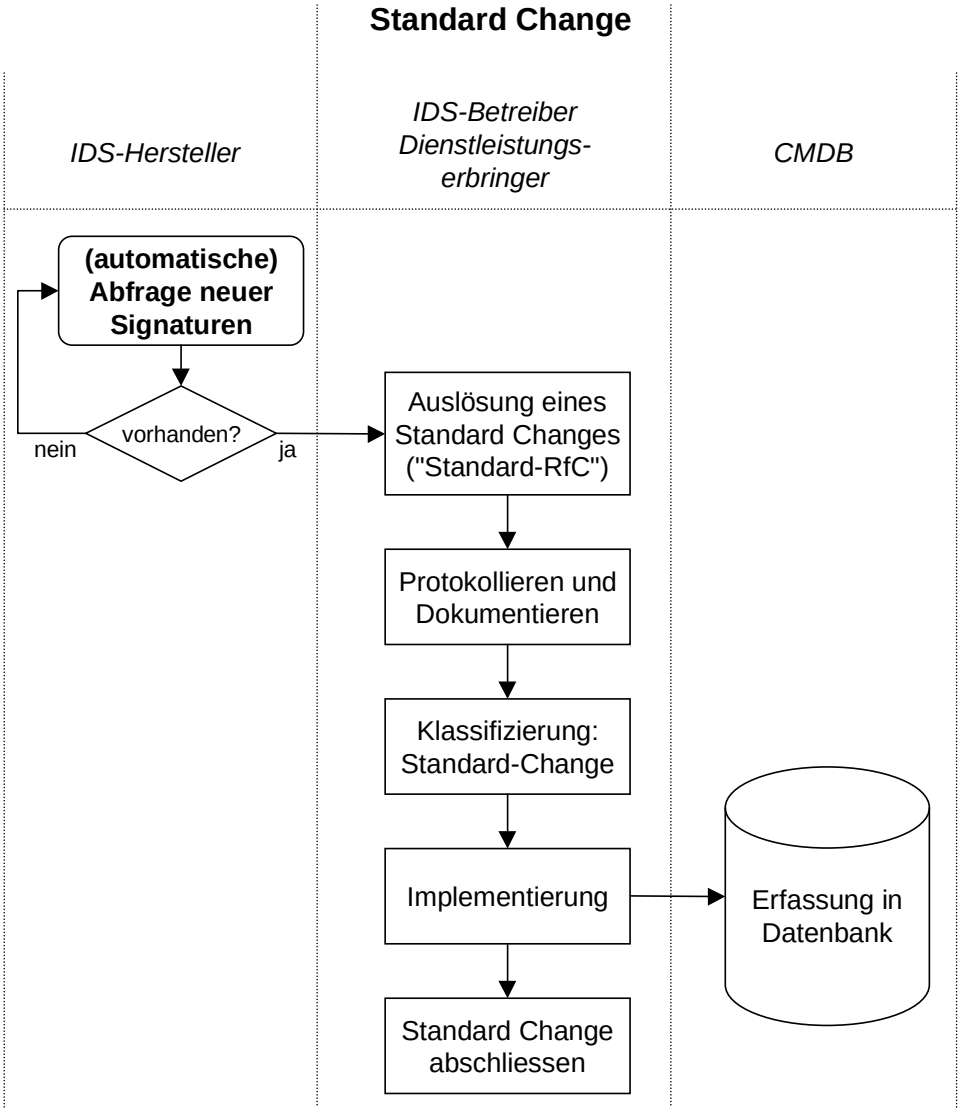


Abbildung 4.4: Einspielen von Signaturupdates basierend auf einem Standard Change

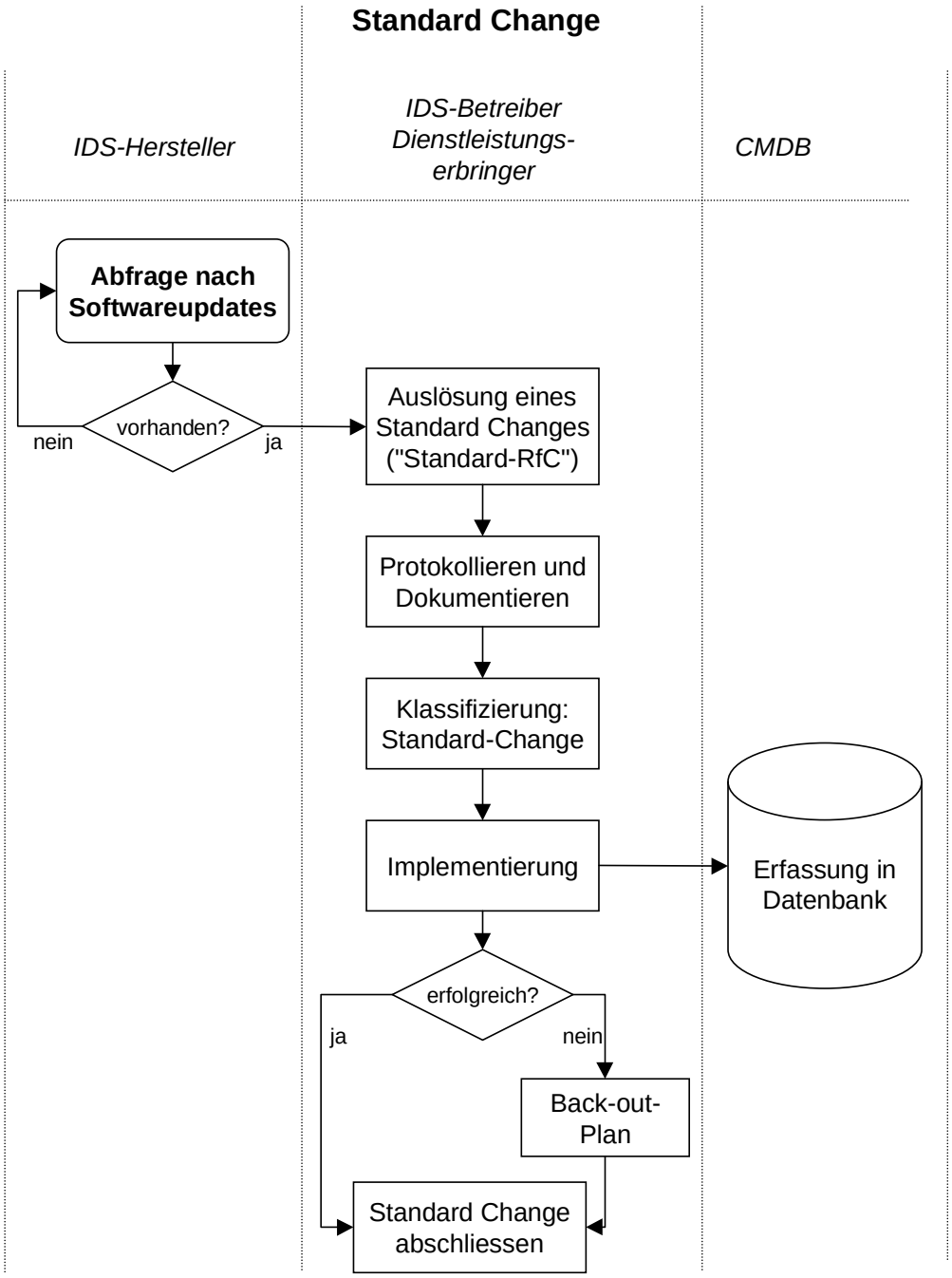


Abbildung 4.5: Einspielen von Softwareupdates basierend auf einem Standard Change

4.4 Auswertung

Die prototypische Umsetzung hat ergeben, dass das in Kapitel 3 entwickelte Managementkonzept für einen praktischen Einsatz geeignet ist. Alle Punkte des Konzepts konnten realisiert werden. Dabei mussten aber an einigen Stellen die Besonderheiten am LfStaD berücksichtigt werden. Sie sollen nachfolgend noch einmal kurz zusammengefasst werden.

Die Platzierung der Sensoren wurde so vorgenommen, dass die Anzahl möglicher Alarmmeldungen von vorneherein beschränkt wird. Diese Beschränkung erfolgt dabei durch die ausschließliche Überwachung des Exchange-Server-Teilnetzes. Sensoren außerhalb dieses Teilnetzes wurden in der ersten Ausbaustufe nicht vorgesehen. Dadurch kann die Anzahl an auflaufenden Alarmmeldungen wirksam reduziert werden, da nur Angriffe gemeldet werden, die tatsächlich bis in das betrachtete Teilnetz durchdringen. Dabei schränkt diese Maßnahme zur Reduzierung der Alarmmeldungen die Wirksamkeit des IDS nicht von vorneherein ein (vgl. Kapitel 3.2.1). Eine späterer Ausbau ist jederzeit möglich.

Schwierigkeiten ergaben sich bei der Umsetzung des in Kapitel 3.3.2 vorgeschlagenen Eskalationsplans auf Basis des Incident Managements. Bei der prototypischen Umsetzung stellte sich heraus, dass Alarmmeldungen in der betrachteten Umgebung zwar auf Angriffe gegen den Exchange Server zurückzuführen sind, die zugrundeliegende Störung (Sicherheitslücke) aber nicht zwangsläufig beim Exchange Server zu suchen sein muss. Es wäre auch eine Schwachstelle in der Firewall denkbar. Diese Problematik kann durch eine zweite Dienstleistungsvereinbarung zwischen IDS-Betreiber (Dienstleistungserbringer) und Firewall-Betreiber (Dienstleistungsempfänger) gelöst werden. Damit ist eine Weiterleitung von Alarmmeldungen, die einer möglichen Störung der Firewall zuzuordnen sind, direkt an den Betreiber der Firewall möglich. Es bleibt somit festzuhalten: *Alarmmeldungen, die aus einem möglichen Angriff auf ein bestimmtes System resultieren, führen zu einer Störungsbearbeitung (Eröffnung eines Incident Records). Die Störungsbearbeitung muss aber nicht zwangsläufig durch das von dem Angriff betroffene System erfolgen.*

Für den praktischen Einsatz eines IDS am LfStaD wurden noch zwei Standard Changes zum Einspielen von Signatur- beziehungsweise Softwareupdates definiert, die eine einfache Handhabung dieser Vorgänge auch nach den Vorgaben der ITIL erlauben. Normalerweise würden diese Änderungen der vollen Kontrolle des Change Mangements unterliegen, was besonders im Falle von Signaturupdates mit einem erheblichen Aufwand verbunden wäre, da diese gegebenenfalls mehrmals täglich notwendig sind. Die Definition von Standard Changes ermöglicht hier eine starke Vereinfachung. Im Falle von Signaturupdates ist sogar eine Automatisierung möglich.

5 Zusammenfassung und Ausblick

In Abschnitt 5.1 werden die letzten Kapitel noch einmal überblickartig zusammengefasst und die wesentlichen Ergebnisse aufgezeigt. Anschließend erfolgt in Abschnitt 5.2 ein Ausblick zu Ansatzpunkten für mögliche Folgearbeiten, die sich im Verlauf dieser Arbeit ergeben haben.

5.1 Zusammenfassung

In den zurückliegenden Kapiteln wurde ein Managementkonzept entwickelt, welches den effizienten Einsatz von netzbasierten Intrusion Detection Systemen erleichtert. Ziel war es das Konzept generisch zu formulieren, um eine produkt- und umgebungsunabhängige Verwendung des Konzepts zu ermöglichen.

In Kapitel 2 wurden die notwendigen Grundlagen gelegt. Zuerst erfolgte eine Einführung auf dem Gebiet der Intrusion Detection Systeme. Im Hinblick auf das spätere Managementkonzept wurde bereits hier eine klare Aufteilung von netzbasierten Intrusion Detection Systemen in einzelne Teilkomponenten vorgenommen, da in der Literatur häufig unterschiedliche Begriffe für die gleiche Komponente oder gleiche Begriffe für verschiedene Komponenten verwendet werden. Anschließend wurde eine Einführung im Bereich des Managements vernetzter Systeme vorgenommen. Anhand der Teilmodelle auf denen eine Vielzahl von Managementarchitekturen aufbauen, erfolgte ein Überblick über den Gesamtkomplex des IT-Managements aus technischer Sicht. Anschließend wurde mit dem ITSM und der ITIL ein Best Practice Framework vorgestellt, welches die technischen Aspekte der Teilmodelle – insbesondere die im Funktionsmodell beschriebenen Funktionsbereiche – aufgreift, dabei aber gleichzeitig die organisatorischen Gesichtspunkte des Managements nicht aus den Augen verliert, da in der ITIL der Dienstleistungsgedanke im Vordergrund steht.

Auf diesen Grundlagen baut Kapitel 3 auf. Im ersten Teil ist es gelungen, die verschiedenen Möglichkeiten zur Anordnung der einzelnen Komponenten, aus denen sich ein IDS zusammensetzt, eingehend zu erörtern und darauf aufbauend konkrete Vorschläge zur praktischen Umsetzung zu machen. Insbesondere beinhaltet dies ein strukturiertes Vorgehen bei der Platzierung der IDS-Sensoren. Auch für die Platzierung der übrigen IDS-Komponenten wurden verschiedene Vorgehensweisen diskutiert, und es konnte eine Empfehlung ausgesprochen werden. Nach der Diskussion zur Schaffung einer geeigneten IDS-Infrastruktur beschäftigte sich der zweite Teil des Kapitels mit dem laufenden Betrieb. Hier erfolgte zuerst eine Einordnung des IDS im Service Management. Ausgangsfrage für diese Einordnung war, welche Rollen ein IDS in einer Dienstleistungsbeziehung einnehmen kann. Anschllließend konnten, basierend auf unterschiedlichen Szenarien, mit Hilfe der ITIL strukturierte Prozessabläufe entwickelt werden. Der Schwerpunkt wurde hier im wesentlich auf den Service Support betreffende Aspekte gelegt.

Kapitel 4 beschreibt eine mögliche Umsetzung des Konzepts in einem Teilbereich des Landesamtes für Statistik und Datenverarbeitung, welches als Betreiber des Bayerischen Behördennetzes fungiert. Aufgrund der hohen Sicherheitsanforderungen die für Teile des Bayerischen Behördennetzes gelten, ist der tatsächliche Nutzen, der durch den Einsatz eines IDS entsteht, sehr groß. Bei der Umsetzung des Konzepts hat sich gezeigt, dass eine Anwendung im praktischen Einsatz durchaus realisierbar ist. Es fanden sich aber auch einige Aspekte, denen bei einer praktischen Realisierung besondere Aufmerksamkeit zuteil werden muss, und wo eventuell eine Anpassung auf die jeweilige Einsatzumgebung notwendig ist.

Als Ergebnis lässt sich festhalten, dass mit der ITIL ein Leitfaden bereitgestellt wird, der ein effektives und effizientes Management vernetzter Systeme unterstützt und somit auch eine Anwendung der Best-Practice-Ansätze beim Betrieb eines IDS möglich ist. Die Arbeit hat gezeigt, dass die in der ITIL beschriebenen Prozesse des Service Support sich auf konkrete Szenarien aus dem laufenden IDS-Betrieb umsetzen lassen und flexibel genug sind, um die Anpassung an eine vorgegebene Einsatzumgebung durchführen zu können.

5.2 Ausblick

Wie im vorigen Abschnitt bereits erwähnt, wurde in der vorliegenden Arbeit besonders dem Bereich Service Support große Aufmerksamkeit zuteil. Um das vorgestellte Managementkonzept zu vervollständigen, könnten die anderen in der ITIL definierten Prozesse integriert werden. Schnittstellen zum Bereich Service Delivery wurden teilweise gezeigt, wobei hier kein Anspruch auf Vollständigkeit erhoben wird. Eine eingehendere Betrachtung dieses Bereichs könnte zu neuen Erkenntnissen führen, was die Gestaltung der hier beschriebenen Prozessabläufe betrifft.

In der Arbeit wurde wiederholt darauf hingewiesen, dass das Configuration Management eine außerordentlich wichtige Funktion zur Unterstützung der anderen Managementprozesse hat (vgl. hierzu auch Abbildung 2.5 und 2.6 in Kapitel 2.2.2). Es hat die wichtige Aufgabe, alle relevanten Informationen über die IT-Infrastruktur eines Unternehmens in der CMDB zu erfassen. Dazu gehören auch die Abhängigkeiten der IT-Komponenten untereinander. Die Effizienz des Managements steht und fällt mit den zur Verfügung gestellten Informationen. Für das ITSM bedeutet dies, es kann nur so gut sein, wie die Datenbasis, die ihm zugrunde liegt. In Kapitel 3.3.3 wurde davon ausgegangen, dass eine entsprechende Basis vorhanden ist. Die CMDB und ihre Bedeutung wurden vorgestellt. Die Entwicklung eines Datenbankschemas für eine solche CMDB gestaltet sich sehr komplex, sodass sie nicht Teil dieser Arbeit war. Insbesondere steigt die Komplexität, wenn das Abhängigkeitsgeflechts der CIs untereinander sehr dicht ist. Der Einsatz generischer Datenbankschemen, die eine flexible Anpassung an die jeweilige zu erfassende IT-Umgebung zulassen, wäre denkbar. Ansätze dazu finden sich zum Beispiel bei Jäger [Jaeg05].

In den letzten Jahren ist der Trend zu einer stetig komplexer werdenden IT-Infrastruktur zu beobachten, da die Unternehmen diese ständig ausbauen, um ihre Geschäftsprozesse durch den Einsatz der IT noch besser zu unterstützen. Dadurch ergibt sich das Problem, dass zwar einerseits die Abwicklung der Geschäftsprozesse erleichtert wird, andererseits aber der Pflegeauf-

wand der IT-Systeme erheblich zunimmt. Damit erhöht sich natürlich auch der Aufwand zum Management dieser Systeme. Es besteht die Gefahr, dass die durch IT-Unterstützung gewonnenen Vorteile durch den hohen Pflegeaufwand wieder verloren gehen, und somit die Effektivität und Effizienz des IT-Managements wieder sinkt. Hier gilt es nach geeigneten Lösungen zu suchen, um dieser Entwicklung gegenzusteuern. Ansätze könnten beispielsweise darin bestehen, die Pflege der CMDB stärker zu automatisieren. Dieser Gedanke widerspricht jedoch auf den ersten Blick den Vorstellungen der ITIL, alle Änderungen kontrolliert durchzuführen. Da die ITIL selbst einem ständigen Verbesserungsprozess unterliegt, erfolgen hier in den nächsten Jahren eventuell aber entsprechende Anpassungen. Schließlich handelt es sich bei der ITIL um ein Best Practice Framework.

Abkürzungsverzeichnis

ARPANET Netzwerk der Advanced Research Projects Agency

BSI Bundesamt für Sicherheit in der Informationstechnik

BYBN Bayerisches Behördennetz

CAB Change Advisory Board

CAB/EC Change Advisory Board Emergency Committee

CCTA Central Computer and Telecommunication Agency

CERT Computer Emergency Response Team

CI Configuration Item

CMDB Central Computer and Telecommunication Agency

CORBA Common Object Request Broker Architecture

DMI Desktop Management Interface

DMZ Demilitarisierte Zone

DNS Domain Name Service

ELSTER Elektronische Steuererklärung

HIDS Host Intrusion Detection System

IDS Intrusion Detection System

IIS Internet Information Server

IP Internet Protocol

IRS Intrusion Response System

ISA Internet Security and Acceleration

ISO International Organization for Standardization

IT Information Technology

ITIL Information Technology Infrastructure Library

ITSM Information Technology Service Management

itSMF Information Technology Service Management Forum

ITU International Telecommunication Union

ITU-T Telecommunication Standardization Bureau innerhalb der ITU

LfStaD Landesamt für Statistik und Datenverarbeitung

MIB Managementinformationsbasis

MO Managementobjekte

MOC Managementobjektklasse

MOF Microsoft Operations Framework

NIDS Network Intrusion Detection System

OGC Office of Government Commerce

RfC Request for Change

SLA Service Level Agreement

SLM Service Level Management

SNMP Simple Network Management Protocol

Tap Test Access Port

TCP Transport Control Protocol

TMN Telecommunications Management Network

VPN Virtual Private Network

Literaturverzeichnis

[Bitt05] BITTERICH, C.: *Klassifizierung und Modellierung von Dienstmanagement-Informationen – ein Design-Pattern basierter Ansatz*. Diplomarbeit, Ludwig-Maximilians-Universität München, Dezember 2005.

[BSI02a] *BSI-Leitfaden für die Einführung von Intrusion-Detection-Systemen*. Studie im Auftrag des Bundesamtes für Informationstechnik (BSI), http://www.bsi.bund.de/literat/studien/ids02/index.htm .

[BSI02b] *ITIL und Informationssicherheit: Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management*. Studie im Auftrag des Bundesamtes für Informationstechnik (BSI), http://www.bsi.bund.de/literat/studien/ITinf/itil.pdf .

[CERT] *Deutscher CERT-Verbund*, http://www.cert-verbund.de/ .

[Ecke03] ECKERT, C.: *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. Oldenbourg Verlag, München, 2. Auflage, 2003.

[Elsa05] ELSÄSSER, W.: *ITIL einführen und umsetzen: Leitfaden für effizientes IT-Management durch Prozessorientierung*. Hanser Verlag, München, 2005.

[Feld05] V. D. GENTSCHEN FELDE, N. O.: *Leistungsfähigkeit von Anomalieerkennungsverfahren in domänenübergreifenden Meta-IDS*. Diplomarbeit, Rheinische Friedrich-Wilhelms-Universität Bonn, März 2005.

[GeNUA] GENUA MBH: *GeNUDetect 2.1 – Manual*, März 2005.

[Gerl04] GERLONI, H., B. OBERHAITZINGER, H. REISER und J. PLATE: *Praxisbuch – Sicherheit für Linux-Server und -Netze*. Hanser Verlag, München, 2004.

[HAN99] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integriertes Management vernetzter Systeme: Konzepte, Architekturen und deren betrieblicher Einsatz*. dpunkt-Verlag, ISBN 3-932588-16-9, Heidelberg, 1999. 607 S.

[Heil97] HEILER, K.: *Eine Methodik zur Modellierung von Konfigurationsvorgängen für Szenarien im Netz- und Systemmanagement*. Dissertation, Technische Universität München, Juni 1997.

[Ilio05] ILIOPOULOS, S.: *Evaluation von Intrusion Detection Systemen für das Bayerische Behördennetz*. Diplomarbeit, Ludwig-Maximilians-Universität München, Juli 2005, http://www.mnm-team.org/pub/Diplomarbeiten/ilio05/ .

[ITSM00] PERSEO CONSULT (Herausgeber): *IT Service Management – Die IT Infrastructure Library (Pocket Guide)*. Perseo Consult, Basel, 2000.

[ITSM02] BON, J. V., G. KEMMERLING und D. PONDMAN (Herausgeber): *IT-Service Management, an Introduction*. Van Haren Publishing, 2002.

[itSMF] *IT Service Management Forum*, http://www.itsmf.de/ .

[Jaeg05] JÄGER, J.: *Entwicklung eines Toolkonzeptes für die Unterstützung der ITIL Service Support Prozesse*. Diplomarbeit, Technische Universität München, Januar 2005.

[Koen03] KÖNIG, H.: *Intrusion Detection – Möglichkeiten und Probleme einer wirksamen Erkennung sicherheitsgefährdender Aktionen im Internet*. Vorlesungsunterlagen, 2003, http://www-rnks.informatik.tu-cottbus.de/ .

[Krae03] KRÄMER, R.: *Management verteilter Systeme*. Vorlesungsunterlagen, 2003, http://www.ihp-ffo.de/systems/ .

[Lang01] LANGER, M.: *Konzeption und Anwendung einer Customer Service Management Architektur*. Dissertation, Technische Universität München, März 2001.

[MSMOF] *Microsoft Operations Framework*, http://www.microsoft.com/mof/ .

[OGC00] OFFICE OF GOVERNMENT COMMERCE (OGC) (Herausgeber): *ITIL – Service Support*. The Stationery Office (TSO), 2000.

[OGC01] OFFICE OF GOVERNMENT COMMERCE (OGC) (Herausgeber): *ITIL – Service Delivery*. The Stationery Office (TSO), 2001.

[OGC05] OFFICE OF GOVERNMENT COMMERCE (OGC) (Herausgeber): *ITIL – Introduction to ITIL*. The Stationery Office (TSO), 2005.

[Sage05] SAGER, F.: *Konzeptentwicklung für Configuration Management in einem Rechenzentrum nach ITIL und MOF*. Diplomarbeit, Technische Universität München, März 2005.

[Somm04] SOMMER, J.: *IT-Servicemanagement mit ITIL und MOF*. mitp-Verlag, Bonn, 2004.

[Spen03] SPENNEBERG, R.: *Intrusion Detection für Linux-Server: Mit Open Source-Tools Angriffe erkennen und analysieren*. Markt+Technik Verlag, München, 2003.

[Szak04] SZAKATS, D.: *IT Maturity and Sourcing Strategies*. Diplomarbeit, Universität Zürich, März 2004.

[Tane03] TANENBAUM, A. S.: *Computernetzwerke*. Pearson Studium, München, 4. Auflage, 2003.

[Utim98] *KES-Utimaco-Sicherheitsstudie 1998*, 1998.

[ViGu04] VICTOR, F. und H. GÜNTHER: *Optimiertes IT-Management mit ITIL*. Vieweg Verlag, Wiesbaden, 2004.

[Wiki] *Wikipedia – Die Freie Enzyklopädie*, http://de.wikipedia.org/ .