JOHANNES KEPLER
UNIVERSITÄT LINZ
Netzwerk für Forschung, Lehre und Praxis



# Network-Monitoring im Netzwerk einer Tageszeitung

Eingereicht von:

*Peter Donko, 0155063*

Angefertigt am:

*Institut für Informationsverarbeitung und Mikroprozessortechnik*

Betreuung:

*o. Prof. Jörg Mühlbacher*

*Dipl.-Ing. Rudolf Hörmanseder*

*Linz, Juni 2008*

# Zusammenfassung

Die Arbeit behandelt das Thema “Network-Monitoring“. Sie ist in drei Teile untergliedert, die inhaltlich folgendermaßen aufgeteilt sind.

Im ersten Abschnitt der Arbeit wird das Thema auf konzeptioneller Ebene betrachtet. Der Nutzen von Network-Monitoring wird ebenso behandelt, wie die grundsätzlichen Strategien die zu einer effektiven Netzwerküberwachung führen (z.B. Data Polling/Data Listening). Weiters wird eine systematische Herangehensweise zur Implementierung einer umfassenden Netzwerküberwachung von komplexen Computernetzwerken vorgestellt.

Im zweiten Teil der Diplomarbeit wird bereits auf den praktischen Aspekt dieser Arbeit Bezug genommen und die vorgestellte Vorgehensweise anhand eines praktischen Beispiels umgesetzt. Anfangs werden die Anforderungen, die von der Geschäftsführung vorgegeben wurden, wiedergegeben, um daraus im Anschluss ein Anforderungsprofil für das Projekt zu erstellen. Anhand dieser Spezifikation werden relevante Tools zur Netzwerküberwachung miteinander verglichen. Nach einer umfassenden Evaluierung der zwei am besten geeigneten Programme wird die tatsächliche Umsetzung einer Network-Monitoring Lösung mit dem gewählten Tool skizziert.

Im letzten Teil der Arbeit wird eine integrative Sichtweise des Themas vorgestellt. Hier wird eine Verbindung mit Aspekten aus der Managementlehre hergestellt. Möglichkeiten werden aufgezeigt, wie Network-Monitoring-Systeme auch als Instrumente der Unternehmensführung eingesetzt werden können.

# Abstract

This master thesis deals with the topic “Network-Monitoring“. It is divided into three parts with the following content.

The first part explains the theoretical background of this paper and delivers a process model for the implementation of a network-monitoring system for a computer network. In the second part the discussed process model is used to create a network-monitoring environment for the network of a daily newspaper. This part covers the whole process, from network analysis to job specification and finally the configuration of a chosen tool. The last part will give an integrative approach towards network-monitoring. It shows that such systems can also be used by the management of a company for risk management and the strategic process.

# Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Masterarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Des weiteren versichere ich, dass ich diese Masterarbeit weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Datum, Ort Unterschrift

# Inhaltsverzeichnis

<

# Abbildungsverzeichnis

# Tabellenverzeichnis

# 1 Einleitung

Am Anfang dieser Arbeit wird die Motivation für das vorliegende Projekt aufgezeigt. Dies wird zuerst auf einer allgemeinen Basis durchgeführt, um daraufhin auf die spezielle Situation einer konkreten Tageszeitung einzugehen. Im zweiten Teil der Einleitung wird eine Abgrenzung des Themenbereichs “Network-Monitoring“ zum weiter gefassten Thema des Network-Managements gezogen.

## 1.1 Motivation

Die Veränderungen, die in der Vergangenheit in Organisationen zu erkennen waren, ergeben neben generellen strukturellen Modifikationen auch eine Vielzahl neuer Anforderungen an die IT eines Unternehmens (Wojtecki Jr & Peters, 2000). In vielen Bereichen der Wirtschaft verlassen sich Firmen schon seit Jahrzehnten auf die korrekte Funktionsweise der IT-Infrastruktur. Systemausfälle verursachen zum Beispiel im Finanzsektor spätestens seit den 80er Jahren des letzten Jahrhunderts schwerwiegende Konsequenzen, und haben dadurch eine starke Beachtung erfahren (BIS IT-Task-Force, 1989). Das Voranschreiten der Unterstützung von Arbeitsprozessen durch Computersysteme veranlasst nun auch Klein- und Mittelbetriebe zu einer Absicherung und kontinuierlichen Überwachung der IT-Infrastruktur. Die in dieser Arbeit behandelte Tageszeitung ist ebenfalls zu dem Schluss gekommen, dass eine umfassende Überwachung des Computernetzwerks benötigt wird.

### 1.1.1 Aufgabenstellung im Umfeld einer Tageszeitung

Um die hohe Aktualität dieser Tageszeitung zu gewährleisten, wird der Redaktionsschluss auf einen möglichst späten Zeitpunkt hinausgeschoben. Daraus ergibt sich ein geringer zeitlicher Rahmen für das Finalisieren und den Druck der Zeitung. Aus diesem Grund gibt es besonders zeitkritische Prozesse, die im Entstehungsprozess dieser Tageszeitung überwacht werden müssen. Da die Zeitung dieses Projekts nicht am Standort der Redaktion gedruckt wird, ist die

funktionierende Verbindung zur Druckerei für die Übermittlung der Daten ebenfalls von großer Bedeutung.

Ein weiterer Punkt ist die Dezentralisierung der redaktionellen Arbeit dieser Tageszeitung. Um aktuelle Berichte verfassen zu können, werden Journalisten an den jeweiligen Ort des Geschehens entsendet. Die vor Ort verfassten Artikel werden an die Zentrale übermittelt, welche diese zu einer Zeitung zusammenfügt. Da aus Effizienzgründen möglichst viele Arbeitsschritte automatisiert ablaufen sollen, wurde ein Redaktionssystem namens Object News 2 (ON2) auf Client-Server Basis entwickelt.

Die beiden genannten Aspekte erklären den Bedarf nach einer hohen Verfügbarkeit der IT dieser Tageszeitung. Daraus leitet sich unter anderem die Forderung nach einer umfassenden Netzwerküberwachung zur Sicherstellung der korrekten Funktionsweise der Netzwerkinfrastruktur ab.

## 1.2 Begriffsabgrenzung

Netzwerküberwachung ist ein Teil des Netzwerk-Management. Dieses wurde von der International Standards Organization (ISO) in der Standardfamilie 10164 definiert (ISO 10164, 1993). Darin werden fünf Teilbereiche des Managements von Netzwerken nach dem ISO/OSI-7-Schichtmodell (Zimmermann, 1980) beschrieben:

| | |
|---|---|
| Fault-Management | Fehlererkennung, -behebung |
| Configuration-Management | Steuerung der IT-Infrastruktur |
| Accounting-Management | Kosten für die Benutzung der IT-Ressourcen |
| Performance-Management | Ermittlung der Effizienz des Computernetzwerks |
| Security-Management | Umsetzung von Sicherheitsrichtlinien |

**Tabelle 1: Teilbereiche des Network-Managements**

Die Netzwerküberwachung bildet einen Teil des Fault-Management und umfasst folgende Bereiche (Tabakoff, 2006):

- Überwachung von Ereignisprotokollen
- Identifikation von Fehlern

- Benachrichtigung festgelegter Empfänger im Fehlerfall

Beachtenswert ist hierbei, dass Network-Monitoring keine Fehlerbehebung umfasst. Somit wird nur die Benachrichtigung über aufgetretene Fehler angeführt.

Nachdem nun der Aufgabenbereich der Netzwerküberwachung abgegrenzt ist, behandelt das nächste Kapitel die Konzepte dieses Bereichs des Netzwerk-Managements.

# 2 Allgemeine Grundlagen des Network-Monitoring

Bevor auf die praktische Umsetzung des Projekts eingegangen wird, werden die konzeptionellen Grundlagen für eine umfassende Netzwerküberwachung vorgestellt.

Zuerst werden der Aufbau und die einzelnen Teile eines Network-Monitoring-Systems erläutert. Im darauffolgenden Abschnitt wird auf die verschiedenen Techniken von Network-Monitoring-Systemen eingegangen. Bevor ein allgemeines Vorgehensmodell zur Erstellung einer Network-Monitoring Umgebung gezeigt wird, werden ausgewählte Protokolle beschrieben, die im Rahmen dieser Thematik von Bedeutung sind.

## 2.1 Aufbau eines Network-Monitoring-Systems

Um die in Abschnitt 1.2 erwähnte Funktionalität bereitzustellen, bestehen Monitoring-Systeme im Allgemeinen aus vier Komponenten (Stallings, 1998):

| Komponente | Funktion |
|---|---|
| | |
| Manager | Verwaltung der Abfragen |
| Netzwerkelement | zu überwachende Einheit |
| Agent | Realisierung der Überwachungsfunktion auf einem Netzwerkelement |
| Monitoring-Programm | Speicherung und Darstellung der gesammelten Informationen |

**Tabelle 2: Komponenten eines Montoring Systems**

Die Netzwerkkomponente besitzt - gemäß dem Konzept von Stalling - zu überwachende Eigenschaften. Der Agent überprüft diese, wenn er dazu aufgefordert wird. Die Ergebnisse werden vom Agent über den Manager an das Monitoring-Programm weitergeleitet. Dieses stellt die Daten dar und schickt eine Nachricht an zuvor festgelegte Empfänger.

Die Zusammenarbeit der einzelnen Komponenten wird in Abbildung 1 dargestellt. Die schattierten Umrahmungen deuten an, dass der Agent und die Netzwerkkomponenten, sowie der

Manager und das Monitoring-Programm in den meisten Fällen auf jeweils einem System implementiert sind (Stallings, 1998).

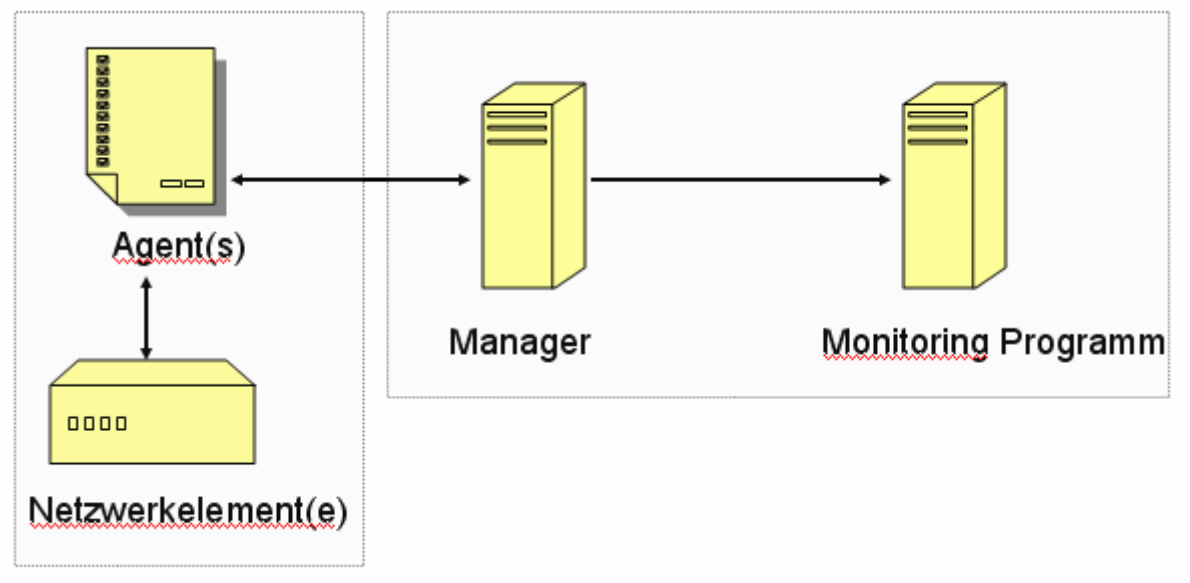


**Abbildung 1: Aufbau eines Nework-Monitoring-Systems**

## 2.2 Methoden

Der Auslöser oder Trigger für die Abfrage des zu überwachenden Wertes durch den Agenten kann an zwei Punkten im Überwachungssystem positioniert sein. Deswegen können zwei Verfahren zur Netzwerküberwachung unterschieden werden: aktives und passives Network-Monitoring(Chiu & Sudama, 1992). Diese Verfahren werden in der Folge erklärt.

### 2.2.1 Aktives Network-Monitoring

Das aktive Network-Monitoring ist dadurch gekennzeichnet, dass die Abfrage eines Wertes durch den Manager des Systems ausgelöst wird. Dieser sendet an den Agenten die Aufforderung, den Wert abzufragen. Der Agent führt die gewünschte Aktion aus und sendet das Ergebnis an den Manager (Hall, 2003).

Der Informationsfluss dieses Konzepts wird in Abbildung 2 verdeutlicht.

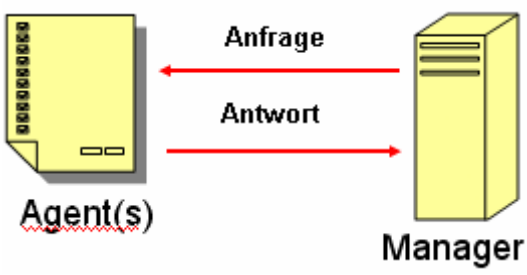


**Abbildung 2: aktives Network-Monitoring**

### *Vorteile*

Ein Vorteil dieses Systems liegt in der zentralen Steuerung der Überwachung. Sowohl periodische als auch außerplanmäßige Abfragen sind komfortabel über den Manager als zentralen Punkt zu realisieren. Auch Verbindungsunterbrechung können hier durch den Manager sofort erkannt werden (Hall, 2003).

### *Nachteile*

Negative Aspekte dieser Vorgehensweise sind eine erhöhte Netzlast durch periodische Abfragen und daraus resultierende Beeinflussung der ermittelten Werte. Periodische Abfragen sind das Grundgerüst einer aktiven Netzwerküberwachung. Diese kontinuierlichen Abfragen erhöhen den Verkehr in einem Netzwerk. Oft wird dies nicht beachtet, was zu unverständlichen Ergebnissen bei der Überwachung führen kann. Im schlimmsten Fall werden die abgefragten Werte selbst durch diese Vorgehensweise stark verändert (Breitbart et al., 2004).

## 2.2.2 Passives Network-Monitoring

Im Gegensatz zur aktiven Netzwerküberwachung werden in der passiven Variante keine Werte vom Manager abgefragt. In diesem Konzept wird von den Agenten entschieden, zu welchem Zeitpunkt die benötigten Daten abgefragt und an den Manager gesendet werden. Dieser hat die Aufgabe, die Daten zu empfangen und an das Monitoring-System weiterzuleiten (Hall, 2003).

Abbildung 3 verdeutlicht das Konzept des passiven Network-Monitoring.

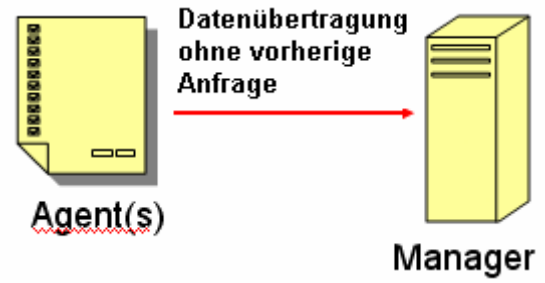


**Abbildung 3: passives Network-Monitoring**

### *Vorteile*

Im Vergleich zur aktiven Netzwerküberwachung ist der Vorteil der passiven Netzwerküberwachung die geringere Belastung der zugrunde liegenden Netzwerkstruktur. Die Agenten überwachen ständig die gewünschten Werte des eigenen Systems. Sie übermitteln die Ergebnisse nur, wenn sich diese verändern und die Veränderung eine zuvor festgelegte Schwankungsbreite überschreitet. Periodische Abfragen sind in diesem Konzept somit nicht vorgesehen, wodurch es, wie bereits erwähnt, zu einem geringeren Netzwerkverkehr kommt (Hall, 2003).

### *Nachteile*

Probleme dieses Konzepts entstehen aus der Unsicherheit der korrekten Übertragung der Werte. Der Manager wartet auf Informationen, überprüft aber nicht die Verfügbarkeit der Verbindung. Damit können hier zwei Probleme auftreten: Entweder die Agenten selbst können keine Daten senden oder die Daten gehen auf dem Weg zum Manager verloren (Hall, 2003). Auch muss eine Anpassung der Konfiguration direkt auf den einzelnen Agenten stattfinden. Dies verursacht einen zusätzlichen Administrationsaufwand. Des Weiteren können im Rahmen der passiven Netzwerküberwachung Daten nur offline analysiert werden. Somit ist zum Beispiel die Überwachung von Real-Time-Systemen nicht möglich (Anagnostakis et al., 2002).

### 2.2.3 Auswahl an problemspezifischen oder experimentellen Methoden

#### *Network-Monitoring auf Basis des Shortest Path Tree Protocol*

In der Arbeit von Breitbart, et al.(2004) wird eine Verringerung des Netzwerkverkehrs in einer aktiven Netzwerküberwachung durch den Einsatz des Shortest-Path-Tree Protokoll erreicht. Die Anzahl der Abfragen wird in diesem Ansatz nicht verringert. Der Weg der Anfragen im Netzwerk wird jedoch minimiert, um so die Last zu verringern. Dies reduziert die bereits erwähnten Probleme einer aktiven Netzwerküberwachung. Es ist jedoch keine Lösung im eigentlichen Sinn, da lediglich eine größere Anzahl von abgefragten Werten ermöglicht wird. Das grundsätzliche Problem einer wesentlich höheren Netzwerkbelastung im Vergleich zum passiven Network-Monitoring bleibt bestehen.

#### *Netzwerküberwachung von Mobile-Agent Systemen*

Mobile-Agent-Plattformen setzen sich in vielen Anwendungsbereichen durch. Trotz der Vorteile gegenüber herkömmlichen Client-Server-Architekturen bergen derartige Plattformen vielfältige Problembereiche. Neben grundsätzlichen Problemen verteilter Anwendungen werden durch die Vertrauensstellung der einzelnen Agenten schwerwiegendere Angriffe durch reguläre Benutzer ermöglicht (Bellavista et al., 2002).

Um dieses Problem lösen zu können, muss es einer Überwachungsinstanz ermöglicht werden, sowohl das Betriebssystem als auch die Virtual Machine, welche den Agent umfasst, zu kontrollieren. Dies wurde für Java-based Mobile Agents in einem Projekt an der Universität von Bologna umgesetzt. Die entwickelte Monitoring-Schnittstelle umfasst neben Betriebssystem abhängigen Komponenten zur Überwachung von computerspezifischen Ressourcen, auch solche zur Überwachung der Java Virtual Machine und somit des Agents (Bellavista et al., 2002).

Obwohl diese Art der Überwachung über das klassische Network-Monitoring hinausgeht, decken sich der Aufbau und große Teile des Aufgabenbereichs mit herkömmlichen Network-Monitoring-Systemen.

## 2.3 Teilaspekte

In Abschnitt 1.2 wurde bereits erwähnt, dass Network-Monitoring-Systeme mehrere Aufgabengebiete umfassen. Diese werden nun näher erläutert. Weiters wird auf den möglichen Einsatz von Network-Monitoring-Systemen zur Dokumentation der IT-Infrastruktur hingewiesen (Josephsen, 2007).

### 2.3.1 Monitoring

*"to monitor: verb keep under constant observation, especially so as to regulate, record, or control"* (Oxford dictionary, 2006)

Nach dieser Definition umfasst der Begriff "to monitor" die ständige Überwachung eines Systems. In Kapitel 2.2 wurden bereits die generellen Methoden zur Überwachung von Netzwerken vorgestellt. Die Methode der passiven Netzwerküberwachung scheint nun im Widerspruch zur gegebenen Definition zu stehen, da hier keine ständige Überwachung vonstatten geht. Daten, so genannte Traps, werden nur im Fehlerfall aufgrund bestimmter Ereignisse an den Manager eines Network-Monitoring-Systems übermittelt. Auf den ersten Blick ist dieser Einwand berechtigt. Jedoch werden die Daten kontinuierlich überprüft, auch wenn diese nicht an den Manager weitergeleitet werden, da ansonsten Ereignisse, welche Traps auslösen sollten, nicht erkannt werden könnten. Somit wird hier die Forderung nach einer ständigen Überwachung ebenso erfüllt. Diese wird jedoch nicht, wie beim aktiven Monitoring, durch den Manager sondern durch den Agent realisiert.

Neben der Überwachung von Abfragewerten sind im Zusammenhang mit dem Teilbereich "Monitoring" auch die folgenden Themen von Interesse.

#### *Sicherheitsaspekte des Network-Monitoring*

Um eine aktive Netzwerküberwachung zu ermöglichen, muss das zu überwachende System vom Manager eines Überwachungssystems über das Netzwerk erreicht werden können. Darüber hinaus muss der Manager berechtigt sein, mit den Agenten des jeweiligen Systems zu kommunizieren. Die Agenten wiederum müssen alle benötigten Rechte für die Abfrage der relevanten Informationen innehaben. Die zentrale Rolle des Managers, aber auch die Berech-

tigungen der einzelnen Agenten sind somit lohnende Ziele für einen Angriff auf das jeweilige Computernetzwerk (Bejtlich, 2004).

Auf Ebene der Netzwerkprotokolle wurde versucht, dieses erhöhte Sicherheitsbedürfnis durch eine Absicherung der Kommunikation zwischen den einzelnen Teilen des Systems zu erreichen. Die weiter unten beschriebene SNMP Protokollfamilie wurde zum Beispiel um ein benutzerbasiertes Sicherheitssystem erweitert (RFC2275, 1998). Weiters ist die Absicherung des Managers und die Platzierung dieses Systems zu beachten. Er sollte sich in einem separaten Management-Netz am Besten in einem privaten Adressbereich befinden. Grundsätzlich ist das Konzept der passiven Netzwerküberwachung zu bevorzugen, da hier seltener Informationen übermittelt werden und der Manager keine Möglichkeit zur direkten Verbindung mit anderen Systemen benötigt (Bejtlich, 2004).

### *Netzlast*

Die Übermittlung der Daten für die Netzwerküberwachung kann zu einer Belastung der Bandbreite führen. Um dies zu veranschaulichen soll folgendes Rechenbeispiel dienen:

| |
|---|
| 100 zu überwachende Einheiten |
| 50 Werte pro Einheit |
| 100 Byte pro übermittelten Wert |
| 100 Server x 50 Werte = 5 000 zu übermittelnden Werte |
| 5 000 Werte x 100 Byte = 500 000 Byte |

Wie man erkennen kann, ist die Belastung in einem LAN nicht beachtenswert, selbst wenn die Werte jede Minute abgefragt werden würden. Wenn jedoch der Manager nur mit einer 2 mBit Standleitung an das eigentlich zu überwachende Netz angeschlossen ist, was im zugrundeliegenden Projekt dieser Diplomarbeit angedacht ist, kommt es zu einer erheblichen Beeinträchtigung der Verbindung während der Abfrage der Werte.

Um diese Last zu verringern, kann passives Network-Monitoring eingesetzt werden, da so die Anzahl der Datentransfers im Vergleich zum aktiven Network-Monitoring vermindert wird. Falls aktives Network-Monitoring eingesetzt wird, sollte dem Intervall der Abfragen Beachtung geschenkt werden. Dies sollte so groß gewählt werden, dass eine durchgängige Überwa-

chung gegeben ist, aber keine unnötigen Wiederholungen durchgeführt werden. Außerdem ist es ratsam, die Anzahl der abgefragten Werte möglichst gering zu halten.

*"Good monitoring systems tend to be focused, rather than chatty."*(Josephsen, 2007, p.19)

### 2.3.2 Analyzing

Nachdem die Werte im Rahmen des Monitoring gesammelt und an den Manager übermittelt wurden, muss dieser nun die Informationen an das Monitoring-Programm, wie Stalling es bezeichnet, weitergeben. Die Aufgabe dieses Programms liegt, wie in Abschnitt 2.1 beschrieben, in der Auswertung und Speicherung der Daten. Die Analyse der Daten wird in den meisten Monitoring-Programmen unter Verwendung von zuvor festgelegten statischen Schwellenwerten durchgeführt. Administratoren benötigen ein tiefes Verständnis der überwachten Systeme um geeignete Schwellenwerte zu ermitteln (Josephsen, 2007).

### 2.3.3 Alerting

Im Gegensatz zum Analyzing umfasst das Alerting mehr Aufgaben, jedoch benötigt die Konfiguration weniger technisches Know How. Die adäquate Verständigung der zuständigen Personen umfasst neben technischen Problemen, wie der Ansteuerung geeigneter Übertragungsmedien, auch strategische Komponenten, wie etwa die Festlegung von Benachrichtigungsintervallen, -zeiten oder Eskalationsszenarien. Im Allgemeinen können folgende Teilbereiche angeführt werden (Barth, 2006):

- Benachrichtigungsintervall
- Eskalation
- Benachrichtigungszeiten
- Benachrichtigungsmedium

#### *Benachrichtigungsintervall*

Das Benachrichtigungsintervall bezeichnet die Zeitspanne, welche zwischen zwei Benachrichtigungen über dasselbe Ereignis an dieselbe Person oder Personengruppe mindestens liegen muss. Mit einer steigenden Anzahl von Benachrichtigungen in einem kurzen Intervall

nimmt die Aufmerksamkeit der Personen für diese ab (Josephsen, 2007). Das Benachrichtigungsintervall sollte somit die Bedeutung des aufgetretenen Ereignisses widerspiegeln. Weniger wichtige Ereignisse sollten eine niedrigere Frequenz als kritische aufweisen. In der Folge gibt ein kurzes Szenario weiteren Aufschluss.

Der Ausfall des Email-Servers sollte in den meisten Unternehmen sehr häufig gemeldet werden. Oft werden hier Intervalle von fünf Minuten eingeführt (Ehringer, 2005). Ein Abfall der Übertragungsrate im Netzwerk ist ebenfalls ein ernst zu nehmender Störfall. Dieser bedarf aber in normalen Unternehmen oft keiner so großen Aufmerksamkeit wie das vorangegangene Problem. Hier wäre vielleicht eine halbstündliche Wiederholung der Nachricht ausreichend. Anders stellt sich die Situation im Umfeld eines Unternehmens dar, das sich auf Web-Hosting spezialisiert hat. Der Rückgang der Übertragungsraten nimmt hier einen wesentlich höheren Stellenwert ein. Hier könnten die oben genannten Frequenzen vertauscht werden.

Man erkennt in diesem Szenario, dass mit Hilfe der Frequenz die Gewichtung des jeweiligen Problems widergespiegelt werden kann. Obwohl die Bedeutung des Benachrichtigungsintervalls in der Literatur oft vernachlässigt wird, kann mit den geeigneten Einstellungen über die Gewichtung einzelner Probleme hinaus sogar die unternehmerische Strategie beeinflusst bzw. durchgesetzt werden (Josephsen, 2007). Dieser Aspekt wird Kapitel 4 dieser Arbeit nochmals aufgegriffen.

### *Eskalation*

Eskalationsstrategie bezeichnet die Benachrichtigung unterschiedlicher Personengruppen bei fortwährendem Bestehen eines Problems (Barth, 2006). Dem obigen Beispiel folgend würde der Ausfall eines Email-Servers in der Eskalationsstufe 1 nur den zuständigen Server-Administratoren gemeldet. Wenn dieses Problem beispielsweise länger als eine halbe Stunde besteht werden Netzwerk-Administratoren und die Vorgesetzten der zuvor benachrichtigten Server-Administratoren verständigt. Dies ist die zweite Eskalationsstufe. Besteht das Problem nach einer Stunde immer noch, wird in der dritten Eskalationsstufe die Leitung der IT informiert. Nach einem halben Tag wird als letzte Eskalationsstufe (Eskalationsstufe 4) das Management über den Vorfall informiert, da der Email-Verkehr als unternehmenskritisch angesehen wird. Die einzelnen Eskalationsstufen spiegeln die Hierarchiestrukturen eines Unternehmens wider, ähnlich einem Organigramm (Abbildung 4).

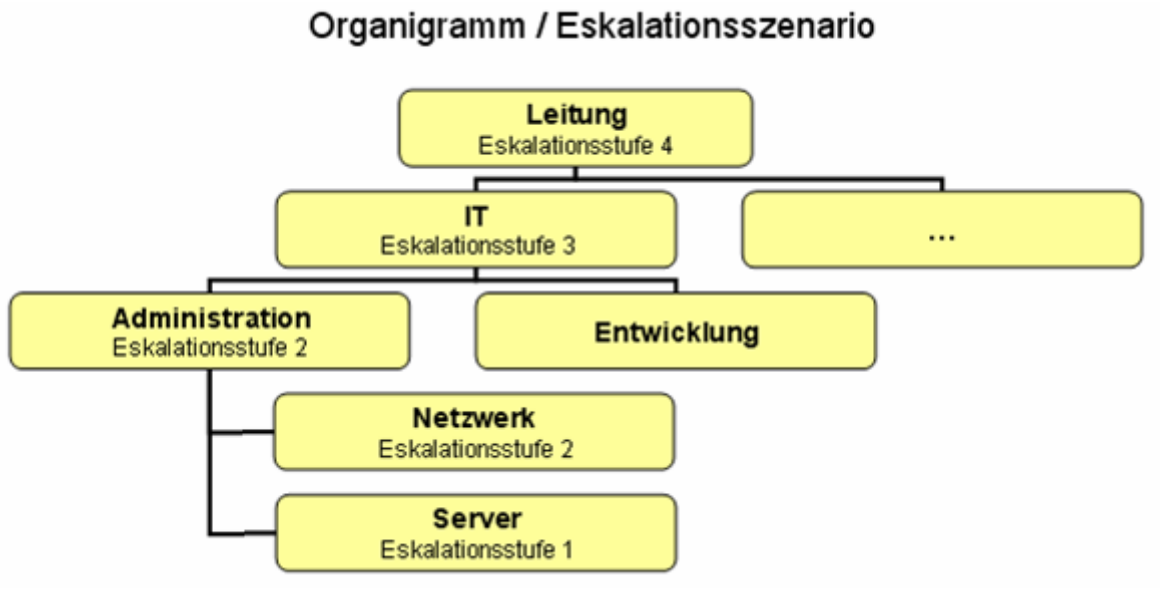


**Abbildung 4: Eskalationsszenario**

Die Eskalationsstrategie gibt dem Einzelnen nicht nur vor, wie viel Zeit er für die Bewältigung des Problems benötigen darf, sondern sie zeigt auch die Bedeutung des Vorfalls. Je wichtiger ein Ereignis ist, desto schneller erreichen die einzelnen Eskalationsstufen die obersten Entscheidungsebenen eines Unternehmens. Dieses Konzept steuert richtig angewandt wiederum die Aufmerksamkeit und den Ressourceneinsatz für ein Problem. Folgerichtig kann auch die Eskalationsstruktur zur Umsetzung von Unternehmensstrategien eingesetzt werden (Josephsen, 2007).

### *Benachrichtigungszeiten*

Unter der Benachrichtigungszeit versteht man jene Zeiten, zu denen eine Person grundsätzlich über ein Ereignis informiert werden kann (Barth, 2006). Wieder kann eine Steuerung der Aufmerksamkeit über dieses Konzept durchgeführt werden (Josephsen, 2007). Wichtige Ereignisse werden während der gesamten Woche und zu jeder Tageszeit gemeldet, andere nur zu den Arbeitszeiten.

Ein interessanter zusätzlicher Aspekt, der in der Literatur nicht behandelt wird, ist die Möglichkeit einer sozialen Ausrichtung der Benachrichtigungszeiten. Wenn für ein gegebenes Problem zwei Administratoren zuständig sind, wobei einer davon Familienvater ist, könnte dieser an Wochenenden von Benachrichtigungen ausgenommen werden. Natürlich müsste hier eine entsprechende Gegenleistung für den zweiten Administrator gefunden werden.

*Benachrichtigungsmedium*

Ähnlich den vorangegangenen Möglichkeiten kann auch die Wahl des Benachrichtigungsmediums für eine Steuerung der Aufmerksamkeit eingesetzt werden. Einer Email wird zum Beispiel weniger Beachtung geschenkt als einer SMS (Rathgeber, 2004).

Neben dieser Steuerungsfunktion besitzt die Wahl des Benachrichtigungsmediums einen technischen Aspekt, da es nicht immer möglich ist sämtliche Medien zur Übermittlung einer Nachricht zu verwenden. Ein Monitoring-System kann zum Beispiel die Benachrichtigung über einen Ausfall des Internetzugangs nicht über einen externen SMS Server verschicken.

### 2.3.4 Dokumentation

Die bisher besprochenen Aufgaben- und Funktionsbereiche eines Network-Monitoring-Systems ergeben sich aus dem in Abschnitt 1.2 gegebenen Konzept. In der Literatur wird ein weiterer Nutzen eines Überwachungssystems erwähnt. Derartige Systeme stellen die gesamte Netzwerkstruktur in einer sehr übersichtlichen Form dar. Weiters sind für jedes Netzwerkelement alle relevanten Dienste angeführt. Zusätzlich unterstützen die meisten Programme zur Überwachung von Netzwerken die Eingabe von Zusatzinformationen über die einzelnen Komponenten. Zu guter Letzt können durch Abhängigkeiten auch die Strukturen des Netzes abgebildet werden. Aus all diesen Punkten ergibt sich die Möglichkeit, Network-Monitoring-Tools auch zur Dokumentation eines Netzwerks zu verwenden. Umfassende Network-Management-Systeme, wie HP OpenView (Hewlett-Packard, 2006) oder IBM Tivoli (IBM, 2006), bewerben diesen Nutzen aktiv. Spezialisierte Produkte, wie WhatsUp Gold oder Nagios, scheuen sich in ihrer Produktbeschreibung auf diesen Nutzen hinzuweisen, obwohl er besonders für Nagios in der Literatur oft angeführt wird (Josephsen, 2007).

## 2.4 Protokolle

Um die genannten Aufgaben des Network-Monitoring erfüllen zu können, muss eine geregelte Kommunikation im Besonderen zwischen dem Manager und den Agents eines Netzwerküberwachungssystems festgelegt werden. Diese wird in Protokollen beschrieben, welche im besten Fall durch allgemein gültige Standards definiert sind.

Im Bereich des Network-Managements wurden von unterschiedlichen Gruppen verschiedene Protokolle erstellt, welche auch im Network-Monitoring zum Einsatz kommen. Die Internet Engineering Task Force (IETF) oder die International Organization for Standardization haben noch keine Standards entwickelt, welche ausschließlich für die Kommunikation von Netzwerküberwachungssystemen erarbeitet wurden. Einige Teilbereiche der umfassenderen Network-Management-Standards wurden jedoch für die Nachrichtenübermittlung in Network-Monitoring-Systemen konzipiert. In der Folge werden die bekanntesten Protokolle vorgestellt. Diese Auflistung erhebt keinen Anspruch auf Vollständigkeit, sondern bezieht sich insbesondere auf die in dieser Arbeit verwendeten Kommunikationsprotokolle.

### 2.4.1 SNMP

Die Version 1 des Simple Network Management Protocol (SNMP) (RFC 1157, 1990) ist das am weitesten verbreitete Protokoll für Network-Management (Stallings, 1998). SNMP kann jedoch nicht als isoliertes Protokoll gesehen werden. Es verwendet weitere Standards, welche die Art der Daten, die Codierung und die Übermittlung der Informationen beschreiben. Bevor auf SNMP selbst eingegangen wird, werden nun die einzelnen Standards, welche von SNMP verwendet werden, näher erläutert.

#### 2.4.1.1 ASN.1

Die Abstract Syntax Notation One (Steedman, 1990), kurz ASN.1, ermöglicht es, Datentypen abstrakt zu beschreiben. Diese Beschreibung ist allgemein gültig und damit unabhängig von der tatsächlichen Darstellung der Daten. Für SNMP ist nur die unten gezeigte Teilmenge der in ASN.1 gültigen Datentypen erlaubt:

- Bit String
- Integer
- Null
- Object Idenifier
- Octet String

Weiters wird in SNMP nicht ASN.1 als solches eingesetzt, sondern eine Abwandlung davon, nämlich die Structure of Management Information (RFC 1065, 1990), kurz SMI. Einzelne Objekte besitzen in SMI mindestens folgende vier Parameter:

| Parameter | Bedeutung |
|---|---|
| | |
| Syntax | Angabe des Datentyps |
| MAX-Access | Festlegung der Schreib-/Leserechts |
| Status | Information über die Kompatibilität mit unterschiedlichen SNMP Versionen |
| Description | Zeichenkette, welche die Funktion des Objekts beschreibt |

**Tabelle 3: SMI Parameter**

Der Parameter MAX-Access ist in der Begriffsabgrenzung von Network-Management und Network-Monitoring von besonderer Bedeutung. Im Network-Management werden Schreibrechte benötigt, da eine Veränderung des Wertes möglich sein muss. Das Network-Monitoring benötigt jedoch nur Leserechte auf die einzelnen Variablen, somit kann der Wert von MAX-access auf “read-only“ gesetzt sein. Dies erhöht die Sicherheit, da keine Manipulation der Werte möglich ist.

Die einzelnen Objekte, welche in SMI definiert sind, werden zu Objektgruppen zusammengefasst. Mehrere Objektgruppen ergeben einzelne Module. Aus dieser hierarchischen Gliederung ergibt sich eine Baumstruktur. Diese wird in der Management Information Base (RFC 1213, 1991), kurz MIB, abgebildet.

#### 2.4.1.2 MIB

Wie bereits erwähnt, dient eine MIB zur Darstellung des SMI Objektbaumes. Die einzelnen MIBs sind somit Teilbäume des ASN.1 Objektbaum. Jedes Element dieses Baumes ist über einen Object Identifier (OID) eindeutig identifizierbar und ansprechbar. Abbildung 5 zeigt einen Teilbereich dieses Objektbaumes.

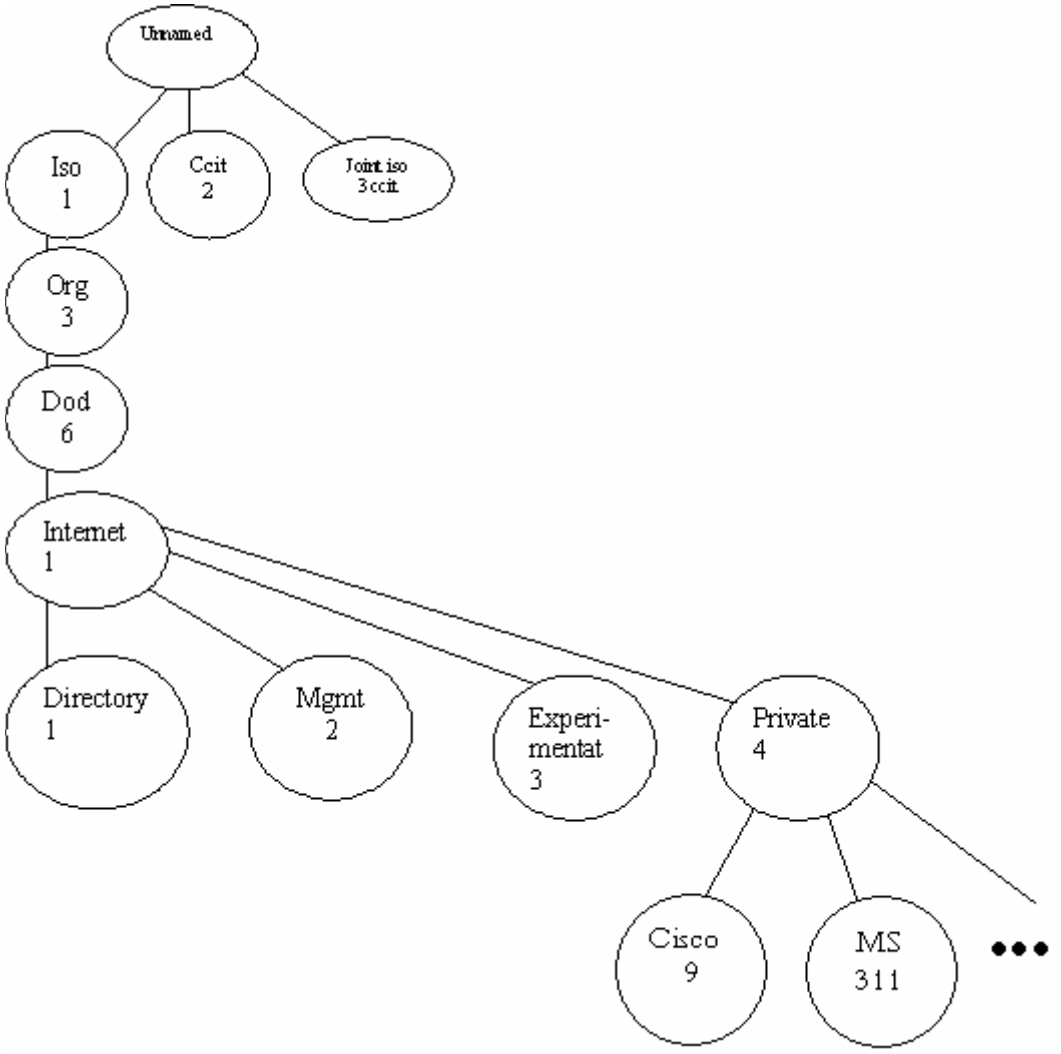


**Abbildung 5: MIB**

Wie man in Abbildung 5 sieht, befinden sich alle Objekte, welche mit der OID 1.3.6.1.2 beginnen, im Management-Subbaum. In diesem sind allgemein gültige Definitionen von Objekten festgelegt, welche von unterschiedlichen Herstellern in der gleichen Weise unterstützt werden. Objekte, deren OID mit 1.3.6.1.4 beginnen, befinden sich im Private-Subbaum. In diesem können die Hersteller ihre produktspezifischen Objekte definieren, welche nur von proprietären Netzwerkelementen unterstützt werden. Dazu müssen die Organisationen eine Private-Enterprise-Number von der Internet Assigned Numbers Authority (IANA) anfordern, um die Eindeutigkeit der einzelnen Objekte zentral gewährleisten zu können.

Das Objekt “sysName“, welches den Namen des Systems angibt, ist zum Beispiel im Management-Baum mit der OID 1.3.6.1.2.1.1.5 zu finden. Das Objekt “cur“, welches die aktuelle Anzahl der anonymen User auf einem Webserver des Typs “Microsoft IIS 6.0“ anzeigt, steht hingegen im Private-Enterprise-Baum der Firma Microsoft und besitzt die OID

1.3.6.1.4.1.311.1.7.3.1.7.0. Die Subbaums der Firma Microsoft besitzt somit die OID 1.3.6.1.4.1.311. In diesem Baum ist es dem Unternehmen möglich eigene Objekte, wie den genannten Wert des Microsoft Webservers, zu definieren.

### 2.4.1.3 Basic Encoding Rules

Die Basic Encoding Rules (CCITT, 1988), kurz BER, legen fest, wie Daten übermittelt werden. Die Struktur der Daten ist in den zuvor beschriebenen Protokollen bereits festgelegt worden. Die BER geben nun an, wie diese Daten zwischen verschiedenen Systemen übertragen werden. Dadurch werden Interpretationsprobleme verhindert. Ein Beispiel hierzu ist die unterschiedliche Definition des Beginns eines Bytes, dies wird als “Little Endian/Big Endian“ Diskurs bezeichnet (James, 1990). In BER werden folglich die Rangfolge und die Bedeutung der einzelnen Bits einer Übertragung festgelegt. Damit ist die Auswertung eindeutig. In Abbildung 6 werden die einzelnen Varianten der BER Codierung gezeigt.

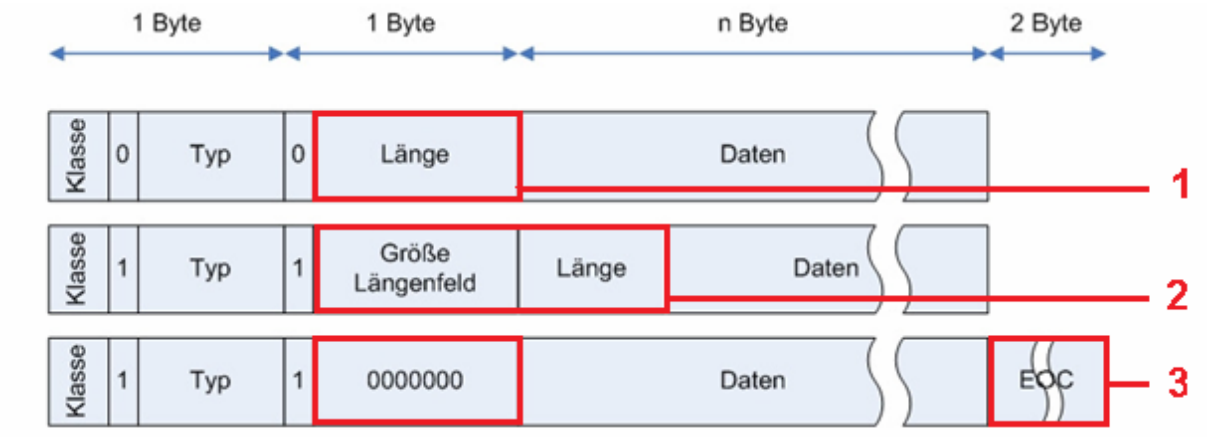


**Abbildung 6: BER Codierung (Tabakoff, 2006)**

Man erkennt, dass sich die einzelnen Typen hauptsächlich bei der Angabe der Länge der Dateneinheit unterscheiden. Diese wird entweder im zweiten Byte direkt angegeben (Abbildung 6–1) oder die Größe der Längenangabe wird in diesem Byte eingetragen (Abbildung 6–2) oder das zweite Byte besteht aus Nullen, wodurch eine Dateneinheit durch eine definierte Bitfolge am Ende einer Dateneinheit beendet wird (Abbildung 6–3). Der Aufbau des ersten Bytes ist für alle Typen gleich. In diesem werden die Klasse und der Typ der Dateneinheit angegeben.

#### 2.4.1.4 SNMP

Mit den Basic Encoding Rules ist nun auch die richtige Interpretation der übertragenen Daten sichergestellt. SNMP v1 (RFC 1157, 1990) beschreibt nun, wie die Kommunikation an sich vonstatten gehen muss. Dieses auf UDP basierende Protokoll definiert Network-Elements, Network-Agents und Network-Management-Stations. Network-Elements verfügen über Network-Agents, welche die eigentlichen Management-Funktionen bereitstellen. Network-Elements kommunizieren mit der Network-Management-Station zum Austausch von relevanten Daten. Dieser Aufbau ist dem allgemeinen Aufbau von Network-Monitoring-Systemen ähnlich (Abbildung 1), jedoch wird in SNMP, da es ein Network-Management-Protokoll ist, kein Monitoring-Programm erwähnt.

Für die Kommunikation zwischen einem Network-Element und einer Management-Station gibt es verschiedene Nachrichtentypen. Diese dienen dazu, Werte aus einem Network Element auszulesen oder diese zu verändern. Im Rahmen des Network-Monitoring werden nur jene Typen verwendet, mit denen Daten ausgelesen nicht aber verändert werden können. Somit wird die in SNMP vorhandene SET-Funktion nicht benötigt. Zum Übermitteln von Daten in SNMP zwischen einem Network-Element und einer Management-Station sind grundsätzlich zwei Varianten vorhanden.

- Get: Diese Variante wird in der aktiven Netzwerküberwachung verwendet und umfasst die Möglichkeit Werte eines Network-Elements auszulesen. Zur Steigerung der Effizienz sind auch die Funktion Get-Next und Bulk-Abfragen möglich, wodurch mehrere Werte gleichzeitig übermittelt werden können.
- Trap: Dieser Nachrichtentyp folgt dem Konzept des passiven Network-Monitoring. Hier werden Daten nicht von der Management Station ausgelesen sondern vom Network-Element eigenständig versendet.

Wie bereits erwähnt, werden Werte im Rahmen des Network-Monitoring nicht manipuliert. Dadurch werden die Möglichkeiten von SNMP nicht vollständig ausgenutzt. Trotzdem können die ausgelesenen Werte sicherheitsrelevante Informationen preisgeben. Deswegen wird im nächsten Abschnitt auf die Sicherheitsproblematik dieses Protokolls eingegangen.

### *Sicherheit*

*"…a person armed with some freely available tools, some basic SNMP knowledge, and some interest in poking at network devices with blunt sticks, can come up with all sorts of interesting and occasionally even confidential information"* (Zwicky, 1998)

SNMP v1 besitzt kaum Sicherheitsmechanismen für den Schutz der Daten. Auch das Auslesen und Verändern von Werten auf Network-Elements durch nicht autorisierte Benutzer kann kaum verhindert werden. Einzig ein so genannter "community string", der unverschlüsselt aus einer Übertragung ausgelesen und nur für ein gesamtes Network-Element festgelegt werden kann, autorisiert einen Benutzer gegenüber dem System. Durch die Einführung von neuen Protokollversionen mit zusätzlichen Sicherheitskonzepten wurde versucht die Sicherheit von SNMP zu erhöhen. Die aktuelle Version SNMP v3 (RFC 3410, 2002) besitzt daher ein ausgereiftes Sicherheitskonzept. Dieses umfasst einen nutzerbezogenen Autorisierungsmechanismus und ermöglicht auch die Verschlüsselung der Daten während der Übertragung zwischen Network-Element und Management-Station. Obwohl SNMP v3 eingesetzt werden sollte um die Sicherheit eines Netzwerks zu gewährleisten, wird es in vielen Fällen nicht verwendet oder wird von verschiedenen proprietären Netzwerkkomponenten nicht unterstützt. Das Betriebssystem Windows Server 2003 bietet zum Beispiel standardmäßig keine Unterstützung von SNMP v3, was auf die Durchsetzung des später beschriebenen WMI Protokolls zurückzuführen ist. Auch im vorgestellten Projekt wurde vom Einsatz von SNMP v3 abgesehen, da der erhöhte Wartungsaufwand beim Einbinden neuer Systeme nach der anfänglichen Konfiguration als zu große Hürde angesehen wurde.

Zusammenfassend kann SNMP, besonders in der Version 3, als ausgereiftes und umfangreiches Protokoll für Network-Monitoring beziehungsweise Network-Management angesehen werden. Aufgrund der Standardisierung und der Flexibilität, welche sich wegen der Erweiterbarkeit des Objektbaums durch Private-Enterprise-Bereiche ergibt, ist SNMP weit verbreitet. Zudem gibt es für viele alternative Protokolle im Rahmen des Network-Management eine Möglichkeit zur Überführung der jeweiligen Daten in SNMP. In der Folge werden weitere, teilweise proprietäre Network-Management Protokolle vorgestellt (Rechenberg, 2002).

### 2.4.2 WMI

Die Windows Management Instrumentation (MSDN Library, 2007), kurz WMI, kann in allen Microsoft Windows Betriebssystemen verwendet werden. Sie setzt auf WBEM (DMTF, 2007) auf, das von der Distributed Management Task Force (DMTF) als Protokollfamilie für die Verwaltung von Netzwerkumgebungen entwickelt wurde. WBEM ist die Abkürzung für Web Based Enterprise Management und umfasst eine Reihe von Standards. Diese beschreiben das Datenmodell, die Codierung der Übertragung und die Zugriffsmethoden auf die einzelnen Werte der WBEM Komponenten. Man erkennt hier einen ähnlichen Aufbau wie bei SNMP, jedoch wurde WBEM speziell für das Management von verteilten Rechnernetzen entwickelt. Aus diesem Grund ist ein eigenes Protokoll namens WBEM Discovery vorhanden. Dieses ermöglicht eine automatisierte Identifikation und Kommunikation zwischen einzelnen WBEM Komponenten.

WMI kann auf alle veränderbaren Einstellungen eines Servers sowie die aktiven Dienste zugreifen. Ein Mapping von WMI auf SNMP steht zwar zur Verfügung, aber dieses ist nicht vollständig und erlaubt im Allgemeinen nur das Auslesen, nicht aber das Setzen von Werten. Zusätzlich wird SNMP v3 nicht unterstützt. Ab der in Windows XP verwendeten Version besitzt WMI jedoch ein eigenständiges Sicherheitskonzept zur Authentifizierung von Benutzern. Derzeit gibt es jedoch noch keine Möglichkeit Daten mittels WMI verschlüsselt zu übertragen. Trotz dieses Mankos muss WMI im Rahmen des Network-Monitoring aufgrund der weiten Verbreitung von Windows Betriebssystemen beachtet werden.

### 2.4.3 DMI

Der letzte hier vorgestellte Standard ist DMI (DMTF, 2007), das Desktop Management Interface. Dieses wurde ebenfalls von der Distributed Management Task Force entwickelt und hat folgendes Ziel:

*“DMI generates a standard framework for managing and tracking components in a desktop pc, notebook or server. DMI was the first desktop management standard.”* (DMTF, 2007)

DMI wird unter anderem von Intel und IBM eingesetzt, weswegen es in dieser Arbeit von besonderer Bedeutung ist. Der Vorteil von DMI ist, dass die Managementfunktionen unabhängig von einem laufenden Betriebssystem zur Verfügung stehen. Sie werden auf eigenen

Controllern realisiert. Dadurch ist es sogar möglich, Management Informationen auszulesen, ohne den Server booten zu müssen.

Obwohl DMI besonders im Bereich der Hardwareüberwachung von Servern Vorteile bietet, wird es kaum von Network-Management Systemen unterstützt. Dieser Umstand ergibt sich durch einen Standard, der von der DTMF entwickelt wurde. Dieser übersetzt die gesamte Funktionalität von DMI in SNMP. Daher ist es nicht nötig, DMI direkt zu unterstützen. Tabelle 4 zeigt zum Beispiel die Übersetzungstabelle der einzelnen Datentypen zwischen den verschiedenen Standards.

| DMI | SNMP v1 |
|---|---|
| | |
| Integer | Integer |
| Interger64 | Octet String (Size(8)) |
| Gauge | Gauge |
| Counter | Counter |
| String | Octet String |
| Octet String | Octet String |
| Date | Octet String (Size(25)) |

**Tabelle 4: Übersetzungstabelle DMI – SNMP (DMTF, 1997, p.16)**

Aufgrund der Entwicklung von WBEM wurde DMI von der DMTF 2005 als veraltet deklariert. Trotz dieses Status wird dieser Standard bei Hardwareherstellern weiterverwendet, weswegen er auch für dieses Projekt relevant bleibt.

## 2.5 Vorgehensmodell zur Implementierung einer Network-Moniotring Umgebung

Nachdem die Grundlagen von Network-Monitoring erörtert wurden, wird in diesem Kapitel ein allgemeines, im Rahmen dieses Projekts entwickeltes Vorgehensmodell zur Erstellung einer umfassenden Network-Monitoring Umgebung vorgestellt. Dieses ist an das Wasserfall Modell der Systementwicklung angelehnt (DOD, 2004). Das Modell umfasst alle Arbeitsschritte, welche beginnend mit der Analyse des Netzwerks über das daraus resultierende An-

forderungsprofil zur Konfiguration bis zur Inbetriebnahme und Wartung durchgeführt werden müssen.

### 2.5.1 Netzwerkanalyse

*"When implemented correctly, a monitoring system can be your best friend. […] When done poorly, however, the same system can wreak havoc"* (Josephsen, 2007, p.XiX)

Um ein Monitoring-System korrekt konfigurieren zu können, ist detailliertes Wissen über das zu überwachende Netzwerk im Gesamten und die einzelnen Netzwerkkomponenten im Speziellen von Nöten. Da es Unternehmen gibt, deren IT-Infrastruktur nicht ausreichend dokumentiert ist, muss der erste Schritt einer erfolgreichen Netzwerk-Monitoring-Umgebung die Erstellung einer aktuellen und genauen Netzwerkdokumentation sein. Diese Dokumentation wird in zwei Teilaspekte aufgeschlüsselt, die technische, welche die Infrastruktur des Netzwerks detailliert abbildet, und die qualitative, welche Aussagen zur Charakterisierung der einzelnen Komponenten macht. In den nächsten beiden Abschnitten werden diese näher erläutert.

#### *Technische Netzwerkanalyse*

Dieser Teil der Dokumentation listet alle Komponenten des Netzwerks und deren technische Eigenschaften, wie zum Beispiel IP-Adressen, auf. Außerdem müssen alle Serverdienste, wie FTP, HTTP usw., ersichtlich sein. Zu guter Letzt sind die physikalischen und logischen Verbindungen zwischen den Systemen bzw. den jeweiligen Diensten in der Dokumentation einzutragen. Somit umfasst dieser Teil die Darstellung der gesamten Netzwerkstruktur. Um ein möglichst genaues Abbild sollte jeweils eine Illustration des Netzwerks auf Layer 2 und eine auf Layer 3 des ISO/OSI-7-Schichtmodell (Zimmermann, 1980) angefertigt werden.

#### *Qualitative Netzwerkanalyse*

Wie bereits erwähnt, umfasst eine vollständige Netzwerkanalyse auch qualitative Aspekte. Diese Vorgaben müssen in Network-Monitoring-Systemen beachtet werden, da es nicht möglich ist, alle Netzwerk-Komponenten mit der gleichen Intensität zu überwachen. Ansonsten würden zu viele Meldungen generiert werden, was dazu führen würde, dass einzelne Meldungen weniger Beachtung erfahren.

*"Bad monitoring systems cry wolf at all hours of the night so often that nobody pays attention anymore."* (Josephsen 2007,p.XIX)

Im Rahmen der qualitativen Netzwerkanalyse müssen zwei Aufgaben bewältigt werden. Die generellen Anforderungen der Geschäftsführung müssen identifiziert und die einzelnen Systeme in einer Netzwerkinfrastruktur entsprechend ihrer Priorität gereiht werden. Diese Reihung kann anhand folgender Fragen des IT-Risk-Managements entschieden werden (Krause, 1999,p.226):

- *What could happen (threat event)?*
- *If it happened, how bad could it be (threat impact)?*
- *How often could it happen (threat frequency, annualized)?*
- *How certain are the answers to the first three questions (recognition of uncertainty)?*

Neben der Vergabe von Prioritäten müssen auch die generellen Anforderungen des Unternehmens an das Netzwerk bekannt sein. Für ein besseres Verständnis der Unternehmensführung für die IT-Infrastruktur können Techniken der industriellen Produktforschung angewendet werden. Eines dieser Verfahren, das zur Entwicklung von neuen Produkten verwendet wird, ist das Quality-Function-Deployment-Verfahren, kurz QFD (Couhen 1995). Im Rahmen des Network-Monitoring entspricht die Implementierung einer Umgebung zur Netzwerküberwachung der Produktneuentwicklung. In groben Zügen umfasst das QFD Verfahren folgende Schritte:

- Die allgemeinen Kundenbedürfnisse werden in einer offenen Befragung identifiziert.
- Die genannten Bedürfnisse werden kategorisiert und konkretisiert.
- Die Kunden vergeben in einer neuerlichen Befragung Prioritäten für die einzelnen Kategorien.
- Bedürfnissen mit hoher Priorität, welche derzeit zu wenig Beachtung finden, werden identifiziert.
- Das Ziel der Produktentwicklung ist die Behebung der im vorigen Schritt identifizierten Mängel.

Der Nutzen des QFD Verfahrens ist eine auf individuelle Kundenbedürfnisse basierende Zielvorgabe des neu zu entwickelnden Produkts. Weiters erhebt das QFD Verfahren den Anspruch, allgemeine, qualitative Aussagen der Produktforschung in technische Anweisungen zu

übertragen. Dies wird durch das Konzept des “House of Quality“ grafisch dargestellt. Wie in Abbildung 7 gezeigt, gibt die horizontale Ebene im “House of Quality“ die Produktforschung wieder. Diese korreliert mit einer horizontalen Ebene, welche den ingenieurwissenschaftlichen Ansatz einer Produktneuentwicklung widerspiegelt (Couhen, 1995).

Im Fall des Network-Monitoring können durch den Einsatz des QFD Verfahrens die qualitativen Anforderungen an das Netzwerk identifiziert und gereiht werden. So kann, je nach der Bewertung im QFD Verfahren, die Stabilität des Netzwerks als vorrangig gegenüber der Performance eingestuft werden oder umgekehrt. Dementsprechend wird das Network-Monitoring-System aufgebaut. Dabei gibt es zwei grundlegende Varianten:

1. viele Überprüfungen werden durchgeführt, um die Stabilität des Netzwerks zu gewährleisten
2. wenige Tests werden durchgeführt, um die Performance des Netzwerks nicht zu belasten

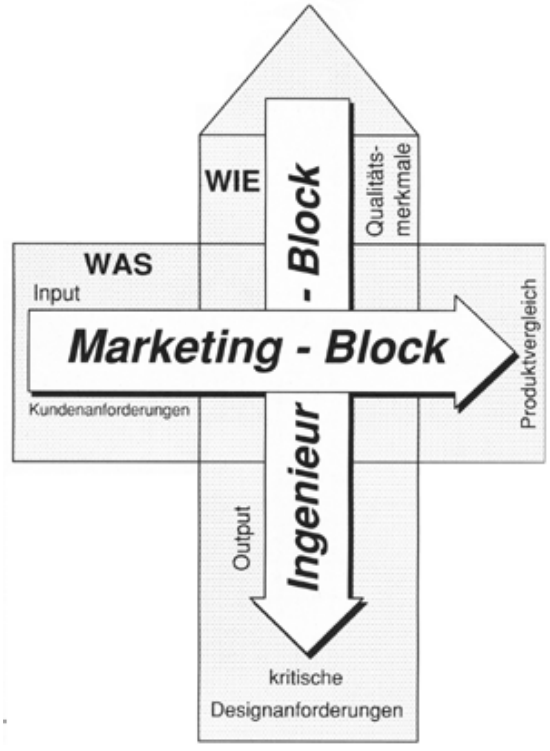


**Abbildung 7: House of Quality (Couhen, 1995)**

### 2.5.2 Anforderungsprofil

Das Anforderungsprofil kann wiederum in zwei Teilbereiche untergliedert werden. Ein Teil basiert auf der technischen bzw. qualitativen Netzwerkanalyse, woraus sich die netzwerkbezogenen Anforderungen an das Network-Monitoring-System ergeben. Der andere Teil befasst sich mit den nutzungsspezifischen Anforderungen, welche an das Tool zur Netzwerküberwachung gestellt werden. Dieser zweite Teil bezieht sich hauptsächlich auf Erkenntnisse aus der Befragung der zukünftigen Benutzer des Systems. Die nächsten beiden Abschnitte zeigen, welche Aspekte in den jeweiligen Teilen des Anforderungsprofils beachtet werden müssen.

#### *Netzwerkbezogenes Anforderungsprofil*

In diesem Teil werden die benötigten Protokolle für die Durchführung einer Netzwerküberwachung identifiziert. Falls zum Beispiel keine Systeme mit einem Microsoft Windows Betriebssystem im Netzwerk vorhanden sind, wird das WMI Protokoll nicht benötigt. Die Auswahl der verwendeten Protokolle zur Netzwerküberwachung hängt folglich sehr stark von der jeweiligen Infrastruktur ab. Da sich diese rasch ändern kann, ist es ratsam weit verbreitete und standardisierte Protokolle, wie SNMP, im Anforderungsprofil auf jeden Fall zu berücksichtigen. Aus demselben Grund sollten erweiterbare Systeme den Vorzug erhalten. Spezifische und proprietäre Protokolle sowie spezialisierte Überwachungssysteme sollten nur zum Einsatz kommen, wenn diese benötigte Funktionalitäten bereitstellen, welche nicht durch ein standardisiertes Protokoll abgebildet werden können (Barth, 2006).

Im netzwerkbezogenen Anforderungsprofil wird überdies die zugrundeliegende Überwachungstechnik des Network-Monitoring-Systems festgelegt. Wie bereits im Abschnitt 2.2 dargestellt, gibt es zwei grundsätzliche Techniken des Network-Monitoring: die aktive und die passive Variante. Beide Techniken haben Vor- und Nachteile. Die jeweiligen Probleme werden minimiert, wenn passive Netzwerküberwachung mit einer aktiven Kontrolle der Übertragungswege kombiniert wird. Die Grundsatzentscheidung zwischen verstärkter aktiver oder passiver Überwachung kann jedoch nur durch eine individuelle Entscheidung auf Basis der qualitativen und technischen Netzwerkanalyse gelöst werden.

Die qualitative Netzwerkdokumentation macht durch die Reihung der genannten Anforderungen allgemeine Vorgaben bezüglich der Ausgestaltung des Monitoring-Systems. Die tatsächliche Implementierung hängt jedoch von den Möglichkeiten ab, welche aufgrund der techni-

schen Gegebenheiten realisiert werden können. Folgendes Szenario kann zum Beispiel auftreten:

- Ergebnis der qualitativen Netzwerkanalyse:
    - Höchste Priorität: Stabilität des Systems A
    - Konsequenz: Einsatz eines aktiven Network-Monitoring-Systems
- Ergebnis der Technischen Netzwerkanalyse:
    - Einschränkungen: Aufgrund von Sicherheitskonzepten darf keine direkte Verbindung zu System A aufgebaut werden
    - Konsequenz: Passive Network-Monitoring Lösung muss eingesetzt werden
- Tatsächliche Implementierung
    - Passives Network-Monitoring-System

Man erkennt, dass in diesem konstruierten Fall eine passive Netzwerküberwachung eingesetzt werden muss, obwohl aufgrund der qualitativen Vorgaben eine aktive Netzwerküberwachung zu bevorzugen wäre.

Die meisten Network-Monitoring-Tools favorisieren entweder aktive oder passive Netzwerküberwachung. Diese Unterschiede äußern sich durch umständliche Konfigurationen von passiven Überwachungsfunktionen einerseits und mangelnden Einstellmöglichkeiten von aktiven Komponenten andererseits. Aus diesem Grund ist es unerlässlich, die Designentscheidung hinsichtlich eines aktiven oder passiven Network-Monitoring-Konzepts im netzwerkbezogenen Anforderungsprofil zu treffen.

### *Produktbezogenes Anforderungsprofil*

Im Gegensatz zum netzwerkbezogenen Anforderungsprofil befasst sich das produktbezogene Anforderungsprofil mit jenen Aspekten, welche mit dem Network-Monitoring-Tool in direktem Zusammenhang stehen. Diese sind unter anderem (Björn, 2004):

- Komplexität der Konfiguration
- Intuitivität der Benutzung
- Support

- Kosten
- Aufwand im laufenden Betrieb
- Aufwand bei Netzwerk-Änderungen
- Aufwand bei Personaländerungen

Die Komplexität der Konfiguration umfasst den Aufwand, der zur Erstellung einer funktionierenden Netzwerküberwachung und zur Erweiterung dieser Überwachung betrieben werden muss. Unter der Intuitivität der Benutzung wird zum Beispiel die Übersichtlichkeit der Überwachungsergebnisse verstanden. Im Zuge des Anforderungsprofils muss die maximale Einarbeitungszeit für den Umgang mit dem Tool angegeben werden. Diese sollte in die Einarbeitungszeit zur Konfiguration und die Einarbeitungszeit zur Benutzung des laufenden Systems aufgeteilt werden (Kecerski, 2005).

Ein weiterer Punkt, der im produktbezogenen Anforderungsprofil entschieden werden muss, ist der gewünschte technische Support. Folgende Fragen sind in diesem Zusammenhang im Rahmen des vorgestellten Projekts von Bedeutung:

- Ist Support nur im Fehlerfall erwünscht oder sollen Workshops den Umgang mit dem Tool erläutern?
- Sollen diese Workshops von einem Trainer geleitet werden oder als Video-Workshops von den einzelnen Usern des Systems in Eigenregie durchgearbeitet werden?

Abhängig vom gewünschten Support werden sich die direkten Kosten eines Network-Monitoring-Tools verändern. Man muss jedoch die gesamten Prozesskosten des Network-Monitoring-Systems beachten, um diesen Aspekt richtig behandeln zu können (Kecerski, 2005). Somit sind neben den Produkt- und Supportkosten auch Personalkosten zur Konfiguration und Benutzung des Systems sowie Kosten der Ressourcen, welche für die Netzwerküberwachung benötigt werden, zu beachten.

### 2.5.3 Produktentscheidung

Ein exaktes Anforderungsprofil schränkt die zur Wahl stehenden Network-Monitoring-Tools ein. Manche Tools unterstützen Netzwerkprotokolle nicht, welche im netzwerkbezogenen Anforderungsprofil aufgeführt sind. Andere Systeme sind durch ihren Designaufbau, der primär entweder auf eine aktive oder eine passive Netzwerküberwachung ausgerichtet ist, für

eine konkrete Aufgabenstellung ungeeignet. Weiters kann ein maximaler Produktpreis für das Tool die Auswahl einschränken.

Neben diesen Kriterien, welche im Vorhinein zu einer Selektion führen, können die Produkte in einer detaillierten Evaluierung verglichen werden. Vor allem die Komplexität der Konfiguration und die Intuitivität der Bedienung können nur im Rahmen einer Probe des Tools durch die späteren User des Systems im Rahmen eines Evaluierungsszenarios bewertet werden.

Nach einer ersten Vorauswahl anhand von technischen Kriterien müssen folglich die Benutzer des zukünftigen Systems in der Produktentscheidung miteinbezogen werden, da sie ein entscheidender Faktor für den Erfolg der Network-Monitoring-Lösung sind. Die endgültige Auswahl muss jedoch von den Entscheidungsträgern der Organisation getroffen werden (Pekruhl, 2000).

### 2.5.4 Konfiguration

Auf die Entscheidung für ein spezifisches Network-Monitoring Tool folgt die Konfiguration dieses Produkts für die Überwachung des konkreten Netzwerks. Die grundsätzlichen Richtlinien der Konfiguration sind vor allem durch das netzwerkbezogene Anforderungsprofil vorgegeben. Die Konfiguration muss eine praktische Umsetzung dieser Vorgaben darstellen. Zwei Schritte können identifiziert werden, welche iterative für die einzelnen Netzwerkkomponenten durchgeführt werden müssen:

#### *Konfiguration der zu überwachenden Infrastruktur*

Der erste Schritt umfasst alle Konfigurationen, welche nicht am Network-Monitoring-Tool durchgeführt werden können. Er umfasst einerseits die Konfiguration der zu überwachenden Systeme, um die gewünschten Werte dieser Komponenten überhaupt abfragen zu können. Die Installation der NET-SNMP Pakete in Linux zur Unterstützung des SNMP Protokolls können hier beispielsweise angeführt werden. Andererseits muss auch die Beschaffenheit der Netzwerkinfrastruktur beachtet werden. So muss gewährleistet werden, dass das Monitoring-Tool in der Lage ist, die gewünschten Werte abzufragen. Sicherheits- oder Routingkonzepte dürfen diese Kommunikation folglich nicht behindern.

Bei passivem Network-Monitoring werden die konkreten Funktionalitäten zur Überwachung einzelner Werte auf den Komponenten der Infrastruktur konfiguriert. Diese werden in diesem

Konzept, wie bereits beschrieben, nicht durch den Manager verwaltet. Weiters muss die Übermittlung dieser Daten an den gewünschten Empfänger bei festgelegten Ereignissen eingestellt werden. Ein Beispiel dafür sind SNMP-Traps. Das auslösende Ereignis ist in diesem Zusammenhang zwar bereits in der MIB definiert, der Empfänger eines Traps und die zu verwendende Protokoll Version müssen jedoch eingestellt werden, um dieses Konzept nutzen zu können.

### *Konfiguration des Network-Monitoring Tools*

Im zweiten Schritt der Konfiguration müssen die nötigen Einstellungen am Network-Monitoring-Tool vorgenommen werden. Dies umfasst folgende Aufgaben (Barth, 2006):

- Konfiguration von aktiven Abfragen
- Sicherstellung des Empfangs von Abfragewerten im Rahmen der passiven Netzwerküberwachung
- Konfiguration einer geeigneten Benachrichtigungspolitik

Zudem sind die nachstehenden Punkte zu beachten, falls sie im gewählten Network-Monitoring-Tool zur Verfügung stehen:

- Konfiguration einer geeigneten Berechtigungsstruktur für verschiedene Benutzer des Systems
- Konfiguration der Reports

## 2.5.5 Inbetriebnahme und Wartung

Praktische Erfahrungen haben gezeigt, dass nach der erstmaligen Konfiguration eines Network-Monitoring-Systems eine schrittweise Inbetriebnahme von Vorteil ist. Dadurch kann eine Überlastung der einzelnen überwachten Systeme oder des gesamten Netzwerks im Zuge von Fehlkonfigurationen verhindert werden. Außerdem führen Fehler in der Konfiguration des Alertings zu einer großen Menge an Fehlalarmen. Dies hat eine Behinderung der zuständigen Administratoren bzw. im Rahmen eines Eskalationsszenarios eine Belästigung von übergeordneten Hierarchiestrukturen zur Folge.

Um derartige Probleme auszuschließen, ist eine schrittweise Durchführung der Inbetriebnahme von Vorteil. Die unten vorgestellte Vorgehensweise besteht aus einer mehrstufigen Konfiguration des Network-Monitoring-Systems. Sie ist somit auch eine Konkretisierung der im letzten Abschnitt erwähnten allgemeinen Punkte zu diesem Thema. Das im Rahmen dieser Arbeit entwickelte Verfahren ermöglicht nach jeder Stufe eine Überprüfung des korrekten Verhaltens des Network-Monitoring-Systems. Dadurch können Auswirkungen von Fehlkonfigurationen auf die jeweilige Stufe der Inbetriebnahme eingeschränkt werden.

1. Aktive Überwachungen werden auf nichtproduktiven Systemen getestet.
2. Die Benachrichtigungen des Network-Monitoring-Systems werden an eine speziell für diesen Zweck eingerichtet Email-Adresse versendet.
3. Die Berechtigungsstruktur sowie das Eskalationsszenario werden abgebildet, wobei die Empfänger der einzelnen Eskalationsstufen die zuvor erwähnte Email-Adresse bleibt.
4. Die getestete Konfiguration wird auf produktive Systeme angewendet.
5. Die Email-Adressen der tatsächlichen Empfänger der Alerts des Network-Monitoring-Systems werden eingestellt.
6. Die gewünschte Benachrichtigungsart, wie zum Beispiel Mail oder SMS, der einzelnen Empfänger wird konfiguriert.
7. Das Verhalten des Systems wird kontinuierlich überwacht.

Das vorgestellte Verfahren verhindert somit die Überlastung von Systemen, indem die Konfiguration der Überwachung zuerst anhand von Testsystemen überprüft wird. Weiters verhindert es eine unnötige Belästigung von Nachrichtenempfängern während der Implementierung des Systems, da alle Nachrichten zuerst in einer Mail Adresse der Testumgebung abgefangen werden. Die Schritte 5 und 6 dienen einer letzten Absicherung. Generell wird akzeptiert, dass im Rahmen der Implementierung eines Monitoring-Systems Fehlmeldungen per Mail empfangen werden. Falsche Alarme per SMS oder Voice-Call werden jedoch als sehr starke Belästigung empfunden und sollten daher vermieden werden. Dies wird durch die Aufteilung in die genannten Schritte erreicht.

Der im ersten Schritt beschriebene Einsatz von nicht produktiven Systemen zum Test der Konfiguration hat einen weiteren entscheidenden Vorteil. Hier können gezielt Situationen hervorgerufen werden, welche zu einer Aktion des Network-Monitoring-Systems führen. So

kann nicht nur eine reibungslose Inbetriebnahme, sondern auch eine korrekte Funktionsweise der einzelnen Komponenten des Systems sichergestellt werden. Als Beispiel kann hier die Überprüfung eines Webservers dienen. Sobald der Webserver nicht mehr aktiv ist, soll ein Alert ausgelöst werden. Um die korrekte Funktion des Network-Monitoring Tools zu verifizieren, wird der nicht produktive Webserver deaktiviert. Anschließend wird überprüft, ob der zuvor festgelegte Alert ausgelöst wurde.

Nach einer erfolgreichen Inbetriebnahme eines Network-Monitoring-Systems muss dieses an die ständigen Veränderungen in einer Organisation, insbesondere in der Netzwerkinfrastruktur, angepasst werden. Diese Wartungsarbeiten sollten ebenfalls einem strukturierten Ablauf folgen. Auch hier kann das vorgestellte Ablaufmodell beim Hinzufügen einer neuen Netzwerkkomponente eingesetzt werden, um mögliche Nebeneffekte ausschließen bzw. eingrenzen zu können.

Das Ausscheiden einer Netzwerkkomponente kann keinem allgemeinen Vorgehensmodell folgen, da das Verhalten der unterschiedlichen Network-Monitoring-Systeme und das gewünschte Ergebnis zu verschieden sind. So kann gefordert sein, dass Reports mindestens ein halbes Jahr nach dem Ausscheiden einer Komponente weiter direkt abrufbar sind. Das verwendete Network-Monitoring-System löscht jedoch zugehörige Reports sobald eine Komponente entfernt wird. Somit muss jede Komponente im Tool für ein halbes Jahr weitergeführt werden, obwohl die jeweilige Komponente bereits ausgeschieden ist. Das gezeigte Beispiel veranschaulicht, dass auch das Vorgehensmodell zum Ausscheiden einer Komponente im jeweiligen Projekt mit den beteiligten Entscheidungsträgern abgesprochen werden muss.

## 2.6 Weiterführende Thematik - Intrusion Detection

In den letzen Kapiteln wurden die grundlegenden Konzepte von Network-Monitoring erklärt und ein allgemeines Vorgehensmodell zur Erstellung einer Network-Monitoring-Umgebung vorgestellt. In der Folge wird der Unterschied zu Security-Network-Monitoring bzw. Intrusion-Detection aufgezeigt.

*“Als Intrusion-Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion-Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsver-*

*letzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.“* (BSI, 2002)

Dieser Definition folgend unterscheidet sich Network-Monitoring von Intrusion-Detection durch die Zielsetzung. Network-Monitoring-Systeme überwachen Netzwerkkomponenten, um Fehler dieser Systeme zu erkennen. Im Gegensatz dazu dient die Überwachung von Computersystemen im Rahmen von Intrusion-Detection der Identifikation von Angriffen auf die überwachten Systeme. Es gibt host-basierte, netzwerk-basierte und hybride Intrusion-Detection-Systems (IDS). Host-basierte-Systeme überwachen einzelne Netzwerk-komponenten, netzwerk-basierte IDS überwachen den Verkehr in einem Netzwerk, hybride Intrusion-Detection-Lösungen umfassen sowohl host-orientierte als auch netzwerk-orientierte Überwachungskomponenten. Die allgemeine Funktionsweise wird in Abbildung 8 graphisch dargestellt.

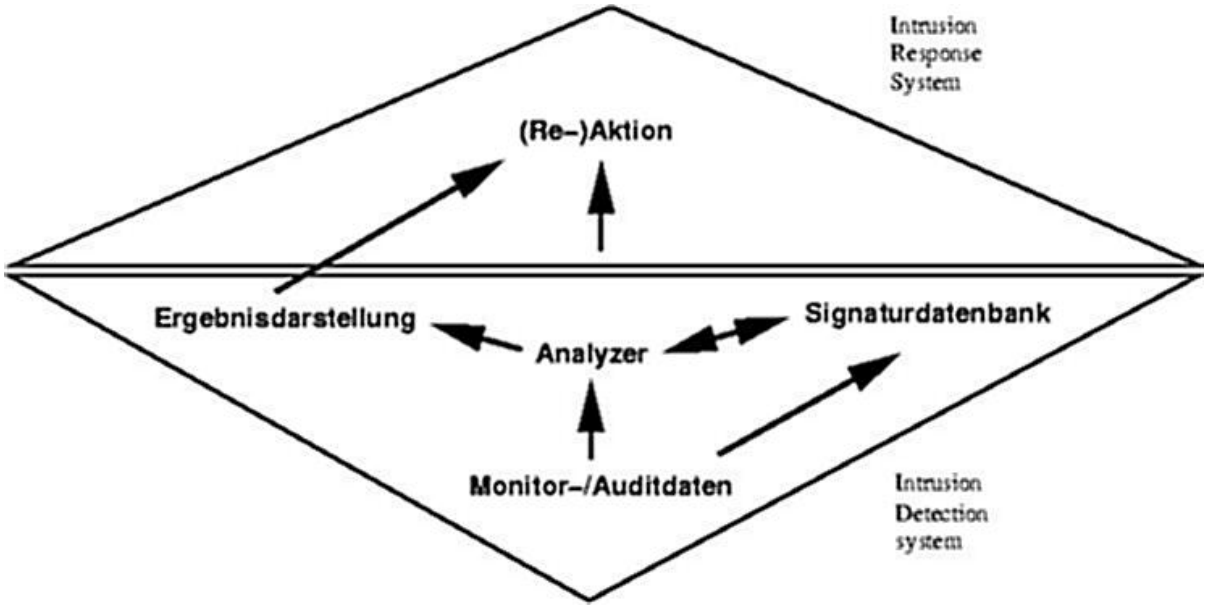


**Abbildung 8: Aufbau IDS (Miyamoto, 2007)**

Wie man sehen kann, werden ermittelte Daten mit einer Signaturdatenbank verglichen, welche Muster von Angriffen enthält. Das Ergebnis dieses Vergleichs wird an die Ergebnisdarstellung übergeben. Falls die IDS-Lösung ein Intrusion-Response-System umfasst, können bei einer Übereinstimmung mit der Signatur eines Angriffs automatisierte Aktionen zur Abwehr dieses Angriffs ausgelöst werden. Ansonsten werden die gewünschten Empfänger über die Attacke informiert. Ein Beispiel einer IDS-Lösung ist das Open Source Projekt “Snort“ (http://www.snort.org/).

# 3 Realisierung eines Best Practice Beispiels im Netzwerks einer Tageszeitung

Nachdem die Grundlagen des Network-Monitoring erörtert wurde, wird nun die Umsetzung eines Network-Monitoring-Systems im Netzwerk einer Tageszeitung vorgestellt. Das Unternehmen beschäftigt rund 70 ständige Mitarbeitern und etwa 40 freie Redakteuren. Die tägliche Auflage umfasst ca. 30 000 Exemplare. Die Zeitung ist damit die drittgrößte Tageszeitung von Oberösterreich.

Obwohl das verwendete Redaktionssystem sowie die Produktion der Zeitungen auf das Computernetzwerk angewiesen sind, wurde bisher noch kein Network-Monitoring eingesetzt. Durch den Ausfall einer Netzwerkkomponente könnte im schlimmsten Fall die Auflage des folgenden Tages nicht fertiggestellt werden. Dies würde zu einem Imageschaden und finanziellen Verlusten führen. Als diese Gefahr erkannt wurde, entschloss sich die Unternehmensleitung zu umfassenden Maßnahmen, um die Stabilität des Netzwerks zu erhöhen. Einerseits wurden redundante Strukturen geschaffen, andererseits wurde ein Network-Monitoring-System in Auftrag geben. Dieses Fallbeispiel folgt dem in 2.5 beschriebenen Vorgehensmodell und beginnt demzufolge mit einer umfassenden Analyse des bestehenden Netzwerks.

## 3.1 Netzwerkanalyse

Das Netzwerk der Tageszeitung kann in folgende Teilbereiche, die sich auf Systemebene teilweise überlagern, untergliedert werden:

- Active Directory zur Unterstützung der täglichen Büroarbeit
- Redaktionssystem
- VoIP Lösung
- Webauftritt
- Standleitungen zu externen Serviceanbietern

Diese Teilbereiche des Netzwerks können einzelnen Business Processes des Unternehmens zugeordnet werden. Dies dient im Besonderen für das bessere Verständnis der Geschäftsfüh-

rung für das Computernetzwerk, was im späteren Verlauf für die Erstellung einer qualitativen Netzwerkanalyse hilfreich ist.

Rummler definiert 1995 Business Processes folgendermaßen:

*“A business process is a series of steps designed to produce a product or service. Most processes (...) are cross-functional, spanning the ‘white space’ between the boxes on the organization chart. Some processes result in a product or service that is received by an organization's external customer. We call these primary processes. Other processes produce products that are invisible to the external customer but essential to the effective management of the business. We call these support processes.”* (Rummler, 1995,p.12)

Der einzig für diese Arbeit relevante Primary-Prozess des behandelten Unternehmens ist Content Creation. Communication und Accounting sind Support-Prozesse, welche eng mit dem Computernetzwerk verbunden sind und dadurch im Rahmen dieses Projekts ebenfalls beachtet werden müssen. Die Zuordnung der in 3.1 genannten Teilbereiche des Netzwerks zu den eben angeführten Business Processes ist in Tabelle 5 dargestellt.

| Business Process | Teilbereich des Netzwerks |
|---|---|
| | |
| Content Creation | Redaktionssystem<br>Web Auftritt<br>Standleitungen zu externen Serviceanbietern |
| Communication | Active Directory zur Unterstützung der täglichen Büroarbeit<br>VoIP Lösung |
| Accounting | Standleitungen zu externen Serviceanbietern |

**Tabelle 5: Business Processes der Tageszeitung**

Nach diesem grundlegenden Überblick über die Struktur und die Aufgabenbereiche wird das Netzwerk detailliert vorgestellt.

### 3.1.1 Technische Netzwerkanalyse

Bevor auf die relevanten Komponenten des Netzwerks genauer eingegangen wird, zeigt Abbildung 9 den generellen Aufbau des Netzwerks. Die Grafik gibt einen guten Überblick über das Netzwerk, obwohl darin unterschiedliche Layer des ISO-OSI-Schichtmodell vermischt werden.

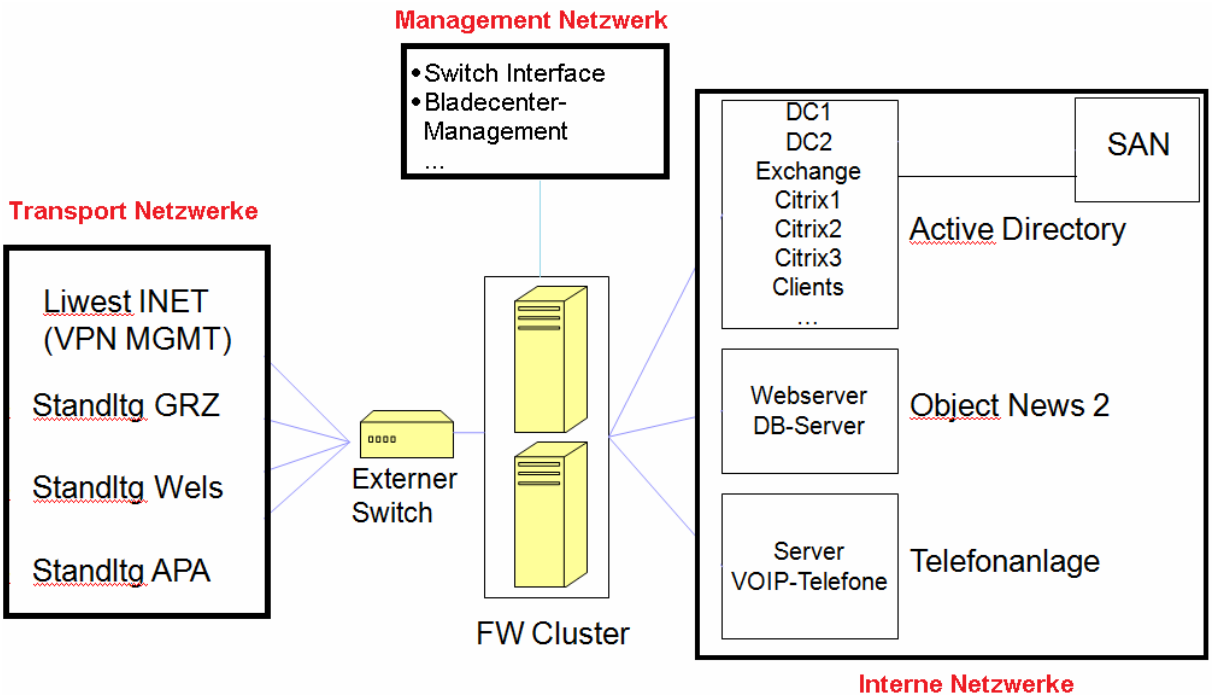


**Abbildung 9: Übersicht des Netzwerks der Tageszeitung**

Wie man in Abbildung 9 erkennt, gibt es mehrere externe Zugänge zu diesem Netzwerk. Die Aufgaben der einzelnen Verbindungen werden in Tabelle 6 angeführt.

| Verbindungsname | Funktion |
|---|---|
| | |
| Liwest | Internetanbindung |
| GRZ – Linz<br>(Großrechenzentrum) | Verbindung zu einem Großrechner für die Buchhaltung und Kundenverwaltung |
| Wels | Verbindung zur Druckerei |
| APA (Austria Presse Agentur) | Direkte Übermittlung der APA News |

**Tabelle 6: externe Verbindungen**

Die externen Bereiche werden physikalisch von einem Switch verwaltet und terminieren an einem Checkpoint Firewall-Cluster, der den Übergang zum internen Netzwerk schafft. Das interne Netzwerk ist neben den in Abbildung 9 gezeigten logischen Teilbereichen in mehrere Subnetze unterteilt. Diese Aufspaltung erfolgt auf Layer 3. Aufgrund eines organischen Wachstums des Netzwerks wurde diese Strukturierung jedoch nicht konsequent eingehalten. Dadurch überschneiden sich die einzelnen Bereiche des Netzwerks. So ist zum Beispiel keine klare Trennung zu dem bestehenden Managementnetzwerk gegeben. Da die Struktur im Rahmen des Projekts aufgrund zu kurzer Wartungsfenster nicht maßgeblich beeinflusst werden konnte, bleiben derartige Probleme bestehen.

Nach diesem allgemeinen Überblick wird die Struktur des Netzwerks im folgenden Abschnitt detailliert erklärt.

#### 3.1.1.1 Netzwerkstruktur

Das Netzwerk der Tageszeitung umfasst folgende Netzwerke:

| Netzwerk | Bezeichnung |
|---|---|
| | |
| 10.48.0.0/24 | Internes Netzwerk |
| 10.48.1.0/24 | IP-Telefonie |
| 10.49.0.0/24 | Management Netzwerk |
| 10.49.1.0/24 | Transport Netzwerk |
| Offizielles Netzwerk/24 | Externes Netzwerk |

**Tabelle 7: Subnetze**

Nachfolgend werden die Netze näher erläutert. Für ein besseres Verständnis werden einzelne Systeme und verwendete Hardware- sowie Softwarekomponenten in Abschnitt 3.1.1.2 kurz aufgelistet.

##### *Internes Netzwerk*

Das interne Netzwerk umfasst alle Server des Active Directory, die Server des Redaktionssystems und die Terminalserver, welche von Redakteuren verwendet werden können. Diesen wird auch ein Zugriff von außerhalb des Firmennetzwerks über Virtual-

Private-Network (VPN) Verbindungen ermöglicht, welche von einer Checkpoint Firewall verwaltet werden. Dabei ist jedoch anzumerken, dass hier aufgrund der verwendeten Technik keine Unterscheidung zwischen dem tatsächlichen internen Netzwerk und den entfernten Benutzern gegeben ist.

Neben diesen kritischen Systemen befinden sich in diesem IP-Bereich auch sämtliche Drucker und Client Systeme. Die fehlende Aufteilung zwischen Servern und Workstations ist hier besonders zu kritisieren, da dadurch keine Überwachung des Verkehrs auf Layer 3 zwischen den unterschiedlichen Bereichen möglich ist., weil die eingesetzte Firewall-Lösung keine Layer 2 Funktionalitäten bereitstellt.

Die für das Monitoring relevanten Systeme dieses Netzwerks sind:

- Spoolserver (10.48.0.232)
- Managementinterface des Switches der internen Netzwerke (10.48.0.239)
- Server des Redaktionssystems (10.48.0.240-242)
- Mail-Server (10.48.0.245)
- Nodes des Checkpoint Cluster (10.48.0.247-248)
- Domain Controller 1 (10.48.0.249)
- Domain Controller 2 (10.48.0.250)
- Terminalserver (10.48.0.236-237, 10.48.0.246, 10.48.0.251-252)
- Virtuelles Interface des Checkpoint Clusters (10.48.0.253)

### *Transport Netzwerk*

In diesem Netzwerk terminieren Fremdnetze. Bevor die Daten ins interne Netzwerk weitergeleitet werden, werden sie durch eine Firewall überprüft. Im Rahmen des Network-Monitoring können die Gegenstellen der Standleitungen überprüft werden, um die Verbindungen zu überwachen:

Die für das Monitoring relevanten Systeme dieses Netzwerks sind:

- Nodes des Checkpoint Clusters (10.48.1.1-2)
- Virtuelles Interface des Checkpoint Clusters (10.48.1.3)

- Gegenstelle der Standleitung zur APA (10.48.1.252) – derzeit noch nicht realisiert
- Gegenstelle der Standleitung zur Druckerei (10.48.1.253)
- Gegenstelle der Standleitung zum GRZ (10.48.1.254)

### *Management Netzwerk*

Der IP Bereich 10.49.0.0 ist für Systeme wie Switches, Router usw. vorgesehen. Diese Aufteilung wurde bis dato nicht konsequent eingehalten. So befinden sich zum Beispiel die Managementinterfaces eines Switches in diesem Netzwerk, andere aber, wie bereits erwähnt, im internen Netz. Ein Netzwerk für Management-Systeme ist grundsätzlich wünschenswert. Da derartige Systeme aber in diesem und im internen Netzwerk aufgeteilt sind, bringt dieses Management-Netzwerk derzeit noch keinen Vorteil. Aufgrund der halbherzigen Aufteilung erhöht es sogar die Komplexität der gesamten Netzwerkstruktur dieser Tageszeitung.

Die für das Monitoring relevanten Systeme dieses Netzwerks sind:

- Managementinterface des Bladecenters (10.49.0.5)
- Managementinterface des Switches der Transport-Netzwerke (10.49.0.10)
- Managementinterface des SAN (Storage Area Network) (10.49.0.20)
- Nodes des Checkpoint Clusters (10.48.0.247-248)
- Virtuelles Interface des Checkpoint Clusters (10.49.0.253)

### *IP-Telefonie*

Dieses Netzwerk besteht nur aus Systemen, die in direktem Zusammenhang mit der IP-Telefonie stehen. Es umfasst die Telefonanlage selbst und die IP-Telefonie-Endgeräte. Die Server der Telefonanlage und die Endgeräte müssen sich im gleichen Subnetz befinden. Somit ist dieses Netz korrekt aufgebaut und es besteht eine saubere Trennung zu anderen Bereichen des Netzwerks.

In diesem IP-Bereich ist neben den Interfaces der Firewalls nur der Telefonanlagen-Server für das Monitoring relevant:

- Nodes des Checkpoint Clusters (10.49.100.1-2)
- Virtuelles Interface des Checkpoint Clusters (10.49.100.3)
- Telefonanlagen-Server (10.49.100.5)

### *Externe Netzwerke*

Wie bereits mehrfach erwähnt, sind im Zuge der Analyse der Netzwerkstruktur der Tageszeitung auch einige Systeme in externen Netzen zu beachten. Obwohl diese Systeme nicht direkt verwaltet werden können, ist es möglich, zumindest die Erreichbarkeit mit Hilfe eines Network-Monitoring-Systems zu überprüfen.

In einem dieser externen Netzwerke befindet sich auch das Monitoring-System. Diese Platzierung ist nicht ideal, da bei einem Ausfall der Verbindung die gesamte Überwachung für das Netzwerk der Tageszeitung ausfällt. Die IT-Abteilung wurde jedoch ausgelagert und befindet sich nicht am selben Standort wie die Redaktion der Tageszeitung. Da der Monitoring Server virtualisiert wurde, um Hardwarekosten zu sparen, und sich die VMWare Infrastruktur am Standort der IT-Abtailung befindet, ist keine andere Lösung möglich.

Die für das Monitoring relevanten externen Systeme sind (hier werden aus Gründen der Sicherheit keine IP Adressen angegeben):

- FTP Server der Druckerei – über Standleitung verbunden
- Großrechner für die Buchhaltung – über Standleitung verbunden
- Großrechner für die Kundenverwaltung – über Standleitung verbunden
- Monitoring-System – über VPN verbunden
- Router der Firma Liwest
- Webserver

Wie man erkennen kann, ist hier kein System der APA aufgelistet. Die relevanten Daten werden im Moment von der APA über das Internet an das Redaktionssystem übermittelt. Dies soll in den nächsten Monaten geändert werden. Dann werden die Daten über eine Standleitung direkt eingespielt und nicht zuvor unverschlüsselt über das Internet übertragen.

#### 3.1.1.2 Netzwerkkomponenten

Nachdem nun die einzelnen IP-Subnetze der Tageszeitung erläutert wurden, wird auf die Netzwerkkomponenten eingegangen. Da eine vollständige Auflistung aller relevanten Daten der einzelnen Komponenten den Rahmen der Arbeit sprengen würde und nicht wesentlich zum Verständnis des Projekts beiträgt, werden nur die wichtigsten Charakteristika der Komponenten erwähnt.

##### *Hardware*

Für die Server sind zwei unterschiedliche Hardware Systeme zu unterscheiden. Einerseits sind stand-alone Server der Firma IBM vorhanden, andererseits gibt es ein Bladecenter der Firma SecureGuard. Beide Systeme besitzen Management-Controller. Das Bladecenter unterstützt SNMP, die Server der Firma IBM verwenden DMI, welches, wie bereits erklärt, auf SNMP gemapped werden kann. Die Switches sind von der Firma Hewlett-Packard und ermöglichen Network-Management über SNMP. Das SAN System, als letztes relevantes Hardwaresystem, ist vom Hersteller Eurostor und verfügt ebenfalls über SNMP Funktionalitäten.

##### *Software*

Auf der soeben beschriebenen Hardware laufen verschiedene Softwareprodukte, welche im Folgenden erwähnt werden.

Für die Server des Redaktionssystems wird Linux Mandriva 2008 als Betriebssystem verwendet. Die restlichen Server laufen auf Windows Server Standard Edition 2003. Einige veraltete Systeme verwenden Windows Server 2000, diese scheiden jedoch in den nächsten Monaten aus und sind daher nicht mehr von Relevanz.

Tabelle 8 zeigt die wichtigsten Softwarekomponenten, welche direkt verwaltet werden. Nur bei diesen Komponenten sind Änderungen der Konfiguration möglich, wenn sie für das Network-Monitoring erforderlich sind. Alle anderen Systeme, wie zum Beispiel der FTP Server der Druckerei, können nur im Rahmen der gegebenen Möglichkeiten überprüft werden. Aus diesem Grund ist die Software dieser Komponenten im Rahmen dieser Auflistung nicht von Bedeutung.

| Software | Funktion |
|---|---|
| | |
| Microsoft Exchange Server 2003 Std | Email-Verkehr |
| Citrix Presentation Server 9.5 (Serverfarm) | Verwaltung der Terminalsitzungen |
| Apache 2.2 | Webserver des Redaktionssysteme |
| MySQL 4.1 | Datenbank des Redaktionssystems |
| ON2XML | Applikationsserver des Redaktionssystems |
| LAMP (Apache 2.0, MySql 4.1, PHP 4.3) | Webserver für die Homepage der Zeitung |
| WhatsUp Gold v11 | Network-Monitoring-System |
| Checkpoint NGX60 | Firewall-Software |

**Tabelle 8: Softwarekomponenten**

Nachdem die für diese Arbeit interessantesten Punkte der technischen Netzwerkanalyse angeschnitten wurden, folgt nun der zweite Teil der Netzwerkanalyse.

### 3.1.1 Qualitative Netzwerkanalyse

Die qualitative Netzwerkanalyse wurde nach dem in Abschnitt 2.5.1 beschriebenen QFD-Verfahren durchgeführt. Für eine möglichst umfassende Analyse wurden neben den Administratoren auch die Geschäftsführung und zwei Mitarbeiter der einzelnen Abteilung miteinbezogen. Des Weiteren wurden offene Interviews mit den Netzwerk-Administratoren geführt. Dies sollte weitere Aufschlüsse im Hinblick auf das produktbezogene Anforderungsprofil geben. Da das eigentliche Verfahren bereits erklärt wurde, werden in der Folge nur mehr die Ergebnisse präsentiert.

Mittels des QFD-Verfahren wurden folgenden Anforderungskriterien identifiziert. Diese sind in der nachfolgenden Liste nach ihrer Priorität gereiht:

1. Stabilität der redaktionellen Arbeit (Redaktionssystem, Email-Verkehr, Terminaldienste, Verbindung zur Druckerei, Verbindung zur APA, VoIP)
2. Performance der Homepage

3. Stabilität der Buchhaltung und der Kundenverwaltung
4. Performance des internen Netzwerks

Die Interviews mit den Administratoren bezogen sich hauptsächlich auf das Network-Monitoring-System selbst. Hier wurde verlangt, dass das System intuitiv zu bedienen sei und einen schnellen Überblick über den Zustand des Netzwerks ermöglicht. Die Forderung nach Intuitivität der Bedienung wurde in den Gesprächen nicht weiter konkretisiert. Sie kann, wie bereits erwähnt, nur im Zuge praktischer Tests der in Frage kommenden Produkte durch die Administratoren konkretisiert werden. Als weiterer Punkt wurde der Wunsch nach einem individuell gestaltbaren Benachrichtigungssystem geäußert. Da die Administratoren in der Vergangenheit schlechte Erfahrungen mit zusätzlichen Hilfsprogrammen auf produktiven Servern gemacht haben, wird verlangt, dass das System ohne auf den Servern zu installierenden Agenten auskommt.

Die Ergebnisse der Analyse und der Interviews wurden der Geschäftsführung präsentiert. Diese stimmte den oben angeführten Punkten vollinhaltlich zu. Als weiteres Kriterium wurde verlangt, dass es Administratoren möglich sein muss, sich innerhalb von zwei Werktagen in das System einzuarbeiten. Auch wurde die Möglichkeit der Übermittlung von Berichten über den Zustand des Netzwerks für die Geschäftsführung gefordert. Schließlich wurden im Rahmen dieses Treffens die maximalen Prozesskosten zur Inbetriebnahme des Systems festgelegt.

## 3.2 Anforderungsprofil

Wie im Vorgehensmodell beschrieben folgt auf die Netzwerkanalyse die Erstellung des daraus resultierenden Anforderungsprofils. Die Kernpunkte des netzwerkbezogenen und des produktbezogenen Anforderungsprofils werden in den folgenden Abschnitten herausgearbeitet.

### *Netzwerkbezogenes Anforderungsprofil*

Die Forderung nach einer hohen Stabilität der redaktionellen Arbeit verlangt nach einem aktiven Network-Monitoring-System. Um die Reaktionszeit auf Fehler zu minimieren, sollte jedoch auch eine passive Überwachung eingesetzt werden.

Aufgrund der im letzten Kapitel genannten vorhandenen Netzwerk- und Softwarekomponenten müssen folgende Punkte unterstützt werden:

- SNMP
- WMI
- TCP/IP Abfragen folgender Protokolle (dhcp, dns, ftp, http, smtp)

Neben diesen grundlegenden Voraussetzungen muss es möglich sein, selbständig Tests zu erstellen, um proprietäre Dienste, wie zum Beispiel den XML Server des Redaktionssystems, überwachen zu können. Außerdem sollten mehrere Subnetze im Rahmen einer Instanz des Monitoring-Systems überwacht werden können.

### *Produktbezogenes Anforderungsprofil*

Im Rahmen der Netzwerkanalyse haben sich folgende produktbezogene Anforderungen herausgebildet:

| | |
|---|---|
| Kaufpreis | höchstens 7000 € |
| Einarbeitungszeit | höchstens zwei Tage |
| Darstellung | übersichtliche, graphisch unterstützte Darstellung, der überwachten Systeme und ihrer Zustände |
| Benachrichtigung | per Mail oder SMS zeit- und personenabängig |
| Agenten | nicht erwünscht |

**Tabelle 9: Produktbezogene Anforderungen**

Es wurden keine Vorgaben bezüglich der benötigten Hardware des Systems gemacht, da das Monitoring-System virtualisert werden soll. Systeme, welche proprietäre Hardware benötigen würden, scheiden aufgrund der Festlegung der Höhe der Prozesskosten von vornherein aus.

## 3.3 Produktentscheidung

Nachdem im vorangegangen Abschnitt aus einer detaillierten und umfassenden Netzwerkanalyse ein vollständiges Anforderungsprofil erstellt wurde, wird nun der Auswahlprozess des schließendlich verwendeten Produkts nachvollzogen.

Zuerst wird eine allgemeine Selektion, welche auf den wesentlichen Kriterien des Anforderungsprofils beruht, durchgeführt. Die passenden Produkte werden danach einer genaueren Analyse unterzogen, bevor - anhand von Beispielkonfigurationen - die zwei relevanten Produkte miteinander verglichen werden.

### 3.3.1 Allgemeine Evaluierung

Am Markt befinden sich unzählige Network-Monitoring Lösungen. Manche werden kommerziell vertrieben, wie HP OpenView, andere sind frei erhältlich, wie zum Beispiel Nagios. Obwohl viele Programme sehr umfangreich sind, hat jedes Tool spezielle Vorteile und Nachteile. Dadurch muss vor der Erstellung einer neuen Network-Monitoring Umgebung eine Evaluierung der zur Verfügung stehenden Produkte durchgeführt werden. Nur so kann für das jeweilige Projekt das am Besten geeignete Produkt identifiziert werden.

Um eine Vorstellung von der Anzahl der zur Auswahl stehenden Produkte zu geben, sind nachfolgend alle Tools aufgelistet, welche im Rahmen dieses Projekts evaluiert wurden:

- SAP Solution Manager
- CA Spectrum Unicenter/Enterprise Man.
- Microsoft Operation Manager
- SysLink Xandria
- IBM Tivoli
- HP Open View
- ManageEngine OpManager
- IPSWITCH WhatsUp Professional 2006
- Intellipool Network Monitor
- Evalesco Systems SysOrb
- MRTG
- Nagios
- ruleIt Monitor Server

- Solarwinds Orion Network Performance Monitor v8
- GFI Network Server Monitor
- HYPERIC HQ
- Opensmart
- Zenoss
- Big Brother

Wie bereits beschrieben, führt eine erste allgemeine Evaluierung anhand von den identifizierten Hauptkriterien zu einer Verdichtung der möglichen Alternativen. Tabelle 10 zeigt die Hauptkriterien im Rahmen des vorgestellten Projekts mit ihrer jeweiligen Priorität. Diese Tabelle ergibt sich aus dem in Anschnitt 3.2 erarbeiteten Anforderungsprofil.

| Kriterium | Priorität |
|---|---|
| | |
| Usability | Sehr Hoch |
| Technische Möglichkeiten | Hoch |
| Preisgestaltung | Mittel |
| Erweiterbarkeit | Niedrig |

**Tabelle 10: Allgemeine Auswahlkriterien**

In den nächsten Abschnitten werden die einzelnen Kriterien nochmals beschrieben und auf die oben genannten Alternativen angewandt. Jene Produkte, welche aufgrund der Hauptkriterien ausscheiden, werden tabellarisch mit einer Begründung aufgelistet.

## *Usability*

Die Usability umfasst alle Anforderungen an die Bedienung der Software. Sowohl eine intuitive Nutzung als auch eine einfache Konfiguration muss möglich sein. Weiters ist die Übersichtlichkeit der Oberfläche des Network-Monitoring Tools in Betracht zu ziehen. Diese soll im Rahmen dieses Projekts ohne Zusatzsoftware aufrufbar sein. Im vorliegenden Projekt wurde zudem festgelegt, dass keine zusätzlichen Network-Monitoring Agents auf den einzelnen Servern installiert werden dürfen.

In einer ersten Evaluierung werden die Produkte, welche keinesfalls entsprechen, aussortiert. Der effektive Grad der Usability kann jedoch nur durch die tatsächlichen Benutzer endgültig entschieden werden.

Anhand des Kriteriums “Usability“ aussortierte Produkte:

| Produkt | Begründung |
|---|---|
| | |
| Opensmart | Bedienung zu komplex (Herbst, 2008) |
| Hyperic HQ | agentenbasierte Lösung |
| Evalesco Systems SysOrb | agentenbasierte Lösung |
| Big Brother | agentenbasierte Lösung |
| ruleIT Monitor Server | agentenbasierte Lösung |
| CA Unicenter | Bedienung zu komplex; Workshops zum Erlernen der Bedienung empfohlen (CA, 2008) |

**Tabelle 11: Auswahlkriterium “Usability“**

## *Technische Möglichkeiten*

Alle Protokolle, die in der technischen Netzwerkanalyse ermittelt wurden, sollen durch das Network-Monitoring Tool unterstützt werden. Weiters müssen die im Rahmen des Anforderungsprofils vereinbarten Möglichkeiten des Reporting und Alerting gegeben sein.

Anhand des Kriteriums “Technische Möglichkeiten“ aussortierte Produkte:

| Produkt | Begründung |
|---|---|
| | |
| MRTG | WMI nicht unterstützt |
| Zenoss | WMI nicht unterstützt |
| Solarwinds Orion Monitor | WMI nicht unterstützt |
| SysLink Xandria | hauptsächlich für die Überwachung von SAP Anwendungen geeignet |

| | |
|---|---|
| GFI Network Server Monitor | WMI Abfragen nur über VBScripts möglich |
| SAP Solution Manager | nur für die Überwachung von SAP Anwendungen geeignet |

**Tabelle 12: Auswahlkriterium "Technische Möglichkeiten"**

## *Preisgestaltung*

Der Einkaufspreis des Produkts ist in diesem Projekt durch die maximalen Prozesskosten beschränkt. Durch die Forderung nach einer möglichst einfachen Bedienung und Erweiterbarkeit wird implizit verlangt, dass keine technische Unterstützung für den Betrieb der Network-Monitoring Lösung benötigt wird. Die Geschäftsführung erwartet ein flexibles Produkt, das zusätzlich zu den einmaligen Anschaffungskosten und den laufenden Personalkosten keine weiteren Aufwendungen verursacht.

Anhand des Kriteriums "Preisgestaltung" aussortierte Produkte:

| Produkt | Begründung |
|---|---|
| | |
| HP Open View | keine unbeschränkte Lizenzierung möglich; zu hoher Preis |
| IBM Tivoli | keine unbeschränkte Lizenzierung möglich; zu hoher Preis |
| Microsoft Operation Manager | Erweiterungen müssen außerhalb eines Partnerprogramms extra lizenziert werden |

**Tabelle 13: Auswahlkriterium "Preisgestaltung"**

## *Erweiterbarkeit*

Aus dem Anforderungsprofil geht hervor, dass es möglich sein muss, das Network-Monitoring-System an Änderungen der Infrastruktur einfach anzupassen. Neue Netzwerkkomponenten sollen während der Betriebszeiten in die Network-Monitoring Umgebung inte-griert werden können. Weiters soll es möglich sein, eigene Überwachungsfunktionen zu realisieren um die grundlegenden Überwachungsmöglichkeiten des Systems zu erweitern.

Anhand des Kriteriums "Erweiterbarkeit" aussortierte Produkte:

| Produkt | Begründung |
|---|---|
| | |
| Intelipool Network Monitor | eigene Überwachungsfunktionen nicht realisierbar |
| ManageEninge OpManager | nur vordefinierte WMI Werte können abgefragt werden |

**Tabelle 14: Auswahlkriterium "Erweiterbarkeit"**

### 3.3.2 Vorstellung der möglichen Alternativen

Im vorangegangen Abschnitt wurden viele Network-Monitoring Lösungen anhand der Hauptkriterien als nicht adäquat für das vorliegende Projekt befunden. Die restlichen Produkte, welche diesen Kriterien genügen, werden nun vorgestellt. In den kommenden Abschnitten wird in Folge einer detaillierten Evaluierung entschieden, welches Produkt tatsächlich eingesetzt wird, um eine Network-Monitoring-Umgebung im Netzwerk einer Tageszeitung zu implementieren.

Nach der allgemeinen Evaluierung bleiben zwei Produkte zur Auswahl, um eine Network-Monitoring Lösung im besagten Netzwerk zu realisieren:

- WhatsUp Gold von IPSwitch
- Nagios

Die Merkmale dieser Produkte werden nun detailliert vorgestellt, bevor im Rahmen einer Beispielkonfiguration eine detaillierte Evaluierung durchgeführt wird.

#### *WhatsUp Gold von IPSwitch*

WhatsUp Gold in der Version 11 wurde von der Firma IPSwitch mit folgendem Ziel entwickelt:

*"Designed for organizations that need to monitor their single-location network 24/7, WhatsUp Gold Premium can be implemented in any environment in under one hour and enables you to discover your network in minutes. All network information is stored in a relational database to*

*enable easy and efficient device management and reporting."* (IpSwitch, 2007)

Diese Zielvorgabe der Firma gibt den besonderen Fokus dieses Produkts an. Es ist für einzelne Netzwerke unter der Prämisse entwickelt worden, dass sehr rasch eine Network-Monitoring-Umgebung erstellt werden kann. Weiters wird besonderer Wert auf Übersichtlichkeit gelegt.

Folgende Key-Features, welche im Anschluss genauer erläutert werden, sind für die Premium Version des Produkts angeführt (IpSwitch, 2007):

- SNMP v1-3 support
- WMI support
- Web interface/Reporting
- Visual mapping
- Personalized workspaces
- Device dependency

Diese Auflistung zeigt, dass alle Anforderungen der gestellten Vorgaben durch dieses Produkt erfüllt werden können. Eine Ausnahme bildet das von den Serverherstellern - IBM, Intel – implementierte DMI Protokoll. Dieses Protokoll kann aber, wie bereits erwähnt, vernachlässigt werden, da es ohne Einbußen der Funktionalität auf das SNMP Protokoll gemapped werden kann. In Bezug auf WMI ist hier anzumerken, dass nur die Premium Version des Produkts von speziellem Interesse für dieses Projekt ist. Nur diese Version unterstützt das im Anforderungsprofil geforderte Protokoll in ausreichendem Maße.

Weitere angeführte Features sind Web Interface/Reporting und Visual Mapping, von dem das Unternehmen eine Drag-and-Drop Umgebung für den Umgang mit dem Programm verspricht. Die genannten Punkte erfüllen diese Forderung nach einer einfachen Bedienung. Durch Personalized Workspaces ist die Möglichkeit von individuellen Sichten gegeben, wodurch die Möglichkeit zur Anpassung an Zielgruppen erlangt wird. Als letztes Feature dieser Auflistung wird Device Dependency angegeben. IpSwitch beschreibt damit die Möglichkeit, Abhängigkeiten im Netzwerk abzubilden. Erst durch dieses Feature ist sichergestellt, dass das zugrundeliegende Netzwerk realitätsgetreu abgebildet werden kann.

Da die genannten Eigenschaften des Produkts Werbebotschaften des Unternehmens IpSwitch sind, werden diese Angaben nach der Vorstellung des Konkurrenzprodukts – Nagios v3.0 - anhand einer detaillierten Evaluierung überprüft.

Bevor nun auf Nagios v3.0 eingegangen wird, zeigt Tabelle 15 die Preisstruktur von WhatsUp Gold v11 Premium Version:

| Anzahl der überwachten Geräte | Preis |
|---|---|
| | |
| Bis zu 100 Geräte | € 2 595 |
| Bis zu 300 Geräte | € 3 795 |
| Bis zu 500 Geräte | € 4 995 |
| Mehr als 500 Geräte | € 6 995 |

**Tabelle 15: Preistabelle WhatsUp Gold v11 Premium Version (IpSwitch, 2008)**

Man erkennt in der Tabelle eine gestaffelt Preisstruktur auf Grundlage der zu überwachenden Komponenten. Wie im Anforderungsprofil erwähnt, ist es möglich eine unlimitierte Lizenz zu erwerben. Im vorliegenden Netzwerk sollte eine Lizenz für 300 Geräte ausreichen, da diese genügend Spielraum für Erweiterungen des aktuellen Netzwerks bereitstellt und um mehr als ein Drittel billiger ist als die unlimitierte Version.

### *Nagios*

Im Gegensatz zu WhatsUP Gold ist Nagios kein kommerzielles Produkt. Dieses Network-Monitoring-Tool unterliegt der GPL (GNU, 2007). Aus diesem Grund fallen keine direkten Anschaffungskosten für die Software an. Für Supportanfragen stehen mehrere Dienstleistungsunternehmen, wie zum Beispiel Nagios Enterprises, zur Verfügung, welche gegen Bezahlung bei Problemen mit Nagios unterstützend tätig werden.

Eine kostenfreie Alternative der Unterstützung lässt sich in zahlreichen Internetforen finden. Das bekannteste englischsprachige Forum ist MEULIE (www.meulie.net), welches Unterstützung von der Installation bis zur Wartung der fertigen Network-Monitoring-Lösung bietet.

Diese breite Unterstützung macht Nagios besonders interessant für das Projekt, da ohne persönliches Know-How rasch Lösungen zu auftretenden Problemen gefunden werden können.

Die folgende Evaluierung zeigt jedoch, dass der Umgang mit Nagios mehr Einarbeitungszeit verlangt als zum Beispiel WhatsUp Gold. Dies gründet unter anderem auf der zugrundeliegenden Logik von Nagios (Abbildung 10).

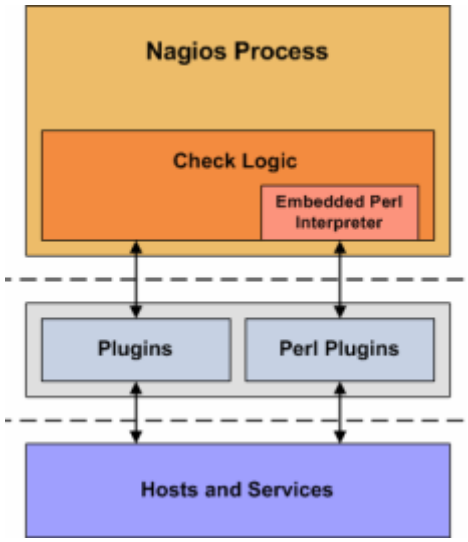


**Abbildung 10: Programmlogik von Nagios (Nagios, 2007a)**

Abbildung 10 zeigt, dass Nagios (in der Darstellung Nagios Process genannt) im Gegensatz zu anderen Produkten keine vollständige Network-Monitoring-Lösung ist. Dieser Prozess realisiert, der Gliederung in Abschnitt 2.1 folgend, nur die Funktion des Managers. Über Konfigurationsdateien können Abfragen gesteuert werden. Die Ergebnisse könnten an unterschiedliche Monitoring-Programme weitergeleitet werden, wobei Nagios selbst ein standardmäßiges Monitoring-Programm integriert hat. Network-Management-Agents, in Nagios PlugIns genannt, werden über Scripts angesprochen und stellen eigenständige Programme dar. Um sie in Nagios zu verwenden, muss jedoch garantiert sein, dass die Ausgabe der Plugins den Vorgaben des Nagios API entspricht (Nagios, 2007b). Aufgrund dieser Struktur besteht auf einfache Weise die Möglichkeit, eigene Plugins für Nagios zu entwickeln. Eine der größten Sammlungen derartiger Plugins ist Nagiosexchange (http://www.nagiosexchange.org/). Hier finden sich Lösungen zur Abfrage von verschiedenen Hardwarekomponenten sowie unterschiedlichen Netzwerkdiensten.

Obwohl die Standardinstallation von Nagios, welche einige grundlegende Plugins enthält, nicht die im Anforderungsprofil geforderte Unterstützung des WMI Protokolls gewährleistet, finden sich in den beschriebenen Plugin-Sammlungen Lösungen zur Unterstützung vieler Protokolle. Aufgrund dieser breiten Unterstützung, vor allem durch die Erweiterungen und den

Support der Nagios Community, ist dieses Produkt geeignet zur Implementierung der Netzwerküberwachung im Netzwerk dieser Tageszeitung.

Die nachfolgende detaillierte Evaluierung zeigt, welches der beiden in den vorangegangenen Abschnitten besprochenen Produkte – Nagios oder WhatsUP Gold – geeigneter zur Realisierung des Projekts ist. Um diese Entscheidung fällen zu können werden beide Programme in einem umfangreichen Praxistest miteinander verglichen.

### 3.3.3 Installation der Produkte

Die Standardinstallation beider Produkte ist sehr einfach und kann rasch durchgeführt werden. Die Installation wird für beide Produkte in der Folge im Überblick dargestellt.

#### *WhatsUP Gold*

Die Installationsdatei von WhatsUP Gold für Microsoft Windows kann von der Homepage des Herstellers bezogen werden. Die Installation an sich folgt einer typischen Installation von Windowsprogrammen.

Die Platzierung der Datenbank für die Speicherung der Abfragewerte von WhatsUP Gold ist jedoch besonders wichtig. IpSwitch gibt an, dass es abhängig von der Anzahl der Abfragen und der Aufbewahrung von Historiendaten dazu kommen kann, dass die Datenbank bis zu ihrer maximalen Größe von 5 GB anwachsen kann. Genaue Werte, wann dies der Fall ist, werden jedoch nicht angegeben (IpSwitch, 2006). Da das nachträgliche Verlegen der Datenbank nicht möglich ist, sollte bereits bei der Installation eine ausreichend große Partition ausgewählt werden. Außerdem sollten die Partitionen auf performanten Speichermedien abgelegt werden, um eine gute Performance des Network-Monitoring-Systems zu gewährleisten (Abbildung 11).

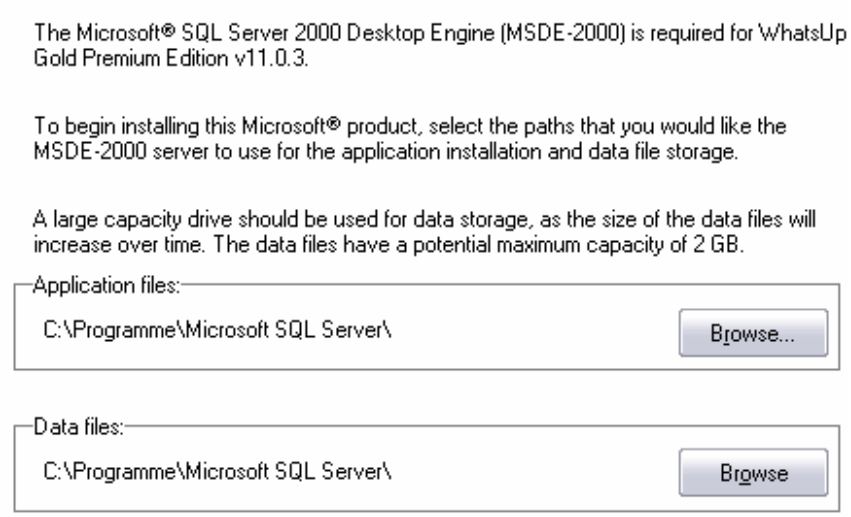


**Abbildung 11: Installationsdialog zur Auswahl der Datenbank von WhatsUp Gold**

Da IPSwitch jedoch angibt, dass nicht einmal 1000 Monitored Devices diese maximale Göße ausnutzen, kommt diese Problematik nur in wirklich großen Netzwerken zum Tragen (IpSwitch, 2006).

Nach einer erfolgreichen Installation ist das Tool unmittelbar betriebsbereit. Die Konfiguration kann sofort begonnen werden, welche unverzüglich zu einer aktiven Netzwerküberwachung führt.

### *Nagios*

Auch die Standardinstallation von Nagios ist nicht sehr komplex. Die Installation kann hier auf mehrere Arten durchgeführt werden. Einerseits kann der Quellcode des Tools eigens kompiliert werden oder es kann eine vorkompilierte Variante mit Hilfe von Installationsscripts ausgeführt werden. Eine andere Möglichkeit ist die Verwendung eines Paketmanagers. Für viele Distributionen gibt es fertige Pakete, welche die Installation erheblich vereinfachen. Unter CentOS 4.5 und der Verwendung des Paketmanagers YUM beschränkt sich die Standardinstallation von Nagios auf die folgende Zeile:

yum install nagios

Abbildung 12 zeigt die Ausgabe des Paketmanager.

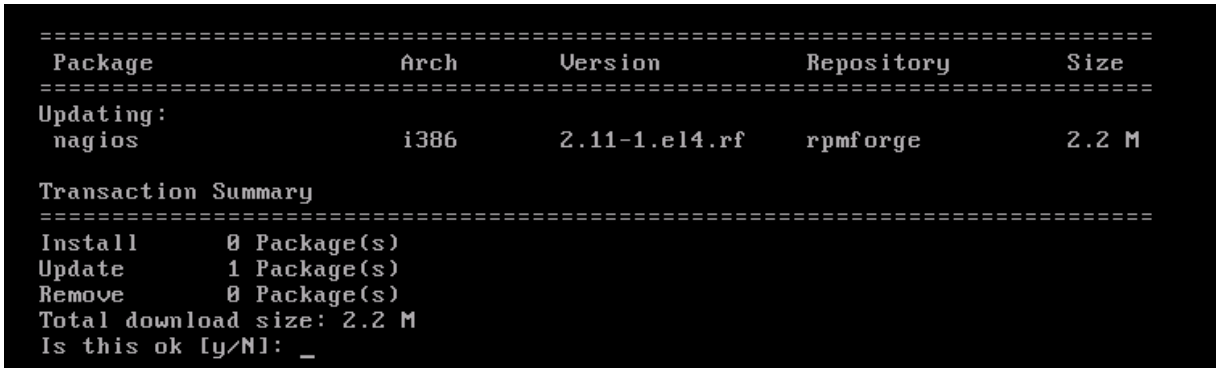


**Abbildung 12: Installation von Nagios mit YUM**

Zusätzlich sollten die Standard-Plugins von Nagios installiert werden, was mithilfe von YUM durch folgenden Konsolenbefehl erfolgt:

yum install nagios-plugins

Durch diese beiden Pakete werden Nagios und besagte Plugins in das System eingespielt und die nötigen Modifikationen an diversen Konfigurationsdateien vorgenommen. So werden die Konfigurationsdateien des Webservers um folgende Einträge erweitert:

*ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin*
*<Directory "/usr/local/nagios/sbin">*
*Options ExecCGI*
*AllowOverride None*
*Order allow,deny*
*Allow from all*
*AuthName "Nagios Access"*
*AuthType Basic*
*AuthUserFile /usr/local/nagios/etc/htpasswd.users*
*Require valid-user*
*</Directory>*

*Alias /nagios /usr/local/nagios/share*
*<Directory "/usr/local/nagios/share">*
*Options None*
*AllowOverride None*
*Order allow,deny*
*Allow from all*
*AuthName "Nagios Access"*
*AuthType Basic*

*AuthUserFile /usr/local/nagios/etc/htpasswd.users*

*Require valid-user*

*</Directory>*

Dies ermöglicht den Zugriff auf das mitgelieferte Webinterface von Nagios, nachdem Userdaten in der dafür vorgesehenen Datei "*htpasswd.users*" mittels *"htpasswd –c filename user"* angelegt wurden. Das Interface ist nicht sehr umfassend und bietet keine Konfigurationsmöglichkeiten. Die überwachten Elemente werden jedoch übersichtlich dargestellt. Die Konfiguration muss, wie später ausführlicher beschrieben, direkt in den einzelnen Konfigurations-dateien vorgenommen werden. Auch Nagios befindet sich nach der Installation bereits in Betrieb. Um Konfigurationsänderungen wirksam zu machen, muss das System jedoch jeweils neu gestartet werden.

Wie in Kapitel 3.3.2 erwähnt, gibt es weitere Monitoring Programme, welche Nagios als Basis verwenden. Im Gegensatz zu Nagios ermöglichen derartige Programme oft eine Konfiguration über ein Webinterface. Dies wäre besonders für die zukünftigen Administratoren dieses Network-Monitoring Projekts hilfreich, da sie wenig Erfahrung im Umgang mit Linux besitzen. Eines dieser Systeme ist Centreon, dessen Installation im Überblick gezeigt wird, da es aufgrund seines Umfangs von besonderem Interesse ist.

Im Gegensatz zu Nagios selbst gibt es für Centreon keine vorgefertigten Pakete. Die Installation erfolgt mit Hilfe von Installationsskripten. Vor der Durchführung des Scripts müssen ca. 50 Bibliotheken und Hilfsprogramme eingespielt bzw. auf die jeweilige Version überprüft werden (Oreon, 2007). Nach diesen Vorbereitungen benötigt man im Zuge der Installationsroutine detailliertes Wissen über das zugrundeliegende System. Unter anderem müssen folgende Fragen beantwortet werden:

- Where is sudo?
- Where is installed RRD perl module?
- Where is rrdtool binary?
- Where is mail binary?
- Where is PEAR path?
- What is name of apache user?

Es zeigt sich somit, dass die Installation von Centreon nicht so einfach ist wie von Nagios selbst oder WhatsUP Gold. Es gibt weitere auf Nagios basierende Monitoring Programme, welche einfacher zu installieren sind. Intensive Recherchen und weitere Evaluierungen haben jedoch ergeben, dass Centreon mehr Konfigurationsmöglichkeiten von Nagios unterstützt als vergleichbare Konkurrenzprodukte.

### *Fazit*

Sowohl die Installation von WhatsUP Gold als auch die Paketinstallation von Nagios ist einfach durchzuführen. Nagios kann aus den bereits erwähnten Gründen in diesem Projekt jedoch nicht ohne eine vernünftige grafische Unterstützung der Konfiguration betrieben werden. Deshalb muss hier auch die Installation von Centreon beachtet werden. Diese ist umständlicher und benötigt eine gewisse Praxis im Umgang mit Linux.

## 3.3.4 Konfiguration

Nachdem die Installation der beiden Produkte beschrieben wurde, wird in der Folge die Konfiguration behandelt. Anhand eines Beispielszenarios wird die Konfiguration der Tools vorgestellt. Um einen verständlichen Überblick über die unterschiedlichen Vorgehensweisen der Programme vermitteln zu können, wird dabei nicht auf alle Details eingegangen.

Das gewählte Beispielszenario ist die Überwachung eines Webservers, der auf einem Windows Betriebssystem betrieben wird. Einerseits soll die Erreichbarkeit und andererseits die korrekte Funktion überwacht werden. Weiters sollen Performancedaten des Webservers ausgelesen werden, um mögliche Engpässe im Vorhinein identifizieren zu können. Warnungen sollen per SMS an eine festgelegte Nummer geschickt werden. Die Darstellung der Abfragen wird in einem späteren Kapitel gesondert behandelt. Die konkreten Anforderungen im Beispielszenario sind folgende:

- Überprüfung ob Port 80 erreichbar ist
- Überprüfung ob die Webseite den korrekten Inhalt anzeigt (“Test“)
- Anzeige der aktuellen Nutzer des Webservers
- Versand einer SMS, wenn sich der Inhalt der Webseite verändert.

Um ein bestmögliches Verständnis für die Konfiguration der Produkte zu gewährleisten, werden alle Anforderungen zuerst in Nagios und danach in WhatsUP Gold konfiguriert. Nachdem beide Systeme einzeln betrachtet wurden, wird auf die Unterschiede und die Vorteile bzw. Nachteile in der Konfiguration dieser Produkte eingegangen.

## *Nagios*

Bevor auf die praktische Umsetzung des Testszenarios eingegangen werden kann, muss die Konfiguration von Nagios auf allgemeiner Basis erklärt werden. Grundsätzlich wird Nagios über Konfigurationsdateien gesteuert. Sowohl allgemeine Programmparameter, wie zum Beispiel der User unter dem das Programm läuft, als auch alle benötigten Angaben zur Netzwerküberwachung selbst werden in diesen Textdateien eingestellt. Da hier nicht in die Tiefe gegangen wird, werden nur die für das Beispielszenario unbedingt benötigten Dateien für Überwachungseinstellungen behandelt.

Im Wesentlichen sind für die Erfüllung der oben genannten Anforderungen folgende Dateien von besonderem Interesse:

| Konfigurationsdatei | Aufgabe |
|---|---|
| | |
| commands.cfg | Konsolenbefehle zum Aufruf externer Plugins |
| hosts.cfg | Konfiguration Netwerkkomponenten und der Empfänger im Benachrichtigungsfall |
| Services.cfg | Konfiguration der Serviceabfragen und der Empfänger im Benachrichtigungsfall |
| Contacts.cfg | Kontaktdaten von Empfängern |
| Timeperiods.cfg | Zeitperioden zur Steuerung von Abfrage- und Benachrichtigungszeiten |

**Tabelle 16: Konfigurationsdateien von Nagios**

Weiters müssen auch die Dateien hostgoups.cfg, servicegroups.cfg und contactgroups.cfg erwähnt werden, welche zur Gruppierung der einzelnen Elemente dienen. Diese Gruppierung ist im Fall der Empfänger von Benachrichtigungen obligatorisch. Ansonsten haben diese Dateien aber im Beispielszenario keine weitere Bedeutung.

Es wird darauf hingewiesen, dass die vorgestellte Struktur nicht zwingend vorgegeben ist. In Nagios könnten zum Beispiel auch sämtliche Parameter in einer Datei angegeben werden. Die vorgestellte Struktur und die verwendeten Namen orientieren sich jedoch an den Vorschlägen der offiziellen Nagios Dokumentation (Galstad, 2007).

Nachdem nun die verwendete Struktur erklärt wurde, wird in der Folge auf die einzelnen Elemente eingegangen. Die Angaben in den einzelnen Konfigurationsdateien werden anhand von Beispielen erläutert, welche auch für das Beispielszenario relevant sind. Zuerst wird die Verbindung von Nagios mit den bereits beschriebenen Plugins erläutert.

Bevor Plugins verwendet werden können müssen die benötigten Aufrufe durch “commands“ angegeben werde. Das “command“ zur Überprüfung der Erreichbarkeit eines Servers sieht folgendermaßen aus:

```
define command{
    command_name    check_host_alive                          // interner Name des Commands
    command_line    $USER1$/check_ping -H $HOSTADDRESS$       //auszuführender Konsolenbefehl
    }
```

Der command_name “check_host_alive“ kann nun von anderen Konfigurationsdateien verwendet werden, um den in command_line gewünschten Konsolenbefehl auszuführen. Das in command_line verwendete Makro “$HOSTADDRESS$“ bezeichnet das “address“-Feld einer Netzwerkkomponente. Nachstehend befindet sich eine exemplarische Konfiguration einer derartigen Komponenten, nämliche dem Webservers des Beispielszenario:

```
define host{
        host_name               testserver          // interner Name der Komponente
        alias                   testserver          // Label z.B. für Weboberfläche
        address                 192.168.150.105     // IP-Adresse der Komponente
        check_command           check_host_alive    //Comand zur Überprüfung der Erreichbarkeit
        max_check_attempts      5                   //Wiederholungen bei Zustandsänderung
        check_period            24x7                //Zeit, zu der Checks durchgeführt werden
        contact_groups          testcontactgroup    //Gruppe, der zu kontaktierenden Personen
        notification_interval   5                    //Zeit, zwischen Benachrichtigungen
        notification_period     24x7                // Zeit, zu der Notification ausgelöst werden
        notification_options    d,u,r               //Ereignisse, die eine Notification auslösen
}
```

In dieser Konfiguration wird der Name der Netzwerkkomponente und ein Alias, der als Label der Komponente in der Weboberfläche verwendet wird, angegeben. Danach wird die IP-Adresse festlegt. check_command ruft das oben beschriebene Kommando “check_host_alive“ mit dem Wert 192.168.150.105 für $HOSTADDRESS$ auf. Das Feld “max_check_attemps“ gibt an, wie oft das Kommando wiederholt wird, bevor der Status der überwachten Komponente auf “nicht erreichbar“ gesetzt wird. check_period gibt an, wann die Netzwerkkomponente überprüft werden soll. Die Periode “24x7“ wird in der timeperiod.cfg zum Beispiel mit folgenden Zeilen festgelegt und ist bei der Standardinstallation von Nagios bereits vorhanden. Sie sieht folgendermaßen aus:

```
define timeperiod{
        timeperiod_name     24x7                          //interner Name der Zeitperiode
        alias               24_Hours_A_Day,_7_Days_A_Week //Label z.B. für Weboberfläche
        sunday              00:00-24:00                   //Zeiten, die in Zeitperiode fallen
        monday              00:00-24:00
        tuesday             00:00-24:00
        wednesday           00:00-24:00
        thursday            00:00-24:00
        friday              00:00-24:00
        saturday            00:00-24:00
}
```

In der vorgestellten Konfiguration des Hosts werden als nächstes die contact_groups angegeben, welche die Empfänger von Benachrichtigungen enthalten. Der Versand einer Mitteilung erfolgt nach den in den notification-Parametern angegebenen Kriterien. notification_interval gibt an, nach wie vielen Minuten die Mitteilung wiederholt wird. notification_period gibt jene in timeperiod.cfg angegebene Zeit an, in der eine Benachrichtigung ausgeschickt werden kann. Schließlich werden in notification_options die Zustände des Servers angegeben, welche eine Benachrichtigung auslösen.

Im oben gezeigten Fall werden Mitteilungen generiert, wenn der Server sich in den Zuständen down (d), unreachable (u) oder recovered (r) befindet. Der Unterschied der Zustände down und unreachable liegt darin, dass bei down der Server grundsätzlich erreichbar wäre, aber nicht reagiert. unreachable bedeutet, dass der Server nicht erreichbar sein kann, da zum Beispiel ein Switch ausgefallen ist und somit keine direkte Verbindung möglich ist.

Das bereits erwähnte Feld “contact_groups“ gibt die Gruppe von Kontakten an, welche Empfänger etwaiger Nachrichten über den jeweiligen Host sind. Einzelne Empfänger werden folgendermaßen konfiguriert:

```
define contact{
        contact_name                    testuser        //interner Name des Empfängers
        alias                           testuser        //Label z.B. für Weboberfläche
        host_notification_period        24x7            //Zeit, zu der Hostereignisse übermittelt werden
        service_notification_period     24x7            //Zeit, zu der Serviceereignisse übermittelt werden
        host_notification_options       d,u,r           //welche Hostereignisse übermittelt werden
        service_notification_options    w, c, u,r       //welche Serviceereignisse übermittelt werden
        host_notification_commands      notify-by-sms   //Art der Benachrichtigung über Hostereignisse
        service_notification_commands   notify-by-sms   //Art der Benachrichtigung über Serviceereignisse
        email                           test@user.com   //Email-Adresse des Empfängers
        pager                           00437321111     //Pagernummer des Empfängers
}
```

Neben dem Namen und den Kontaktdaten, wie Email-Adresse und Pagernummer, werden die Benachrichtigungsoptionen angegeben. Auch wird festgelegt wie (notify-by-sms), bei welchem Ereignis (d, u, r) und zu welcher Zeit (24x7) ein Kontakt Mitteilungen empfangen kann. Hier wird unterschieden zwischen Nachrichten, welche Netzwerkkomponenten betreffen, und solchen, die aufgrund von überwachten Diensten abgeschickt werden. In der Folge werden die benötigten Einstellungen eines solchen Dienstes für die Überwachung der Erreichbarkeit des Port 80 angegeben:

```
define service{
        host_name                       testserver      //Host, welcher dieses Servicev bereitstellt
        service_description             http            //interner Name des Service
        check_command                   check_http      //command zur Überprüfung des Services
        max_check_attempts              5               //Wiederholungen bevor hard state erreicht wird
        normal_check_interval           5               //Checkintervall während hard state
        retry_check_interval            1               // Checkintervall während soft state
        check_period                    24x7            //Zeit, zu der Überprüfung durchgeführt werden
        notification_interval           5               //Intervall, zwischen zwei Benachrichtigungen
        notification_period             24x7            //Zeit, zu Notifications ausgelöst werden kann
        notification_options            d,u,r           //Ereignisse, die Notifications auslösen
        notification_options            w, c, u,r       //Ereignisse, die Notifications auslösen
        contact_groups                  testcontactgroup //Gruppe, der zu kontaktierenden Personen
}
```

Man erkennt, dass über das Feld host_name die Verbindung zu einem Serverelement hergestellt wird. Natürlich ist es auch möglich mehrere durch Beistriche getrennte Hosts oder Hostgroups anzugeben. Das Service wird dadurch auf allen angegeben Hosts überwacht. Die meisten Felder sind auch in anderen Konfigurationen vorhanden und wurden bereits erklärt. Zur Überprüfung des Port 80 wird das Kommando check_http verwendet. In commands.cfg steht der zugehörige Konsolenbefehl, welcher verwendet wird, um eine Verbindung auf den gewünschten Port herzustellen. Weiters ist hier das Feld retry_check_intervall von Interesse. Dieses gibt an in welchem Abstand die Überprüfung ausgeführt werden soll, wenn sich der Status des Services ändert (weicher Zustand). Wenn die max_check_attempts erreicht werden, wechselt der Zustand in einen harten Zustand und es wird wieder das normale check_intervall verwendet.

Die notification_options wurden noch nicht vollständig erklärt. Der Status unreachable (u) und recovered (r) wurden bereits erwähnt. Warning (w) und critical (c) ersetzen den Status down (d) in der Beschreibung eines Hosts. Durch die Aufteilung ist es möglich spezielle Benachrichtigungen zu versenden, wenn ein Service ein ungewöhnliches Verhalten (warning) aufweist und wenn dieses Service ein schwerwiegendes Problem meldet (critical).

Da es grundsätzlich nicht möglich ist einzelne contacts als Empfänger anzugeben, muss die Konfigurationsdatei zur Gruppierung von contacts erwähnt werden. Diese Elementbeschreibung ähnelt im Aufbau den Dateien zur Gruppierung von Servern und Diensten, weswegen nur die Beschreibung einer contact_group angeführt wird:

```
define contactgroup{
        contactgroup_name       testcontactgroup        //interner Name der Gruppe
        alias                   testcontactgroup        //Label z.B. für Weboberfläche
        members                 testuser, testuser2     //contacts dieser gruppe
}
```

Mit diesem Element ist die einführende Konfiguration von Nagios beendet. Das in den einzelnen Konfigurationen erkennbare komplexe Zusammenwirken der einzelnen Konfigurationsdateien wird in Abbildung 13 nochmals grafisch aufbereitet.

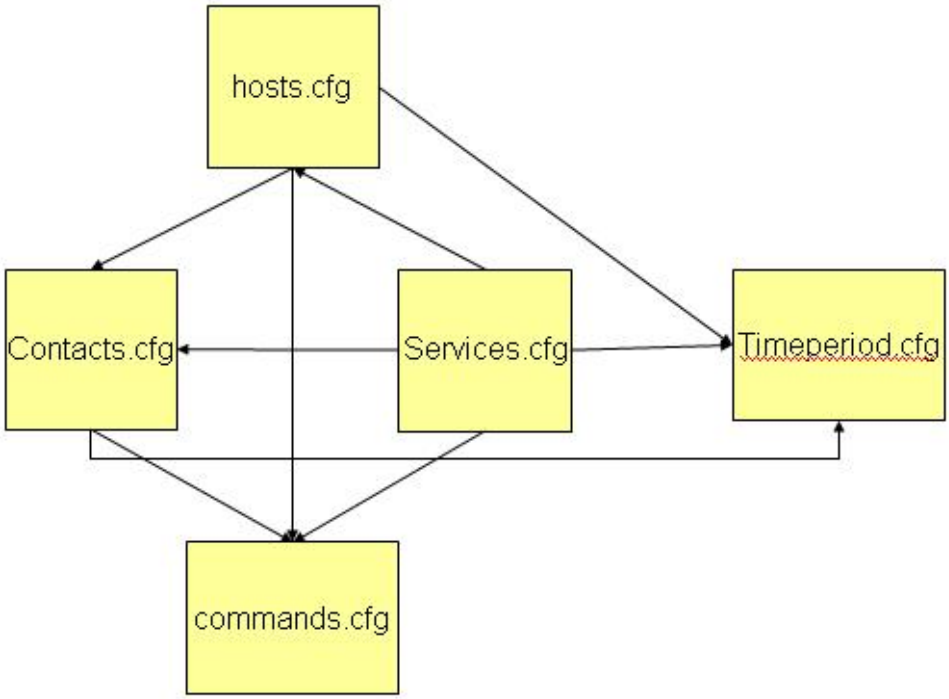


**Abbildung 13: Verbindung der Konfigurationsdateien von Nagios**

In der Folge werden die restlichen benötigten Angaben in Bezug auf das Beispielszenario gezeigt. Es werden hier nur jene Teile explizit angegeben, welche von den bereits vorgestellten Elementkonfigurationen abweichen. Aus diesem Grund werden hier nur mehr die zusätzlich benötigten Kommandos und Servicekonfigurationen angeführt ohne näher darauf einzugehen. Die Einstellungen des hosts, der timeperiod, des contacts, der contactgroup sowie das bereits beschriebene service und das vorgestellte command werden unverändert in der Konfiguration des Beispielszenarios verwendet. Die in den zusätzlich benötigten Kommandos verwendeten Konsolenbefehle werden nicht näher erläutert, da die Verwendung der einzelnen Tools unabhängig von der Konfiguration von Nagios zu sehen ist. Für weitere Informationen wird auf die Dokumentation der einzelnen Plugins verwiesen. Neben den Kom-mandos wird die tatsächliche Verwendung der allgemeinen Kommandos in den Servicekonfigurationen angegeben. Die restlichen Parameter werden nicht nochmals angeführt, da sie sich größtenteils mit jenen der bereits vorgestellten Einstellungen decken.

- Das für die Überprüfung der Erreichbarkeit des Port 80 verwendete Kommando:

```
define command{
    command_name            check_http
    command_line            $USER1$/check_http -H $HOSTADDRESS$
    }
```

Konkrete Verwendung dieses Kommandos in der Servicekonfiguration:

```
check_command          check_http
```

- Das für die Überprüfung des Inhalts der Website verwendete Kommando:

```
define command{
    command_name          check_http_content
    command_line          $USER1$/check_http -H $HOSTADDRESS$ -s $ARG1$
    }
```

Konkrete Verwendung dieses Kommandos in der Servicekonfiguration:

```
check_command          check_http_content!test
```

- Das für die Anzeige der aktuellen User verwendete Kommando:

```
define command{
        command_name          check_snmp
        command_line          $USER1$/check_snmp -H $HOSTADDRESS$ -o $ARG1$ -w $ARG2$ -C
$ARG3$
}
```

Konkrete Verwendung dieses Kommandos in der Servicekonfiguration:

```
check_command          check_snmp!1.3.6.1.4.1.311.1.7.3.1.7.0!2!public
```

Die bisher angeführten Kommandos finden sich in dieser oder ähnlicher Form bereits in einer Standardkonfiguration, welche bei der Installation von Nagios mitgeliefert wird. Die Auflistung soll ein Verständnis von der unterschiedlichen Komplexität der einzelnen Verwendungen geben.

Das Kommando zum Versand einer SMS wird näher behandelt. Hier wird nicht nur eine völlig neues command sondern auch die Installation und Konfiguration eines zusätzlichen Tools benötigt. Nagios verwendet zum Versenden von Nachrichten, ähnlich den Plugins zum Überwachen von Werten, externe Programme. Diese werden über einen Konsolenbefehl, welcher in der commands.cfg festgelegt wird, mit den jeweiligen Parametern aufgerufen. Zum Versand einer SMS über ein an der seriellen Schnittstelle angeschlossenes Mobiltelefon

empfiehlt sich das Programm “gnokii“. Dieses Tool kann bei einigen Distributionen über einen Paketmanager installiert werden und unterstützt viele verschiedene Typen von Mobiltelefonen. Auf die nötige Konfiguration dieser Software wird hier nicht eingegangen, da sie nicht für den Umgang mit Nagios relevant ist. Um gnokii in Nagios wie in dem bereits gezeigten Kontaktelement verwenden zu können, müssen folgende Angaben gemacht werden:

```
define command{
        command_name  notify-by-sms
        command_line     /usr/bin/gnokii $CONTACTPAGER$ "Der Inhalt der Website wurde veraendert!!"
}
```

Da Centreon bereits erwähnt wurde und in Bezug auf das Projekt dieser Diplomarbeit von Interesse ist, zeigt Abbildung 14 die Oberfläche zur Beschreibung eines Host mit diesem Programm.

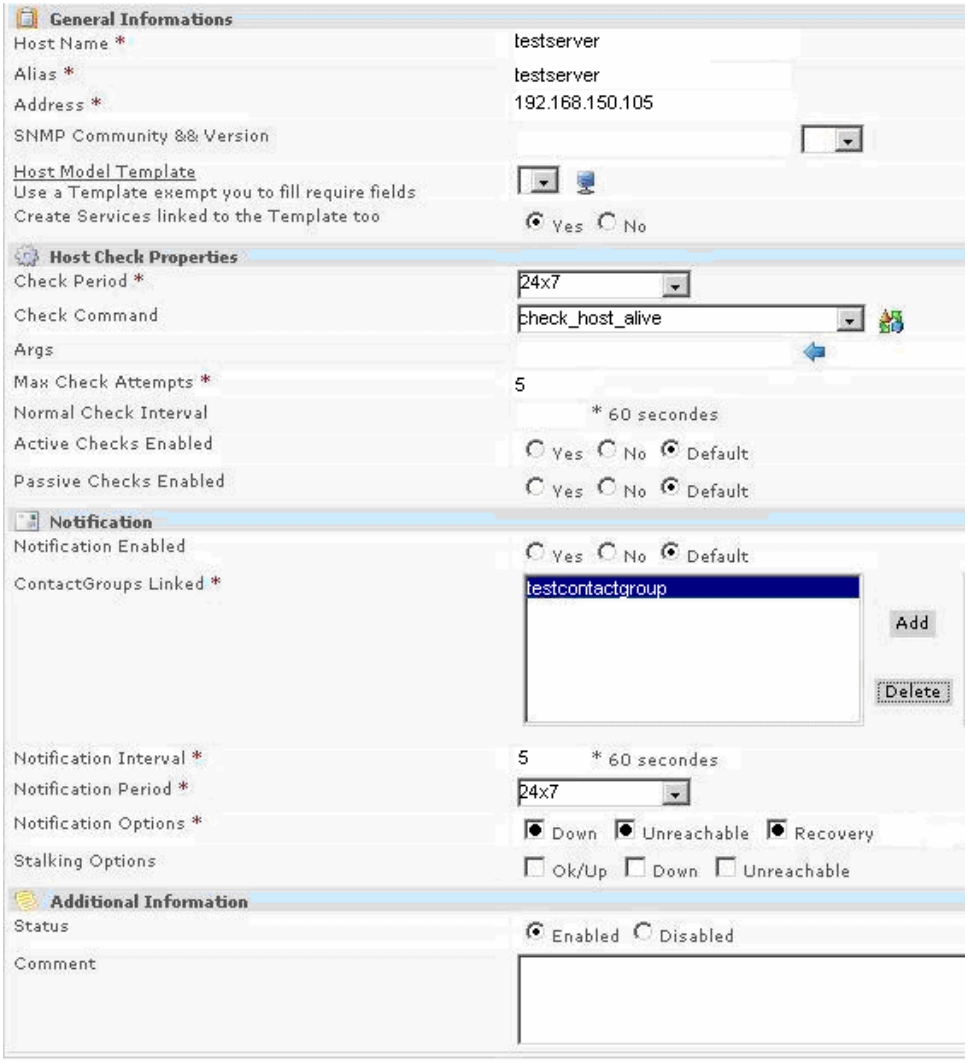


**Abbildung 14: Centreon Host-Konfiguration**

Wie man erkennen kann, vermindert sich der Aufwand der Konfiguration nicht wesentlich. Die übersichtliche Darstellung und die Kennzeichnung der verpflichtenden Angaben helfen jedoch Usern, welche in Linux unerfahren sind oder eine Abneigung gegenüber der Verwendung der Kommandozeile hegen. Man kann ebenfalls erkennen, dass es neben den vorgestellten Parametern wesentlich mehr Einstellungen gibt. Diese dienen aber keinem besseren Verständnis und werden daher nicht näher erwähnt.

## *WhatsUP Gold*

Nach der Konfiguration von Nagios werden nun die Aufgabenstellungen des Beispielszenarios in WhatsUP Gold implementiert. Im Gegensatz zu Nagios wird anfangs keine allgemeine Erklärung zur Konfiguration von WhatsUP Gold gegeben, da diese aufgrund der gut strukturierten grafischen Oberfläche sehr intuitiv ist.

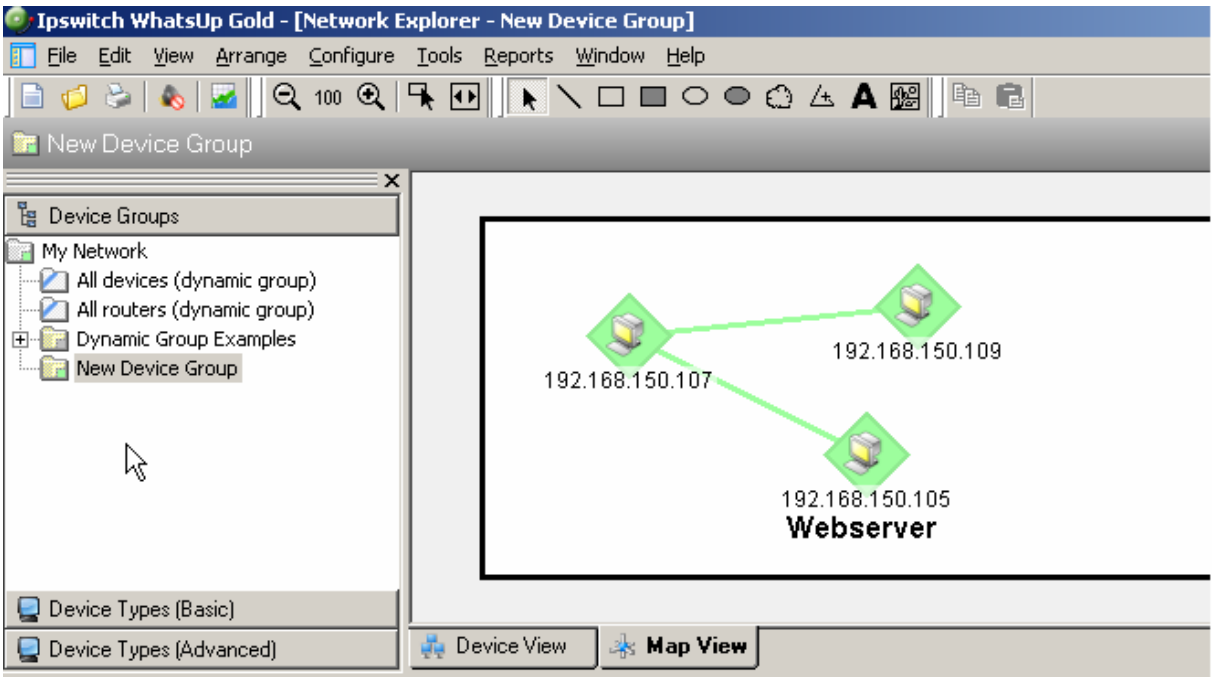


**Abbildung 15: WhatsUp Gold GUI**

Im ersten Schritt wird in diesem Tool die Netzwerkkomponente, in diesem Fall der Webserver, über “Datei -> Neues Device“ angelegt. Dazu muss nur die IP-Adresse angegeben werden. Netze können auch automatisiert nach Systemen durchsucht werden, was aber nicht zum Verständnis der grundlegenden Konfiguration beitragen würde.

Im “Eigenschaften“-Menü (Abbildung 16-1) des erstellten Objekts können nun die gewünschten Abfragen konfiguriert werden. Hier können vordefinierte Tests verwendet (Abbildung 16-

2) oder neue konfiguriert werden (Abbildung 16-3). Die neu erstellten Überwachungs-funktionen werden daraufhin in eine allgemeine Datenbank gespeichert und sind somit im gesamten Monitoring-System verfügbar.

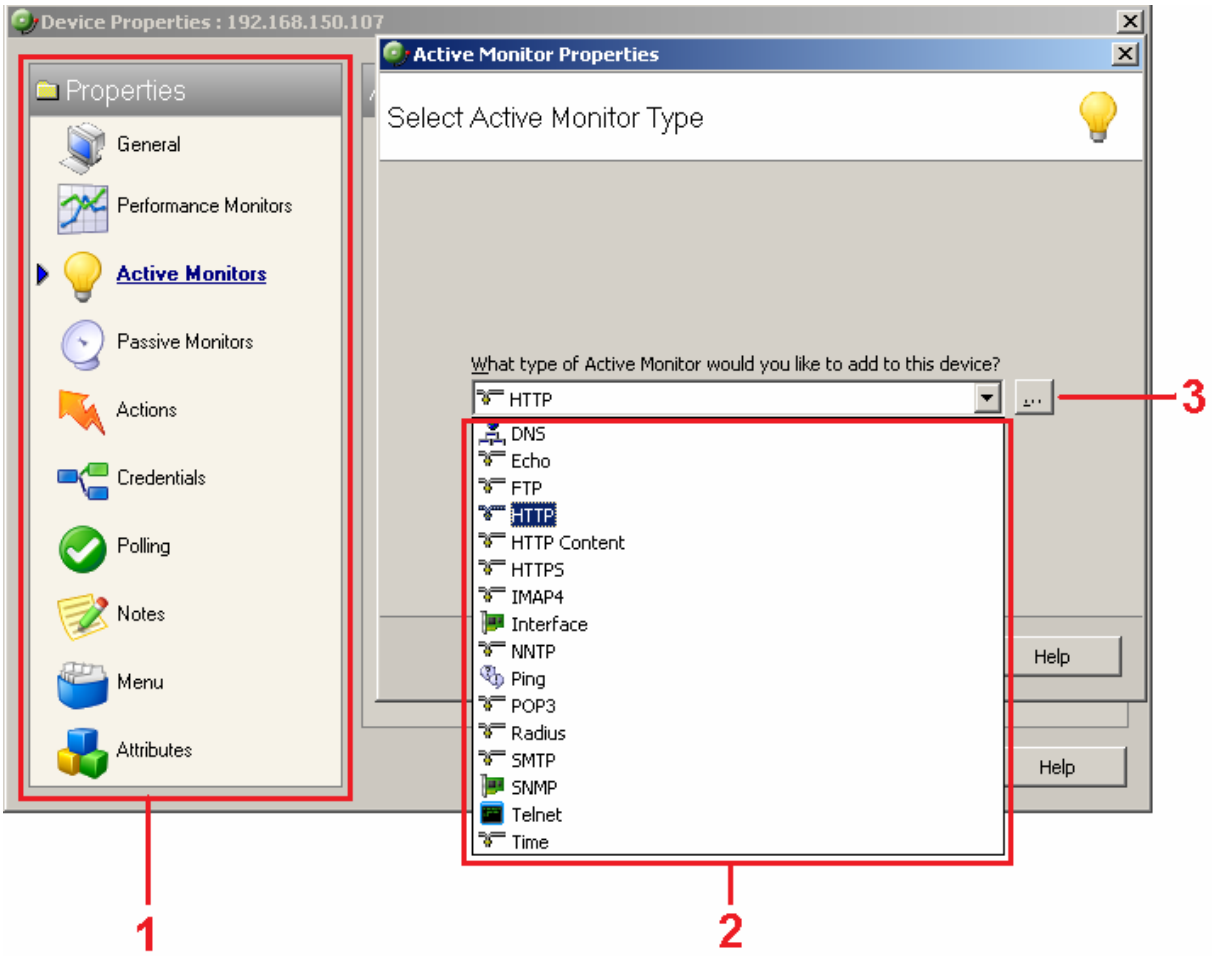


**Abbildung 16: WhatsUp Gold Host-Abfragen**

Für den geforderten Test der Erreichbarkeit von Port 80 gibt es bereits eine bestehende Funktion (Abbildung 16 – Blaue Markierung), welche verwendet werden kann. Auch für die Abfrage des Inhalts einer Website gibt es eine vordefinierte Funktion (Abbildung 17-1), diese muss aber noch an die gestellte Anforderung angepasst werden. Hierzu muss man den erwarteten Inhalt der Seite auf einen normalen http-Request angeben. In diesem Fall das Wort “Test“ (Abbildung 17-2).

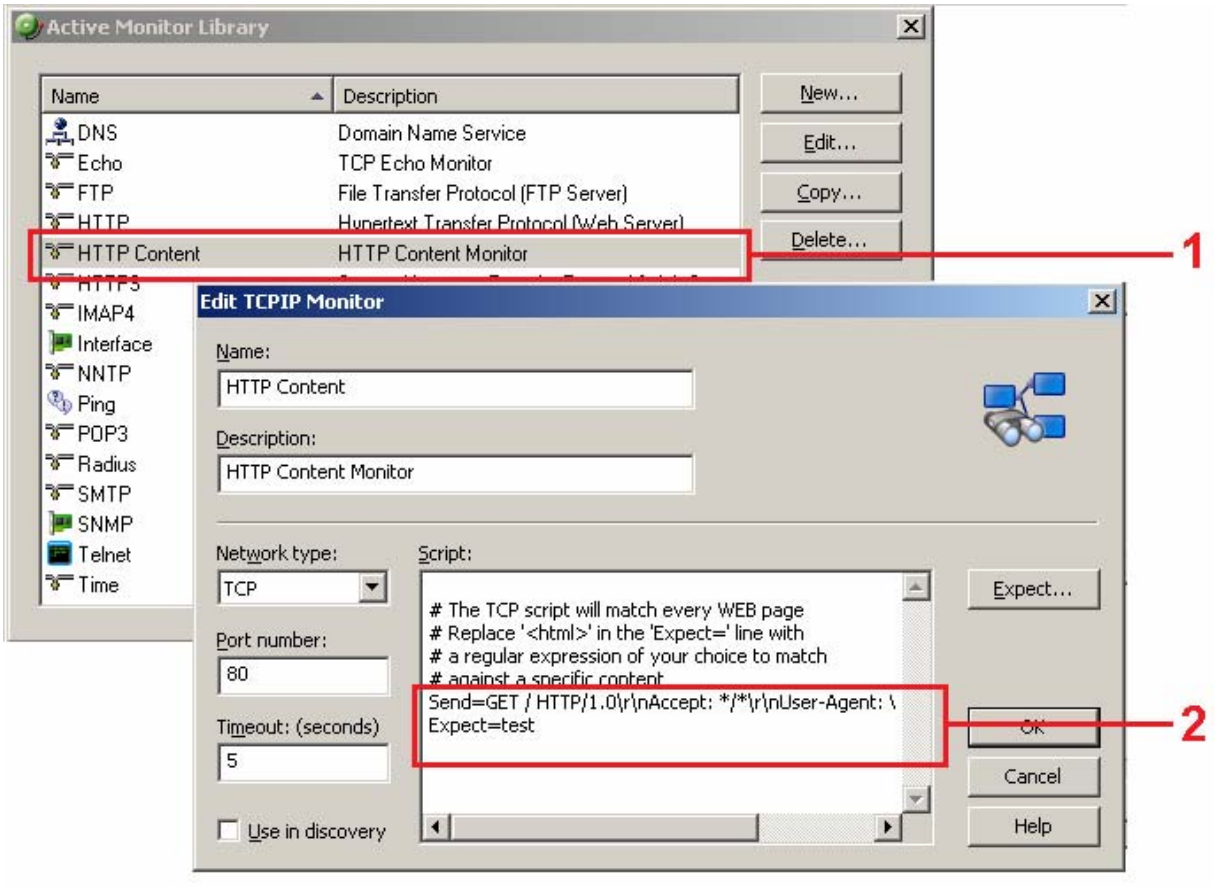


**Abbildung 17: WhatsUp Gold HTTP-Content**

Die dritte Aufgabe dieses Beispielszenarios ist die Überwachung der aktiven User des Webservers. Diese könnte, wie in Nagios gezeigt, ebenfalls in SNMP realisiert werden. Da in diesem Fall jedoch ein Windows System im Einsatz ist, wird hier das bereits vorgestellte proprietäre Protokoll WMI verwendet. Im Gegensatz zu SNMP muss so die MIB des Webservers nicht extra in WhatsUp Gold eingespielt werden. In Abbildung 18 ist das Programmfenster zur Erstellung eines WMI-Monitors gezeigt.

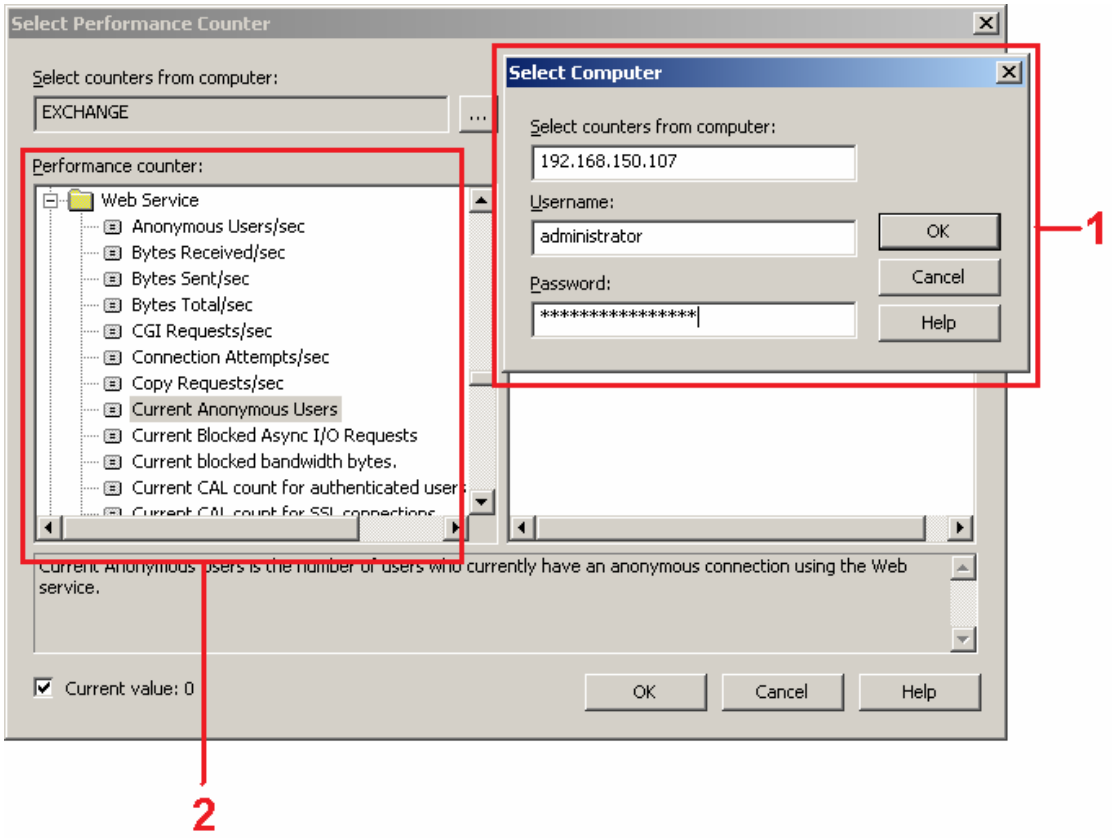


**Abbildung 18: WhatsUp Gold WMI**

Zuerst muss eine Verbindung zur Management Einheit des Systems hergestellt werden (Abbildung 18-1). Dann kann der gewünschte Wert ausgewählt werden (Abbildung 18-2).

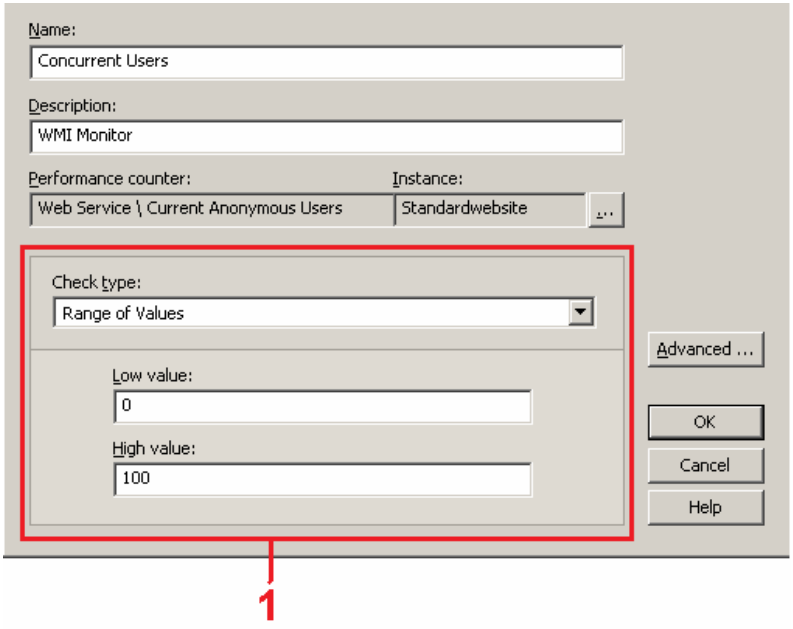


**Abbildung 19: WhatsUp Gold WMI Range**

Für den überwachten Wert können Regeln über den zu erwartenden Bereich angegeben werden (Abbildung 19-1). Wenn dieser verlassen wird, wird eine zuvor festgelegte Aktion ausgeführt. Auch für die restlichen Überwachungsfunktionen können Aktionen konfiguriert werden, welche im Fehlerfall auszuführen sind. Ähnlich den Abfragen gibt es in WhatsUp Gold bereits einige vordefinierte Aktionen. Eigene Aktionen können aber z.B. über VBScripts realisiert werden.

Im Beispielszenario soll eine SMS versendet werden, sobald der Inhalt der Webseite verändert wird. Dafür gibt es eine bestehende Funktion (Abbildung 20). Diese kann entweder eine zuvor festgelegte Nachricht per Mail an einen SMS Serverdienst im Netzwerk oder eine SMS über das Standardmodem der Systemumgebung verschicken (Abbildung 20-1).

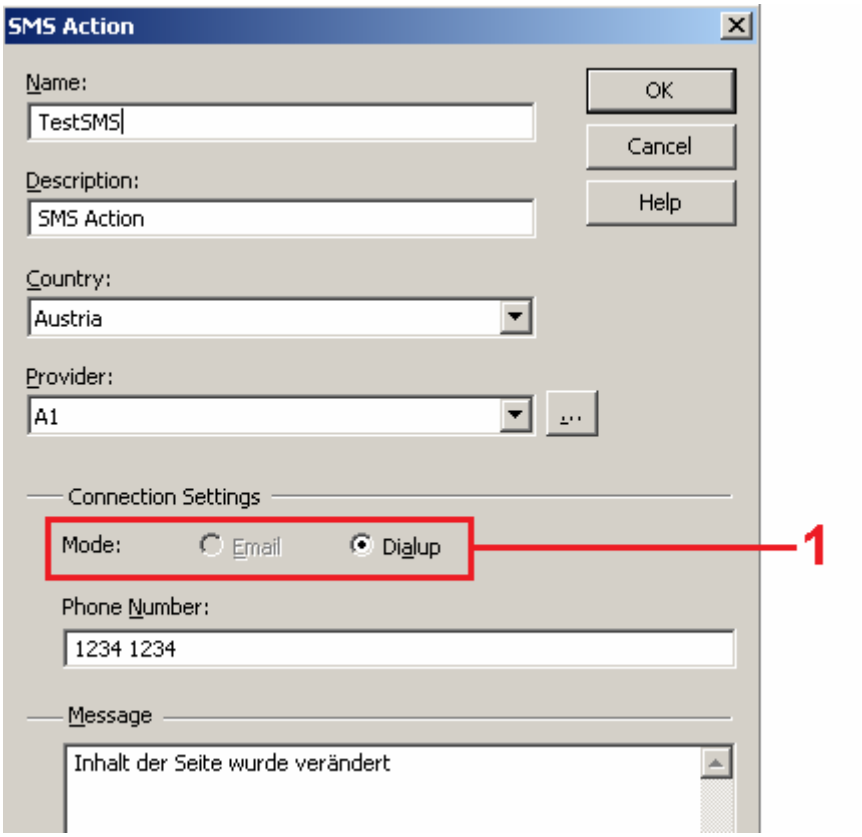


**Abbildung 20: WhatsUp Gold SMS Benachrichtigung**

Mit dem letzten Schritt wurden alle Aufgaben des Beispielszenarios erfüllt. Neben den vorgestellten Konfigurationsmöglichkeiten ist es in WhatsUp Gold natürlich genauso wie in Nagios möglich, grundsätzliche Abfrage- oder Benachrichtigungszeiten festzulegen oder das Abfrageintervall zu verändern. Da hier nur das Konzept der Konfiguration von WhatsUp Gold vorgestellt wird, wird auf diese zusätzlichen Einstellungen nicht eingegangen.

Es ist jedoch anzumerken, dass in Nagios derartige Parameter auf Ebene der Netzwerkkomponenten und der Services angegeben werden können. In WhatsUp Gold sind viele Einstellungen, wie zum Beispiel die Angabe von Wartungsfenstern, in denen keine Abfragen stattfinden sollen, nur für Netzwerkkomponenten möglich. Somit können Komponenten nur zentral außer Betrieb genommen werden.

### *Fazit*

In den vorhergehenden Kapiteln wurden die Grundkonzepte der Konfiguration beider Programme vorgestellt. Zwei vollkommen unterschiedliche Zugänge sind festzustellen. Nagios setzt auf eine sehr ausgefeilte Struktur und benötigt aus diesem Grund ein tieferes Verständnis für die Konfiguration. WhatsUp Gold hingegen versucht einen sehr einfachen Zugang herzustellen und ermöglicht auch mit Hilfe der guten graphische Unterstützung eine rasche Einarbeitung.

Es muss jedoch klargestellt werden, dass Nagios durch eine größere Vielfalt an Konfigurationsmöglichkeiten besticht. Hier werden neben den Netzwerkkomponenten die überwachten Dienste ebenfalls als eigenständige Objekte behandelt. So ist es nur in Nagios möglich, für die einzelnen Dienste einer Netzwerkkomponente unterschiedliche Konfigurationen bezüglich der Abfrage- bzw. Wartungszeiten anzugeben. Obwohl es in dem vorgestellten Beispiel nicht benötigt wurde, ist auch die Abhängigkeit zwischen einzelnen Diensten in Nagios realisierbar. In WhatsUp Gold hingegen können Abhängigkeiten nur für Hosts eingestellt werden.

Abschließend kann gesagt werden, dass Nagios mehr Konfigurationsmöglichkeiten besitzt, jedoch aufgrund der fehlenden prozeduralen Unterstützung der Konfiguration eine längere Einarbeitungszeit als WhatsUp Gold benötigt. Da die einfache Bedienung eine besonders hohe Priorität in diesem Projekt spielt, ist unter dem Gesichtspunkt der Konfiguration WhatsUp Gold zu bevorzugen.

## 3.3.5 Darstellungsmöglichkeiten

Die Darstellung der Überwachungsresultate und des aktuellen Status sind in beiden Programmen über eine Weboberfläche realisiert. Nagios bietet drei Abstraktionsebenen. Die erste gibt einen Überblick über alle Dienste und Systeme sowie ihren derzeitigen Status. In der mittleren Ebene können entweder alle Dienste oder alle Hosts mit den Ergebnissen der

zuletzt durchgeführten Tests betrachtet werden. Auf der untersten Ebene können einzelne Services oder Hosts betrachtet werden. Hier können minimale Anpassungen der Konfiguration durchgeführt werden. So kann zum Beispiel die Überwachung für eine Netzwerkkomponente gestoppt werden.

Die Oberfläche wirkt sehr aufgeräumt und präsentiert alle Informationen des zugrundeliegenden Monitoring-Systems auf eine sehr übersichtlichen Art und Weise (Abbildung 21). Ein Kritikpunkt ist hier jedoch die graphische Darstellung des Netzwerks. Diese ist funktional aber wirkt sehr primitiv. Für eine Präsentation vor dem Management einer Firma ist sie nicht geeignet.

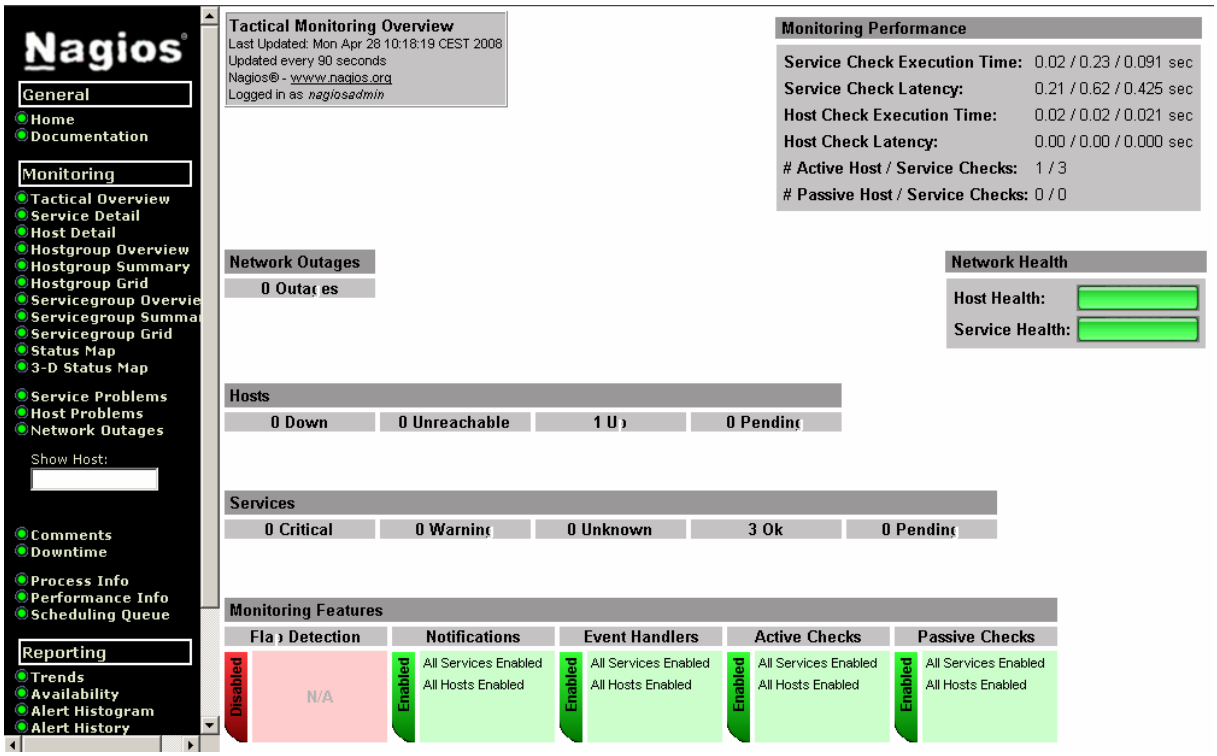


**Abbildung 21: Nagios Weboberfläche**

Das bereits mehrmals erwähnte alternative Monitoring-Programm von Nagios, namens Centreon, bietet in den Darstellungsmöglichkeiten der Überwachungsergebnisse keine Erweiterungen zu Nagios. Der Unterschied beschränkt sich auf die Verwendung von anderen Graphiken. Trotzdem erscheint die Weboberfläche von Centreon nach Meinung der Administratoren der Tageszeitung im Gesamten professioneller (Abbildung 22). Centreon umfasst darüber hinaus eine vollständige Konfigurationsumgebung für Nagios. Dadurch können auch Administratoren ohne Linux Kenntnisse mit einer vorinstallierten Nagios/Centreon-Umgebung diese Network-Monitoring-Lösung einsetzen.

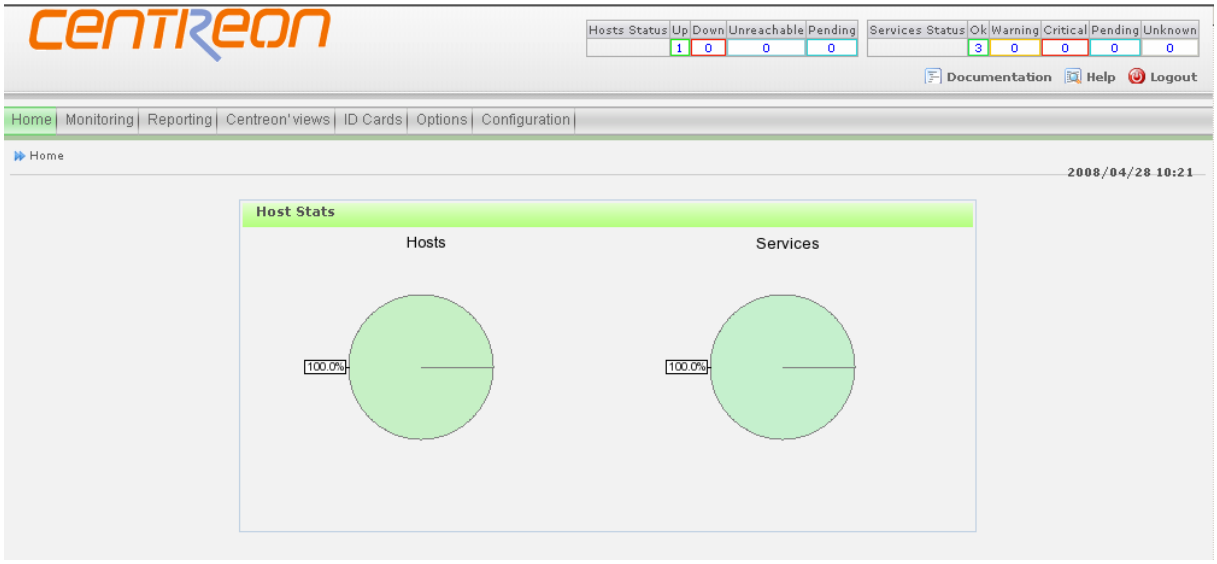


**Abbildung 22: Centreon Weboberfläche**

Im Gegensatz zu Nagios oder Centreon wirkt die Oberfläche von WhatsUp Gold, wie Abbildung 23 zeigt, im ersten Moment überladen.

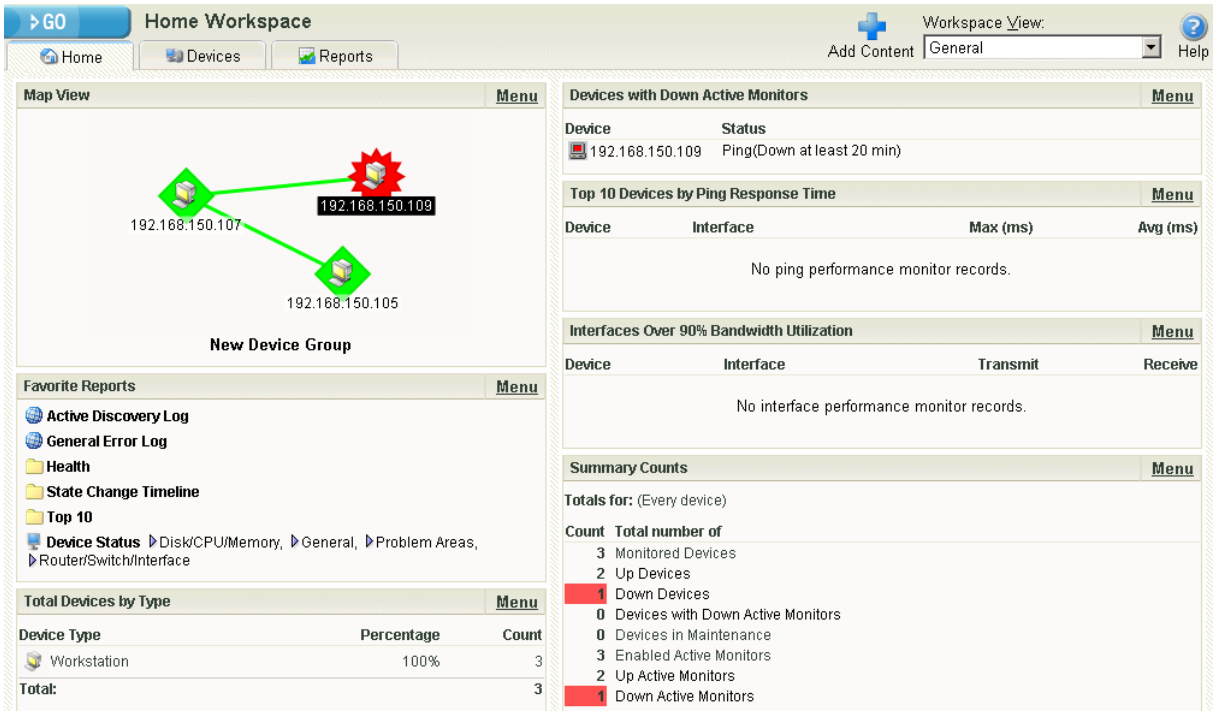


**Abbildung 23: WhatsUp Gold Weboberfläche**

Dies ist der Fall, weil im sogenannten Workspace für einen neuen Benutzer sehr viele unterschiedliche Informationen präsentiert werden. Da der Benutzer aber selbst bestimmen kann, welche Übersichten und Reports angezeigt werden sollen, kann die Anzeige auf die für den jeweiligen Benutzer interessante Informationen reduziert werden. Der modulare Aufbau ist

innovativer als das starre Darstellungskonzept von Nagios bzw. Centreon. Dadurch ist eine gute Anpassung der Anzeige an die jeweilige Zielgruppe zu erreichen. Bevor dieses Thema im nächsten Absatz näher betrachtet wird, soll noch erwähnt werden, dass in der Weboberfläche von WhatsUp Gold im Gegensatz zur Standardoberfläche von Nagios eine vollständige Konfiguration des Network-Monitoring-Tools möglich ist.

Bezüglich der Anpassung an die Zielgruppe werden in Nagios und daraus resultierend in Centreon den einzelnen Usern nur jene Komponenten oder Dienste in der Übersicht angezeigt, für die sie als “contact“ eingetragen sind. Somit ist es möglich, einzelnen Administratoren oder Usern die Übersicht auf die für sie relevanten Systeme zu beschränken. Man kann jedoch nicht unterschiedliche Darstellungsarten für unterschiedliche Benutzer festlegen oder die Konfigurationsmöglichkeiten einschränken.

In WhatsUp Gold hingegen gibt es über die Einstellungen von Nagios hinaus noch die Möglichkeit, unterschiedliche Berechtigungen für Benutzer festzulegen. So kann es einem Administrator erlaubt werden eine Netzwerkkomponente zu verwalten (Abbildung 24-1). Einem anderen Benutzer ist es aber nicht möglich, die Konfiguration zu ändern, obwohl ihm die Komponente sichtbar ist.

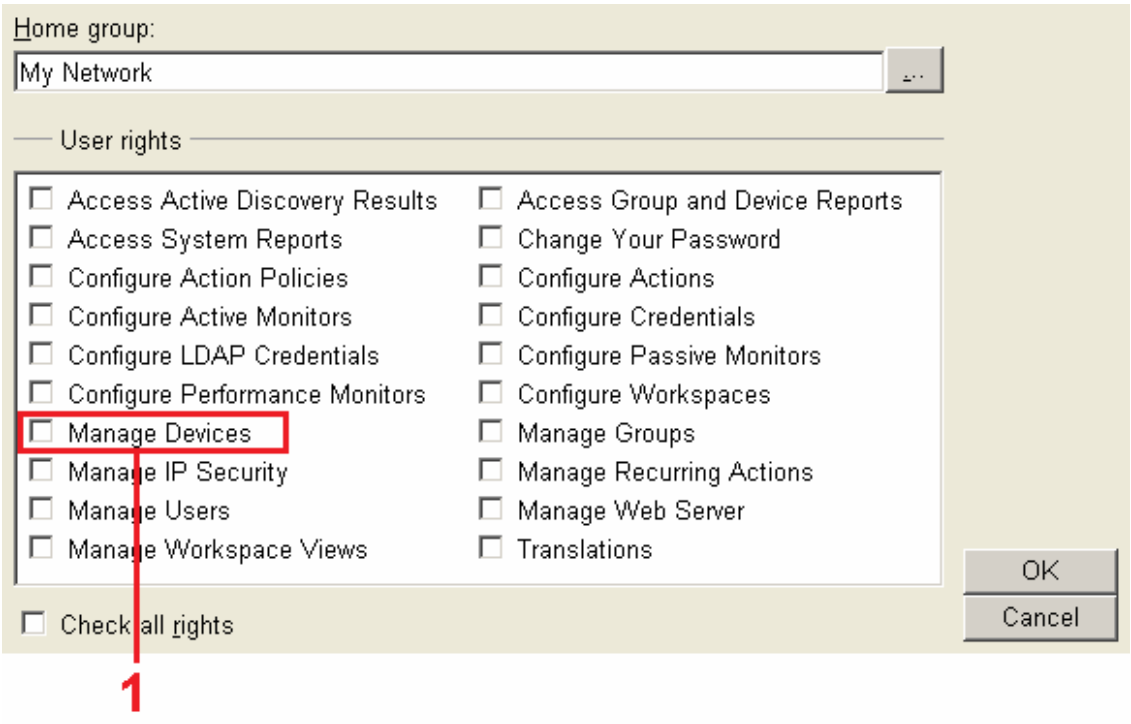


**Abbildung 24: WhatsUp Gold User Management**

Obwohl in WhatsUp Gold noch kein Rollenkonzept verwendet wird, können durch eine konsistente Vergabe der Berechtigungen Rollen für unterschiedliche Benutzer eingestellt werden. Somit kann eine sehr gute Anpassung an die jeweilige Zielgruppe erreicht werden.

*Fazit*

Die Weboberflächen beider Programme präsentieren die Ergebnisse der Überwachungen auf übersichtliche Art und Weise. Auch Reports, welche hier nicht extra behandelt werden, können den Anforderungen entsprechend generiert werden. Centreon inkludiert wie WhatsUp Gold eine Konfigurationsumgebung in der Weboberfläche. Somit sind die grundsätzlichen Funktionalitäten beider Systeme gleichwertig.

Unterschiede ergeben sich jedoch bei der Anpassung an die jeweilige Zielgruppe. Nagios/Centreon ermöglichen eine userspezifische generelle Anzeige der einzelnen Objekte. Die Darstellung bzw. die Manipulation dieser Objekte kann jedoch hinsichtlich der unterschiedlichen Benutzer nicht konfiguriert werden. Die genannten Vorteile von WhatsUp Gold ermöglichen eine bei weitem bessere Anpassung, wodurch das Produkt in diesem Punkt zu bevorzugen ist.

### 3.3.6 Abschluss der Evaluierung

In den letzten Abschnitten wurde das Vorgehen bei der praktischen Evaluierung nachvollzogen, um ein Verständnis für beide Produkte zu vermitteln. Die Ergebnisse der einzelnen Punkte führten zu der Entscheidung, dass WhatsUp Gold für dieses Projekt besser geeignet ist.

Die Begründung liegt darin, dass dieses Produkt durch eine wesentlich einfachere Bedienbarkeit hervorsticht. Die negativen Aspekte des Anschaffungspreises und etwas geringeren technischen Möglichkeiten im Vergleich zu Nagios fallen in diesem Fall weniger ins Gewicht. Diese Entscheidung basiert hauptsächlich auf der praktischen Evaluierung beider Produkte und auf der qualitativen Netzwerkanalyse.

Wie man erkennen kann, zeigt sich hier der Vorteil der in Kapitel 2 beschriebenen Vorgehensweise. Ohne die Ergebnisse des QFD-Verfahrens gäbe es keine Reihung der einzelnen Anforderungen. Die Entscheidung müsste folglich intuitiv gefällt werden. So kann die Wahl

für das jeweilige Produkt auf die Ergebnisse der Analyse gestützt werden, was zu einer höheren Entscheidungssicherheit führt.

## 3.4 Konfiguration

Nach dem Abschluss der Evaluierung und der Entscheidung für WhatsUp Gold kann nun mit der tatsächlichen Konfiguration des Network-Monitoring-Systems begonnen werden. Die Struktur und die zu überwachenden Systeme wurden bereits vorgestellt, weswegen hier nicht noch einmal auf alle Systeme im Einzelnen eingegangen wird. Besonders interessante Punkte werden in diesem Kapitel herausgegriffen. Für eine vollständige Konfigurationsanleitung wird auf das Benutzerhandbuch von WhatsUp Gold bzw. die Network-Management-Handbücher der einzelnen Systeme verwiesen.

### 3.4.1 Vorbereitende Konfiguration der Komponenten

Bevor die Konfiguration des Network-Monitoring Tools begonnen werden kann, müssen die einzelnen zu überwachenden Komponenten jeweils richtig parametrisiert werden. Die gewünschten Werte müssen ausgelesen werden können und das Monitoring-System als Nachrichtenempfänger von Informationen im Zuge von passiver Netzwerküberwachung festgelegt werden. Um dies mit Beispielen zu belegen wird nun die Aktivierung von SNMP für unterschiedliche Systeme vorgestellt.

#### *Windows*

Wie bereits erwähnt wurde, soll unter Windows grundsätzlich WMI verwendet werden. Dies wird bei der Installation von Windows mitinstalliert und ist sofort einsatzbereit. Aufgrund der Serverhardware muss jedoch zusätzlich SNMP installiert werden, da das von den Servern verwendete DMI Protokoll, welches von WhatsUp Gold nicht unterstützt wird, nur auf SNMP gemapped werden kann.

Der hierfür benötigte Dienst kann einfach über die Komponentenverwaltung von Windows installiert werden. Hier könnte auch die Funktion, dass WMI-Daten über SNMP zugänglich gemacht werden, nachträglich eingespielt werden. Diese wird im vorgestellten Fall jedoch nicht verwendet Zur abschließenden Konfiguration müssen die Eigenschaften des Dienstes

angepasst werden. Die Verbindungsparameter müssen festgelegt werden. Der Community name “nvbsnmp“ (Abbildung 25-1) wird festgelegt und das Monitoring-System als Empfänger von SNMP Traps eingestellt (Abbildung 25-2).

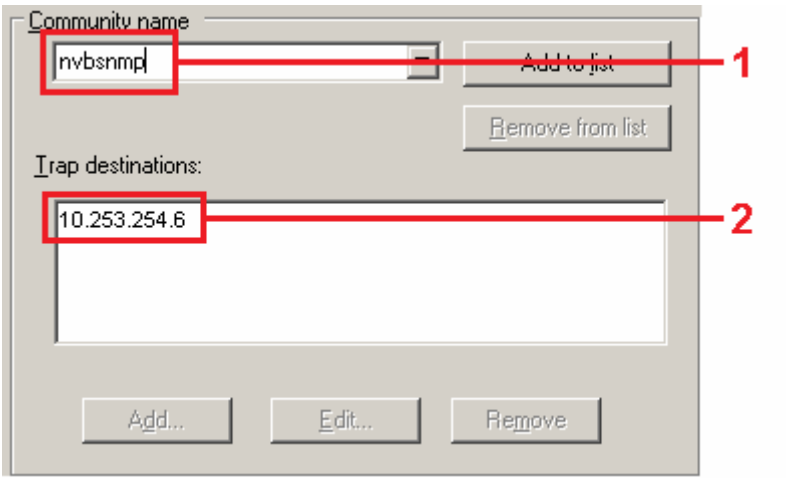


**Abbildung 25: Windows SNMP Traps**

Nach diesen Schritten kann ein Windows System in eine Network-Monitoring Umgebung eingebunden werden.

## *Linux*

Wie in Windows müssen in Linux zusätzlich Komponenten installiert werden. In diesem Fall werden die NET-SNMP Pakete verwendet, welche mittels des bereits erwähnten Paketmanagers YUM installiert wurden. Für die Einstellungen des Dienstes müssen, wie in Linux üblich, die relevanten Konfigurationsdateien adaptiert werden. In der snmpd.conf muss folgende Zeile eingefügt werden, um Traps an das Monitoring-System zu übermitteln:

*trapsink 10.253.254.6 nvbsnmp*

In Linux werden Meldungen der einzelnen Komponenten neben SNMP auch über den sogenannten Syslog Dienst verwaltet. Dieser Dienst ist dem in Windows vorhandenen Eventlog ähnlich. Hier können sämtliche Meldungen an einen zentralen Log-Server übermittelt werden. Da WhatsUp Gold als ein derartiger Syslog-Server fungieren kann, wird diese Funktion im vorgestellten Projekt verwendet. Dazu muss die Datei /etc/syslog.conf editiert werden. In dieser Datei können für die unterschiedlichen Log Meldungen Ziele angegeben werden. Diese können entweder Dateien auf dem lokalen Rechner oder eben auch

entfernte Server sein. Die nachfolgende Konfigurationszeile sendet zum Beispiel alle kritischen Meldungen an den Host “monitor“.

**.err;*.crit;*.emerg @monitor*

Der Host “monitor“ ist in der Datei /etc/hosts.conf folgendermaßen konfiguriert.

*10.253.254.6 monitor*

Zusätzlich muss nun analog zu Windows ein Tool zur Übersetzung der DMI Werte des Servers in SNMP installiert werden. Dazu müssen zuerst zusätzliche Driver über das mit der Serversoftware mitgelieferte Paket osa_ipmi eingespielt und mit dem Skript build_osadrv installiert werden. Danach wird das eigentliche Tool zur Übersetzung der Werte mit folgenden Befehlen auf den verwendeten Centos 4.4 Systemen installiert:

*rpmbuild --rebuild ibmsp6a-1.05-2.src.rpm*
*cd /usr/src/packages/RPMS/i386*
*rpm -ivh ibmsp6a--1.05-2.i368.rpm*

Damit sind nun auch die im Einsatz befindlichen Linux Systeme für das Network-Monitoring vorbereitet.

## *Server*

Neben den bereits erwähnten Installationen auf den Betriebssystemen müssen für die einzelnen Server auf BIOS Ebene weitere Einstellungen vorgenommen werden. Dies ergibt sich dadurch, dass die verwendeten Server einen eigenen System-Management-Controller besitzen, welcher unabhängig von einem Betriebssystem arbeiten kann. Dadurch ist es möglich, SNMP Traps zu versenden, ohne dass der Computer gebootet wird. Da die unterschiedlichen Hersteller sich hier in der Konfiguration sehr stark unterscheiden, wird für Einzelheiten nochmals auf die technischen Handbücher verwiesen. Im Allgemeinen müssen, wie in SNMP üblich, die Verbindungsparameter und der Empfänger festgelegt werden. Außerdem benötigt der Controller selbst einen eigenständigen Zugang zum Netzwerk, um die Daten versenden zu können. Abbildung 26 zeigt das diesbezügliche Konfigurationsmenü für IBM eServer.

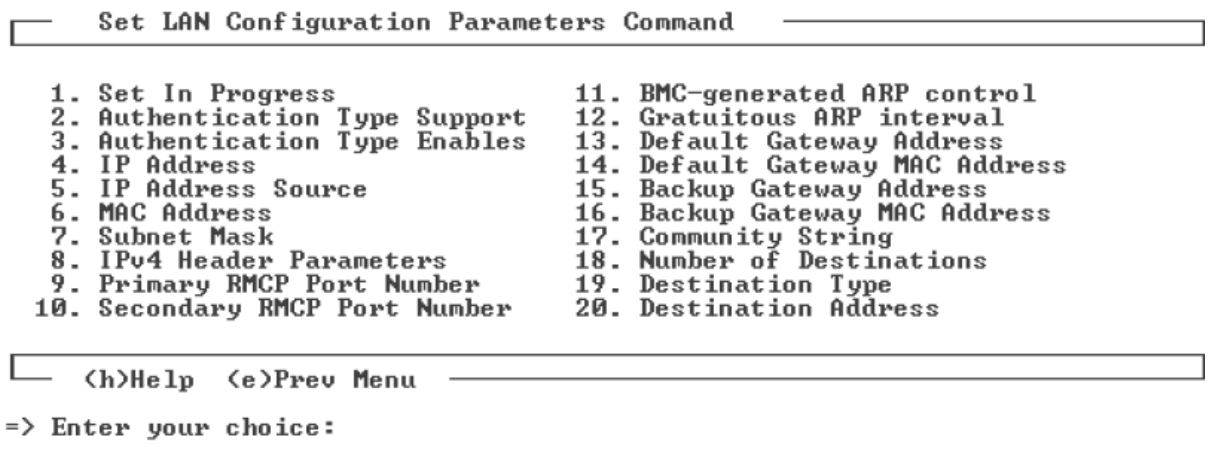


**Abbildung 26: IBM Management Controller Konfiguration (IBM, 2005:24)**

## *Switch*

Im Netzwerk der Tageszeitung werden Switches der Firma Hewlett Packard unterschiedlichen Typs verwendet. Da sich die einzelnen Typen in der Konfiguration der SNMP Funktionalität nicht sonderlich unterscheiden, wird hier nur eine Variante der Konfiguration angegeben.

*Snmp-server community nvbsnmp*

Diese Zeile setzt den für SNMP v1 benötigten Verbindungsparameter auf den Wert nvbsnmp. Somit sind Verbindungen nur mit Angabe dieses Strings möglich, was die Sicherheit etwas erhöht gegenüber dem Standardwert “public“.

Als nächstes wird mit

*snmp-server host ip-addr 10.253.254.6*

der Network-Monitoring-Server als Empfänger von SNMP Traps eingestellt. Damit ist die SNMP Basiskonfiguration des Switches für dieses Projekt bereits abgeschlossen.

## *Bladecenter*

Das im Zuge der Netzwerkanalyse bereits erwähnte Bladecenter beherbergt einige der wichtigsten Server des Netzwerks. Unter anderem befinden sich hier die Server des Checkpoint Firewall-Clusters, der Microsoft Exchange Server und die Citrix Terminalserver. Aus diesem Grund muss das Bladecenter selbst überwacht werden, da bei Problemen sämtliche Server betroffen sind.

Das Bladecenter der Firma SecureGuard kann über SNMP überwacht werden. Die Konfiguration ist sehr übersichtlich, wie man in Abbildung 27 sieht. Hervorzuheben ist hier, dass die benötigte MIB für eine einfachere Darstellung der OID im SNMP Programm direkt auf der Konfigurationsoberfläche zum Download bereitgestellt wird (Abbildung 27-1). Das ist von besonderer Bedeutung, da MIBs der Firma SecureGuard nicht so leicht gefunden werden können wie die MIBs der bisher vorgestellten Systeme von größeren Herstellern.

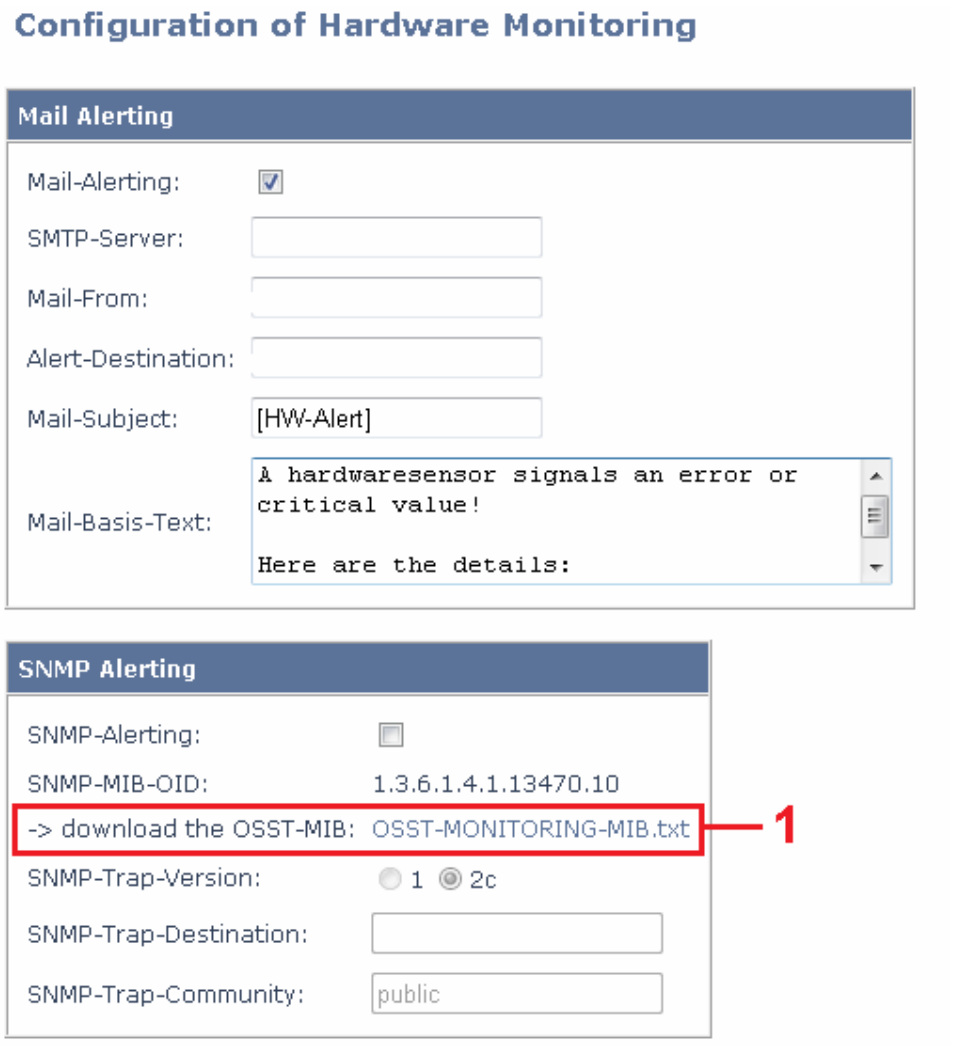


**Abbildung 27: Bladecenter SNMP Konfiguration**

Unabhängig von der Verwendung von SNMP ermöglicht das Bladecenter, wie die Abbildung zeigt, auch ein direktes Alerting via Email. Diese Funktion wird jedoch im vorliegenden Fall nicht benötigt, da sämtliche Alerts über SNMP Traps an das Monitoring Programm geschickt werden. Dieses verwaltet daraufhin die Benachrichtigung der zuständigen Personen per Mail oder SMS.

*SAN*

Das SAN im Netzwerk der Tageszeitung ist vom Typ Eurostor ES-6600 SATA RAID und verwaltet die Daten des Mailserver. In Zukunft werden hier auch die Daten eines eigenständigen Fileservers gelagert. Auch dieses System unterstützt SNMP (Abbildung 28). Die zur Interpretation der OIDs benötigten MIBs werden jedoch nicht mitgeliefert. Auch das Manual gibt keine Auskunft, welche MIBs unterstützt werden. Im Internet kann man auf firmenfremden Seiten nachlesen, dass für dieses System keine eigene MIB entwickelt wurde, sondern die Fibre Channel Maintenance Information Base verwendet wird. Dies zeigt, dass es oft umständlich sein kann, die vorhandene SNMP Funktionalität eines Systems richtig nutzen zu können. Eine erwähnenswerte Besonderheit dieses Systems ist, dass ausgewählt werden kann, welche Arten von Traps verschickt werden sollen.

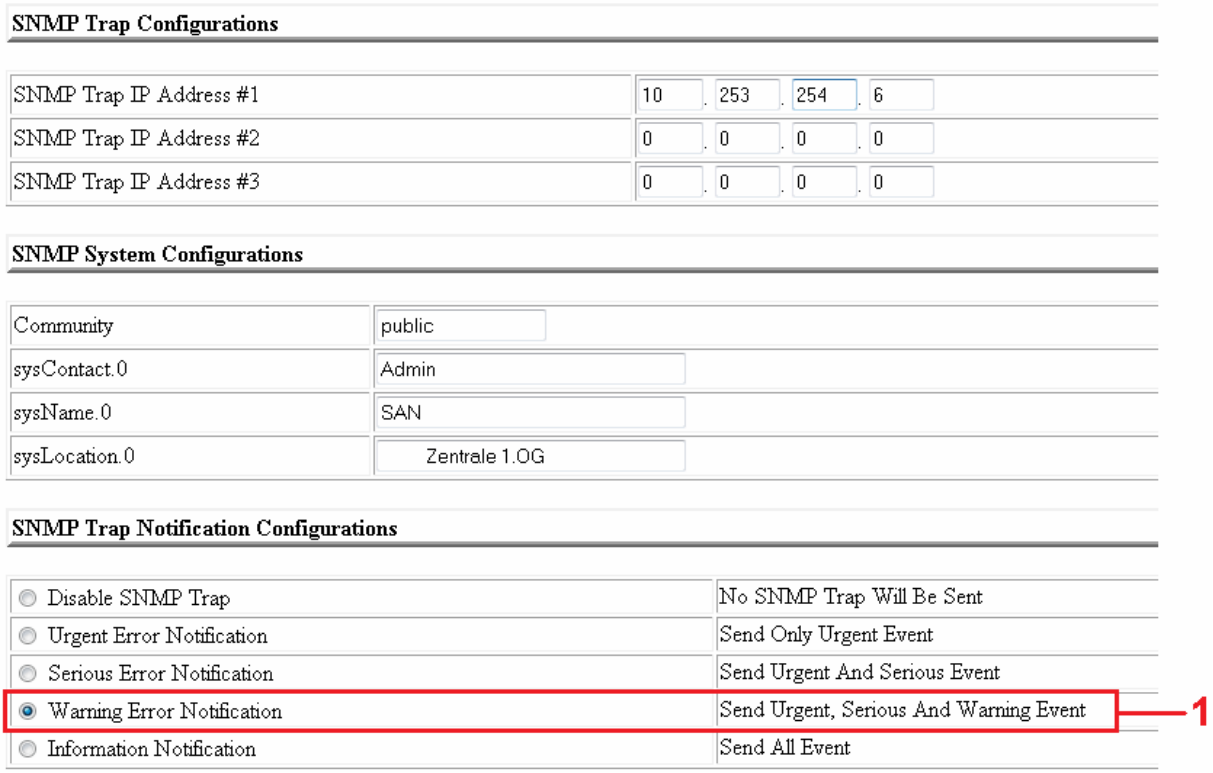


**Abbildung 28: SAN SNMP Konfiguration**

Im Rahmen dieses Projekts wurde ein ziemlich geringer Level bezüglich der Wichtigkeit eines Traps gewählt (Abbildung 28-1). Das hat zur Folge, dass sehr häufig Informationen versendet werden. Die SAN ist jedoch von enormer Bedeutung und rechtfertigt daher die erhöhte Aufmerksamkeit. Außerdem wird das Alerting durch das Monitoring Programm verwaltet,

wodurch so genannte Trap-Storms nicht zu einer Benachrichtigungswelle der Administratoren führen.

## *Firewall*

Der Cluster, welcher aus zwei Firewall-Systemen der Firma Checkpoint besteht, unterstützt SNMP. Diese Funktionalität wird jedoch nicht verwendet, da in der Literatur darauf hingewiesen wird, dass die Verwendung von SNMP auf Firewalls aufgrund von Sicherheitsüberlegungen bedenklich ist (Zwicky, 1998).

Auf der Firewall müssen jedoch Einstellungen vorgenommen werden, bevor das Network-Monitoring-System aktiviert werden kann. Die benötigten Berechtigungen müssen für das Monitoring-Programm eingestellt werden. Dabei ist in besonderem Maße darauf zu achten, dass nur unbedingt benötigte Berechtigungen vergeben werden. Abbildung 29 zeigt die konfigurierten Regeln.

| | | | | |
|---|---|---|---|---|
| 70 | Monitoring.mgmt.lpl | intern.nvb<br>intern.VoIP.NVB<br>mgmt.nvb<br>transport.lvu.nvb | UDP snmp<br>TCP http<br>TCP ftp<br>TCP smtp<br>TCP microsoft-ds<br>TCP nb_epmap<br>TCP imap<br>TCP telnet<br>ICMP echo-request | accept |
| 71 | Monitoring.mgmt.lpl | * Any | * Any | drop |
| 72 | intern.VoIP.NVB<br>transport.lvu.nvb<br>mgmt.nvb<br>intern.nvb | Monitoring.mgmt.lpl | UDP snmp-trap<br>ICMP echo-reply | accept |
| 73 | * Any | Monitoring.mgmt.lpl | * Any | drop |

**Abbildung 29: Firewallregeln**

Es werden nicht nur die Berechtigungen für die einzelnen Verbindungen, die vom Monitoring-System ausgehend bzw. ankommend erlaubt sind, angegeben. Weiters werden sämtliche andere Dienste explizit blockiert. Dies verhindert, dass andere Angaben im Regelwerk weitere Verbindungen zum Monitoring-Programm ermöglichen. Die einzelnen Regeln haben folgende Bedeutung:

| Regel | Bedeutung |
|---|---|
| | |
| Regel 70 | Angabe der Dienste, welche vom Monitoring-System in den relevanten Netzen verwendet werden können |
| Regel 71 | Verweigerung aller weiteren Verbindungen, welche vom Monitoring-System ausgehen |
| Regel 72 | Angabe der Dienste, welche von den relevanten Netzen auf das Monitoring-System zugreifen können |
| Regel 73 | Verweigerung aller weiteren Verbindungen, welche versuchen auf das Monitoring-System zuzugreifen |

**Tabelle 17: Firewallregeln**

Die Tatsache, dass die Regeln für das Monitoring-Programm erst am Ende des Regelwerks erstellt werden, hängt damit zusammen, dass die Verwaltung des Firewall-Clusters auf einem zentralen Managementserver liegt. Vor diesen Regeln befinden sich Berechtigungen für andere Firewalls, welche ebenfalls von diesem Managementserver aus verwaltet werden, aber nichts mit dem Netzwerk der Tageszeitung zu tun haben.

### 3.4.2 Konfiguration des Produkts

Nachdem die einzelnen vorbereitende Konfigurationen durchgeführt wurden. Kann die jeweilige Konfiguration von WhatsUp Gold begonnen werden. Im Zuge der Evaluierung wurden bereits viele Details diesbezüglich vorgestellt. In diesem Kapitel wird auf weitere interessante Punkte eingegangen, für eine detaillierte Beschreibung der einzelnen Konfigurationen sei wiederum auf die Dokumentation des Produkts verwiesen.

Eine besonders wichtige Einstellung ist die Aktivierung des Systems als Empfänger von SNMP-Traps und Syslog-Meldungen. Die nötigen Einstellungen für das gesamte System können über das Menü “Configure“ in den Programmoptionen getätigt werden. Dazu sind die nötigen Listener allgemein zu aktivieren. Danach müssen Listener für die konfigurierten Hosts aktiviert werden. Hier kann auch exakt eingestellt werden, welche SNMP Traps verarbeitet werden (Abbildung 30).

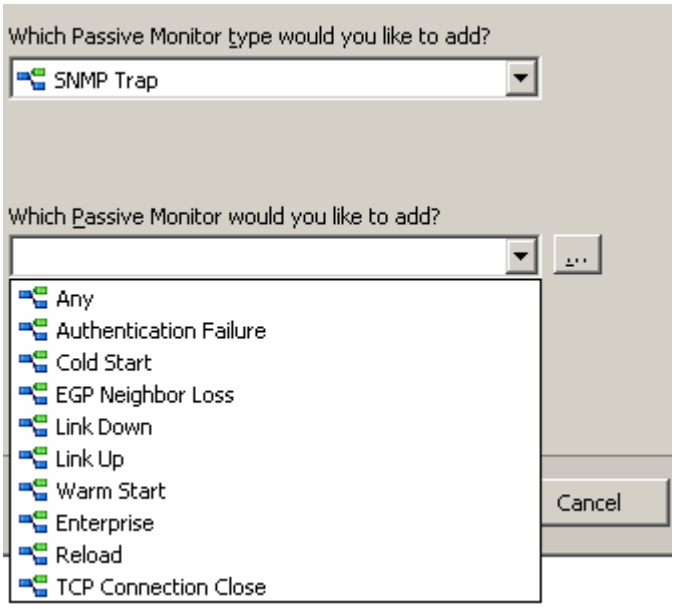


**Abbildung 30: WhatsUp Gold SNMP Traps**

Ähnlich funktioniert auch der Empfang von Syslog-Meldungen, jedoch müssen hier Matching-Regeln zur Spezifikation der zu empfangenen Meldungen angegeben werden.

Der Vorgang zur Abfrage von WMI und SNMP Werten wurde bereits in der Evaluierung behandelt. Bezüglich der Wahl der abgefragten Daten und der zulässigen Werte können kaum allgemeingültige Aussagen getroffen werden. Man erkennt dies daran, dass selbst der in der Premium Version von WhatsUp Gold vorhandene Exchange-Connector an den jeweiligen Microsoft Exchange Server angepasst werden muss. Der in Abbildung 31 abgebildet standardmäßige Monitor unterstellt eine sehr performanten Mailserver-Struktur.

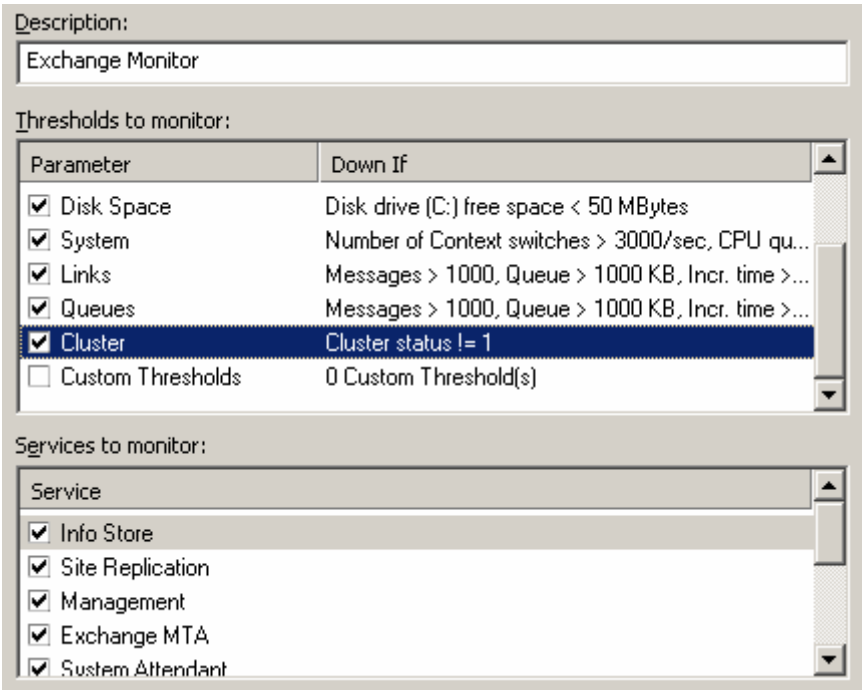


**Abbildung 31: Exchange Monitor**

Das behandelte Netzwerk verwendet nur einen Mail Server. Aus diesem Grund wurde zum Beispiel das in der Abbildung blau markierte Feld deaktiviert. Hier wird überprüft, ob mehr als ein Exchange Server im aktuellen Cluster zur Verfügung stehen. Auch die Number of Context switches wurde sehr hoch angesetzt. Im vorliegenden Fall wurde der Maximalwert von 3000 auf 500 “context switches/sec“ heruntergesetzt. Ab dieser Zahl treten im konkreten Fall bereits massive Performanceprobleme auf. So wie die gezeigten Änderungen, müssen sämtliche abgefragten Werte an die jeweilige Infrastruktur und das zu überwachende System angepasst werden. Aus diesem Grund wird hier nicht weiter auf die einzelnen Abfragen eingegangen, da diese sehr spezifischen Einstellungen nicht weiter von Interesse sind.

An dieser Stelle sei jedoch erwähnt, dass es sehr große Probleme mit der Überprüfung der externen Systeme gegeben hat. Sämtliche Systeme in externen Netzen konnten nicht gepingt werden, da die Administratoren dieser Netzwerke nur minimale Berechtigungen erteilten. Aus diesem Grund mussten neue Monitore in WhatsUp Gold erarbeitet werden, welche die angebotenen Services direkt überprüfen. Sobald ein Service nicht mehr erreichbar ist, gilt das gesamte System als nicht mehr erreichbar. Im Falle des Buchhaltungsprogramms wurde ein TCP/IP-Monitor konfiguriert, welcher an Port 23 die Zeichenkette “User Hansel“ schickt und “Geben Sie das Passwort ein“ als Antwort erwartet. Damit wird sichergestellt, dass das Programm reagiert und einsatzbereit ist. Ähnlich wurde die Überprüfung des FTP Servers der Druckerei konfiguriert. Da die APA Meldungen derzeit direkt auf einen Server im eigenen

Netz geschickt werden, wird hier der FTP Dienst des eigenen Servers überprüft. Um die Verbindung überprüfen zu können, obwohl kein Service auf Seiten der APA ansprechbar ist, wurde mit der Administration des entfernten Netzwerks vereinbart, dass das Monitoring-System den sendenden Host pingen darf.

#### 3.4.2.1 Konfiguration des Alerting

Nach diesem Überblick über die Konfiguration der Monitore in WhatsUp Gold wird nun das Alerting-Szenario vorgestellt. Grundsätzlich gibt es drei Hierarchieebenen. In der ersten Stufe werden die zuständigen Administratoren verständigt. Diese Verständigung beginnt sofort beim Auftreten eines Problems. Nach einer Stunde werden die Abteilungsleiter informiert. Bereits zwei Stunden nach Eintreten eines kritischen Fehlers wird die Geschäftsleitung informiert. Die Festlegung der kritischen Fehler wurde zusammen mit der Geschäftsleitung erstellt. Falls ein Fehler als nicht kritisch erachtet wurde erhält das obere Management auch bei längerem Bestehenbleiben des Problems keine Meldung.

Administratoren werden während der Arbeitszeit über einen Fehler jede halbe Stunde per Mail informiert. Bei kritischen Fehlern wird zusätzlich eine SMS an ein Diensthandy verschickt, welches der diensthabende Administrator bei sich tragen muss. Außerdem werden Fehler hier auch außerhalb der Arbeitszeiten gemeldet. Dazu gibt es zu jeder Zeit einen Administrator, der auf Bereitschaft ist und ein Diensthandy bei sich trägt. Die Abteilungsleiter und die Geschäftsführung erhalten die relevanten Meldungen nur per Mail. Abbildung 32 zeigt die für kritische Fehler festgelegte Action Policy in WhatsUp Gold.

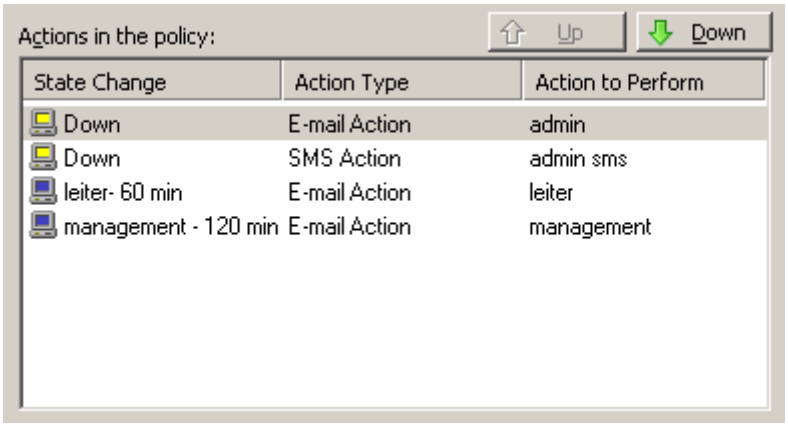


**Abbildung 32: WhatsUp Gold Action Policy**

Die schnelle Tendenz der Information der Geschäftsleitung bei kritischen Fehlern ist nötig, da die Tageszeitung aufgrund der hohen Aktualität in manchen Bereichen keine langen Ausfälle

aufweisen darf. So wurde zum Beispiel die Unterbrechung der Verbindung, welche zur Übermittlung der APA Pressemitteilung verwendet wird, als kritischer Fehler eingestuft obwohl sich dieser nicht auf das restliche Computernetzwerk auswirkt.

### 3.4.2.2 Vorstellung der Darstellungsmöglichkeiten

WhatsUp Gold zeichnet sich, wie bereits in der Evaluierung erwähnt, durch eine sehr umfangreiche Reporting Funktionalität aus. So können für die einzelnen User unterschiedliche Views auf den so genannten Workspace gezeigt werden. Abbildung 33 zeigt den Workspace der Abteilungsleiter.

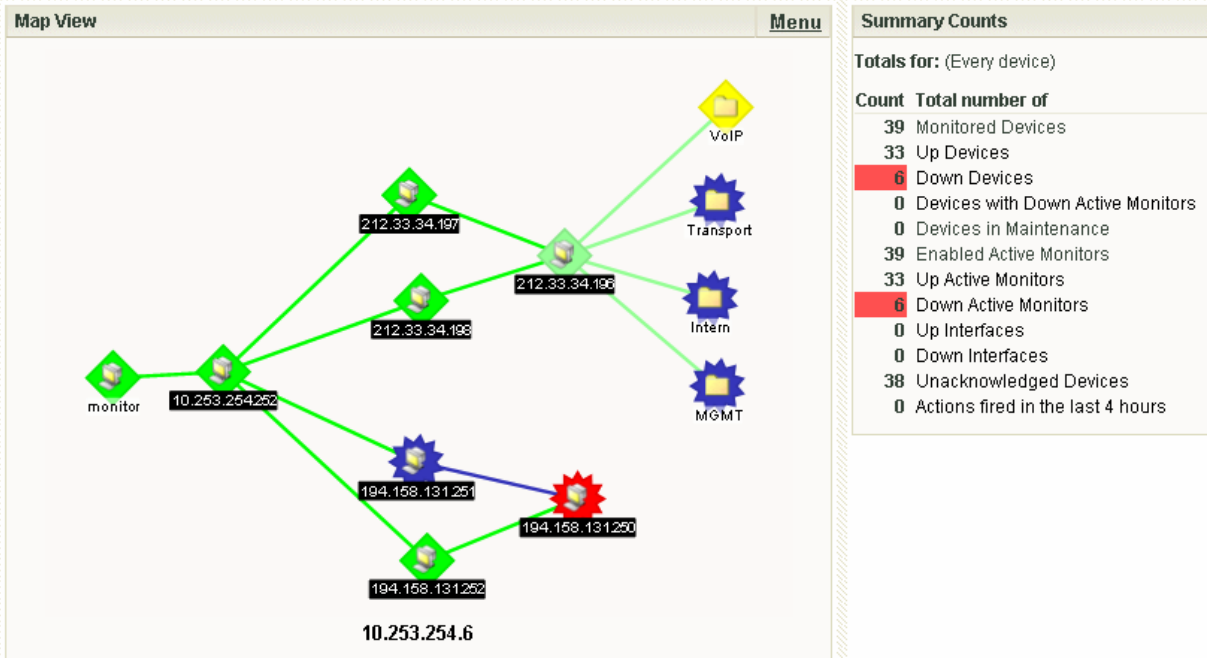


**Abbildung 33: WhatsUp Gold Workspace Abteilungsleiter**

Man erkennt, dass den Abteilungsleitern auf dieser Oberfläche wenige Übersichten zur Verfügung stehen. Diese geben jedoch einen guten Überblick über den Status des gesamten Netzwerks. Die Abbildung zeigt das Network-Monitoring-System in einer Testphase, wodurch die vielen Fehler erklärt werden.

Es ist nun möglich für einen Benutzer weitere Workspace-Views zu erstellen. So ist es dem Abteilungsleiter zum Beispiel schnell möglich einen detaillierteren Überblick zu erlangen, indem er in einen View mit mehr und vor allem genaueren Reports wechselt.

Dem Management hingegen wird nur der Map View angezeigt, da diese Übersicht einen schnellen Überblick ohne Verständnis für die technischen Details des Netzwerks ermöglicht. Hier wurden auch keine weiteren Views erstellt, da genauere Informationen für das

Management nicht von Relevanz sind. Sobald kritische Fehler länger bestehen bleiben, wird ohnehin ein Email-Alert versandt, wie dies im vorhergehenden Kapitel beschrieben wurde.

Der Workspace eines Administrators umfasst in diesem Projekt standardmäßig eine Ansicht jener Devices, deren CPU, Memory, Plattenkapazität oder ein eigener Monitor eine Auslastung von 80% übersteigt. Dies ermöglicht ein Eingreifen der Administratoren, bevor ein Problem auftritt. Außerdem werden sämtliche Devices mit Active Monitors im Zustand Down angezeigt. Zusätzlich zu diesen Reports können sich die einzelnen Administratoren ihren Workspace mit weiteren Übersichten erweitern, welche für sie von besonderem Interesse sind. Außerdem ist es ihnen möglich, eigene Views anzulegen.

Die beschriebene Reporting-Struktur ermöglicht eine sehr gute Anpassung an die jeweilige Zielgruppe und wurde von allen Mitarbeitern, welche mit dem Tool arbeiten, sehr positiv aufgenommen. Vergangenheitsbezogene Berichte, welche in WhatsUp Gold möglich sind, werden nur für Meetings oder ähnliche Anlässe erstellt.

## 3.5 Inbetriebnahme und Wartung

Mit der Fertigstellung der Konfiguration konnte die Inbetriebnahme nach dem in Kapitel 2.5.5 vorgestellten Model durchgeführt werden. Dies war möglich, da die zu überwachenden Infrastruktur auf virtuellen Maschinen modelliert wurde. So konnten die gewünschten Tests auf nicht produktiven Systemen durchgeführt werden. Dies gilt jedoch nur für Server. Netzwerkkomponenten wurden direkt in das Network-Monitoring-System übernommen, da hier keine Testsysteme zur Verfügung standen.

Um eine Überlastung der Netzwerkadministratoren durch mögliche Fehlmeldungen zu verhindern, wurden anfangs alle Meldungen des Monitoring-Systems an eine eigens dafür eingerichtete Email-Adresse geschickt. Erst im zweiten Schritt wurde die bereits besprochene Alerting-Struktur aktiviert.

Da die Tageszeitung eine sehr flache hierarchische Struktur aufweist und das Management nicht wollte, dass Benutzer außerhalb der IT-Abteilung auf das System zugreifen können, wurde keine dezidierte Berechtigungsstruktur eingeführt. Sämtliche Benutzer des Systems besitzen volle Berechtigungen. Die einzige Adaption war die Konfiguration der Oberfläche für das Management. Hier wurden sämtliche Detailreports weggelassen und nur die beiden

bereits erwähnten Gesamtreports eingeblendet. Außerdem wurden den Benutzern des Managements sämtliche Konfigurationsmöglichkeiten unterbunden.

Aufgrund der gewissenhaften Vorbereitung konnte die Inbetriebnahme ohne Probleme beendet werden. Die Nutzer des Netzwerks meldeten keine Verschlechterung der Performance und die Administratoren wurden gezielt über Probleme informiert aber nicht mit Meldungen überhäuft. Einzig das Intervall von wiederholten Email-Benachrichtigungen wurde auf 20 Minuten erhöht, da ein 5-minütiges Intervall zu kurz ist. Bei kritischen Problemen wird zusätzlich eine SMS versendet, womit dieses 20-minütige Intervall im Allgemeinen für nicht kritische Probleme ausreichend ist.

### *Ausscheiden/ Hinzufügen einer Netzwerkkomponente*

Um auch die Wartung zu systematisieren, wird die in Kapitel 2.5.5 vorgestellte Vorgehensweise für das Hinzufügen einer Netzwerkkomponente verwendet. Es ist hier jedoch anzumerken, dass es in manchen Fällen nicht möglich ist die Abfragen des Network-Monitoring-Tools auf nicht produktiven Systemen zu testen. Die Verwendung eines neuen Microsoft Exchange Servers zum Beispiel ist unmöglich ohne eine funktionierende Domäne. Im Rahmen der Inbetriebnahme wurde eine Testdomäne erstellt. Im Zuge der Wartung würde dies jedoch einen unrentablen Mehraufwand für eine einzige Komponente darstellen. Aus diesem Grund sollten hier die Abfragen des Network-Monitoring-Tools einzeln aktiviert werden, wodurch eine Fehlkonfiguration schnell lokalisiert und behoben werden kann.

Wie bereits angesprochen wurde, muss die Vorgehensweise beim Ausscheiden einer Netzwerkkomponente in jedem Projekt mit den zuständigen Entscheidungsträgern festgelegt werden. In diesem Fall wurde festgelegt, dass die Daten einer ausgeschiedenen Komponente für ein halbes Jahr abrufbar sein müssen.

WhatsUp Gold löscht sämtliche Daten, sobald eine Komponente aus dem System entfernt wird. Aus diesem Grund wurde eine Gruppe angelegt, welche sämtliche ausgeschiedenen Objekte aufnimmt. Die Abfragen für diese Komponenten sind inaktiv und sämtliche Verbindungen zu anderen Systemen sind gelöscht.

Die Namen der ausgeschiedenen Objekte werden nicht geändert, jedoch werden sie mit dem Datum des Ausscheidens versehen. Die Aufgabe der Administratoren ist es Systeme, welche länger als das geforderte halbe Jahr ausgeschieden sind, vollständig aus der Network-Monitoring Lösung zu entfernen.

Diese Vorgehensweisen ermöglichen eine Wartung ohne unerwartete Konsequenzen für das gesamte Netzwerk. Als weiteres Thema der Wartung muss hier der Support des Produkts selbst angesprochen werden. Die Unternehmensführung hat gefordert, dass neben den Kosten für das Produkt keine weitern Ausgaben anfallen dürfen. Aus diesem Grund wurde kein technischer Support zugekauft. Bei Softwareproblemen von WhatsUp Gold selbst ist somit der zuständige Administrator verantwortlich für die Lösung. Viele freie Internetforen stehen zur Verfügung, jedoch wurde entschieden, dass der Server täglich vollständig gesichert wird, um bei schwerwiegenden Problemen auf diese Sicherung zurückgreifen zu können. Man verliert dadurch maximal 24 Stunden an Abfragewerten aber erspart sich den teuren technischen Support im Rahmen eines Service-Agreements mit der Firma IpSwitch.

# 4 Rückkopplung des Network-Monitoring auf das Management

In der bisherigen Arbeit wurde Network-Monitoring hauptsächlich im Kontext der IT vorgestellt. Bereits in der Beschreibung der qualitativen Netzwerkanalyse wurde jedoch auf eine Verbindung zwischen Network-Monitoring und Management einer Unternehmung im Rahmen des QFD Verfahrens hergestellt, welche nun erweitert wird.

Im diesem Kapitel wird eine integrative Sicht des Network-Monitoring vorgestellt. Network-Monitoring wird als eines von vielen vollwertigen Instrumenten des strategischen Managements vorgestellt. Im Rahmen dieses Managementbereichs kann Network-Monitoring speziell in der sogenannten Performance-Messung eingesetzt werden. Bevor dieser Zusammenhang näher erläutert wird, muss das Konzept des strategischen Managements und der Performance-Messung vorgestellt werden.

## 4.1 Strategisches Management

Dieser Bereich der Managementlehre erweiterte die traditionellen Theorien um einen ganzheitlichen, systemorientierten Ansatz. Unternehmungen werden nicht mehr als mechanische Maschinen sondern als reziproke, organische Systeme angenommen, welche in ständiger Wechselwirkung mit unterschiedlichen Einflüssen auf die Unternehmung stehen. Eine Konsequenz ist, dass das Management nicht mehr als aneinandergereihte, einzelne Entscheidungen gesehen wird, vielmehr muss es als kontinuierlicher Prozess verstanden werden. Nicht mehr nur das Auffinden der richtigen Entscheidung ist von Interesse, darüber hinaus befasst sich das strategische Management auch mit der Umsetzung sowie dem Einfluss der getätigten Maßnahmen auf das Unternehmen und seine Umwelt. Diese Veränderungen werden im strategischen Management nicht nur auf finanzielle Kennzahlen reduziert. Im Sinne des erweiterten Systemfokus werden zum Beispiel auch Auswirkungen auf Systemprozesse, wie zum Beispiel die Reaktionszeiten eines Web-Portals, in Betracht gezogen (Welge, 2004).

Diese beschriebene Erweiterung des Managementprozesses verlangt nach neuen Formen von Kontrollsystemen. Konventionelles Controlling liefert keine ausreichenden Informationen für das strategische Management. Nicht nur die hauptsächlich finanziell ausgerichteten Kontroll-

größen sondern auch die vergangenheitsorientierte Messung sowie die Vernachlässigung von Wirkzusammenhängen sind zu eingeschränkt für ein Kontrollkonzept im Sinne des strategischen Managements. Aus diesem Grund wurde die eingangs erwähnte Performance-Messung entwickelt. Hierbei handelt es sich weniger um ein einzelnes Messinstrument sondern um ein Konzept, welches die Eigenschaften von Kontrollsystemen im strategischen Management definiert. Wie in Abbildung 34 gezeigt wird, müssen derartige Systeme neben finanziellen, quantitativen, ex-post und internen Messgrößen, wie sie im Controlling verwendet werden, auch nicht-finanzielle, qualitative, ex-ante und externe Informationen bereitstellen (Müller-Stewens, 2005).

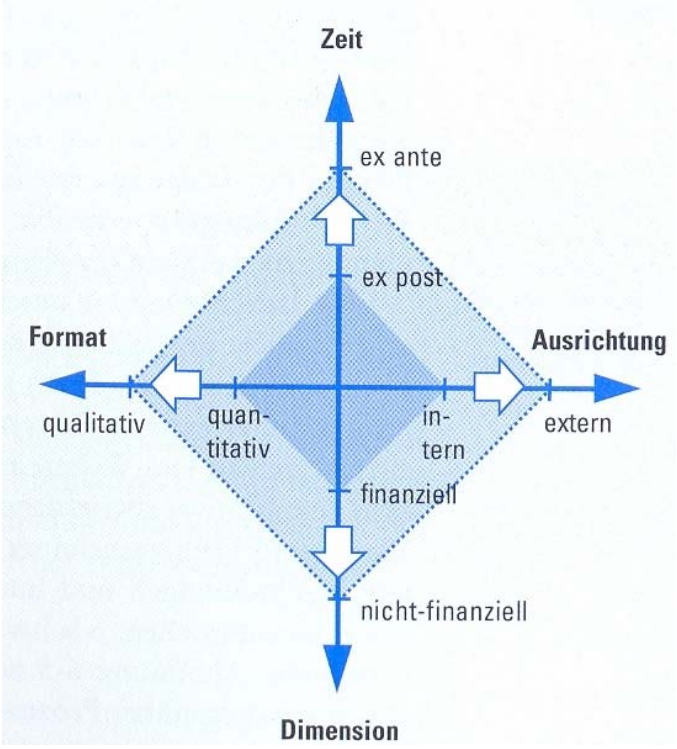


**Abbildung 34: Performance Messung (Müller-Stewens, 2005, p.638)**

Aufgrund der soeben besprochenen Erweiterung der strategischen Kontrollsysteme können Network-Monitoring-Systeme als Instrument der Performance Messung des strategischen Managements angesehen werden. Dies beschränkt sich zwar nicht nur auf IT-Unternehmen sondern auf sämtliche Unternehmen, welche sich auf Computernetzwerke verlassen, jedoch ist in IT-Unternehmen der Zusammenhang zwischen der Netzwerkinfrastruktur und der Managementstrategie besonders offensichtlich.

## 4.2 Einsatzmöglichkeiten

Nachdem die Verbindung von Network-Monitoring und Performance Messung auf einer konzeptionellen Grundlage hergeleitet wurde, werden nun Einsatzmöglichkeiten des Network-Monitoring in Bezug auf die Performance Messung vorgestellt.

Robert Kaplan, der Entwickler der Balanced Score Card (BSC), dem bedeutendsten Instrument des strategischen Management, folgt mit der Entwicklung der BSC dem Grundgedanken *"what you can't measure, you can't manage"*. Diese Aussage trifft auch auf das Computernetzwerk einer Firma zu. Solange es keine Messungen der Leistung gibt, ist es nicht möglich objektive Managemententscheidung zu treffen. Somit sind Network-Monitoring-Systeme nötig, um die IT-Infrastruktur managen zu können.

Das in dieser Arbeit vorgestellt Projekt kann hier als Beispiel dienen. Bevor eine umfassende Network-Monitoring-Lösung implementiert wurde, wurden dem Management häufig Probleme einzelner User mit der IT berichtet. Ein Resultat war eine negative Grundhaltung gegenüber der Belegschaft dieser Abteilung und der IT-Infrastruktur im Gesamten. Nachdem auf Grundlage von Daten aus der Netzwerküberwachung die objektive Leistung der IT dargestellt werden konnte, erkannte das Management, dass die einzelnen Fehler punktuelle Probleme ohne gröbere Auswirkungen auf die Gesamtperformance waren. Dadurch änderte sich die Einstellung gegenüber der IT, und die zuvor erwähnten Probleme wurden als vernachlässigbar eingestuft.

Neben dieser Objektivierbarkeit von Managemententscheidungen durch neue Messgrößen bietet die Performance-Messung implizit auch eine Möglichkeit zur Ausrichtung auf die Strategie eines Unternehmens. In der Literatur wird festgestellt, dass die Auswahl von Messgrößen das Verhalten der Mitarbeiter beeinflusst und somit als strategisches Steuerungsinstrument eingesetzt werden kann (Müller-Stewens, 2005).

Wiederum kann ein konkretes Beispiel diese These bestätigen und zeigen, dass Network-Monitoring-Systeme in diesem Sinne eingesetzt werden können. Das Management der Tageszeitung verfolgte unter anderem folgende Unternehmensmission:

*"Höchste Aktualität des Webauftritts"*

Dies sollte durch einen direkten Import der APA Pressemeldungen in das Content-Management-System der Homepage via FTP realisiert werden. Obwohl dieser Punkt dem Management derartig wichtig ist, dass er im Rahmen einer strategischen Mission festgehalten

wurde, fand keine regelmäßig Überprüfung der korrekten Funktionsweise des Imports statt. Dadurch schenkte das IT-Personal diesem Vorgang wenig Aufmerksamkeit. Probleme wurden meist erst nach einiger Zeit durch externe Besucher der Homepage erkannt und gemeldet. Im Rahmen des Network-Monitoring-Systems werden die Verbindung zum APA-Server sowie die Funktionsweise des FTP-Dienstes überprüft, da dies die festgestellten Ursachen für einen Ausfall des Imports waren. Somit werden die Administratoren unverzüglich über Probleme informiert und können diese umgehend beheben. Die strategische Mission des Managements wird folglich erst durch das Network-Monitoring-System konkret durchgesetzt.

Das soeben genannte Beispiel zeigt noch eine weitere Funktion der Performance Messung respektive des Network-Monitoring. Es dient als Kommunikations- und Übersetzungsinstrument von Vision und Strategie. Im beschriebenen Fall wird die allgemein formulierte Mission “Höchste Aktualität des Webauftritts“ in eine konkrete Anweisung, nämlich der Aufrechterhaltung des Imports der APA Meldungen, übersetzt.

Als letzter Nutzen eines Network-Monitoring-Tools im Rahmen der Performance-Messung sei hier die Möglichkeit des raschen Feedbacks für den Mitarbeiter erwähnt. Dieser kann anhand von Vorgaben und den Daten der Network-Monitoring-Umgebung erkennen, ob er die geforderte Leistung erbringt. Wenn dies nicht der Fall ist, kann er proaktiv das Management auf mögliche Fehler der Strategie hinweisen, wenn die geforderten Leistungen aufgrund von strukturellen Fehlern nicht zu erbringen sind. Somit dient das Network-Monitoring-System nicht nur dem Feedback für den Mitarbeiter, sondern auch als Basis für Reflexion der Unternehmensstrategien.

Die genannten Punkte zeigen, dass Network-Monitoring-Systeme über eine technische Verwendung hinaus auch als Instrumente der Unternehmensführung eingesetzt werden können. Aufgrund des bisher fehlenden Bezugs zum strategischen Management, wurde aber ein derartiger Ansatz kaum näher betrachet. Im vorliegenden Projekt konnte das Management aber vom dargestellten Nutzen überzeugt werden.

# 5 Zusammenfassung

Die vorliegende Arbeit hat gezeigt, dass Network-Monitoring-Systeme ein tiefes Verständnis über die zugrundeliegende Netzwerkstruktur und die verwendeten Technologien benötigen. Zuerst wurde ein Vorgehensmodell erstellt, um die Implementierung einer Netzwerküberwachung in allen Schritten zu systematisieren. Die Umsetzung des Modells im Netzwerk einer Tageszeitung im Rahmen eines Best Praxis Beispiels hat die Anwendbarkeit bestätigt. Weiters traten aufgrund der detaillierten Analyse im Vorfeld und der schrittweisen Inbetriebnahmen kaum Fehlkonfigurationen auf und das sensible Computernetzwerk der Tageszeitung konnte ohne Performance-Verlust oder ähnlichen Seiteneffekten weiterbetrieben werden. Die Responsezeiten der Administration haben sich bei kritischen Problemen um mehr als die Hälfte verkürzt und seit dem Einsatz des Monitoring-Systems konnten die Administratoren sämtliche Fehler der Netzwerkinfrastruktur vor den eigentlichen Benutzern identifizieren.

Schließlich konnte der besprochene mögliche Nutzen von Network-Monitoring-Systemen im Rahmen des Managements eines Unternehmens verifiziert werden. Die erwähnten Beispiele zeigen, dass derartige Systeme im Rahmen der Performance-Messung eingesetzt werden sollten, um dem Management eine möglichst gute Informationsbasis zu geben. Außerdem wurde die in der Literatur des strategischen Managements besprochene Lenkungsfunktion von Kontrollsystemen bestätigt und anhand eines genannten Beispiels gezeigt.

Das bisher in der Literatur oft sehr praxisorientierte Thema des Network-Monitoring wurde in dieser Arbeit auf einer allgemeinen Basis systematisiert werden. Aufgrund einer ganzheitlichen Sicht des Themenbereichs und der Einbettung in das Management konnte darüber hinaus ein Zusatznutzen bei der Verwendung derartiger Systeme für das Management gezeigt werden.

# Literaturverzeichnis

ANAGNOSTAKIS, K. G., IOANNIDIS, S., MILTCHEV, S., GREENWALD, M., SMITH, J. M. & IOANNIDIS, J. (2002) Efficient packet monitoring for network management. Poceedings ofNetwork Operations and Management Symposium 2002, 423-436, Philadelphia.

BARTH, W. (2006) Nagios: System And Network-Monitoring, Open Source Press, München.

BEJTLICH, R. (2004) The Tao of Network Security Monitoring. Beyond Intrusion Detection, Addison-Wesley Longman, Amsterdam.

BELLAVISTA, P., CORRADI, A. & STEFANELLI, C. (2002) How to Monitor and Control Resource Usage in Mobile Agent Systems. Proceedings of the 3rd International Symposium on Distributed Objects & Applications, 65–75, Rome.

BIS IT-TASK-FORCE (1989) Risks in Computer and Telecommunication Systems. Bank for international Settlements, Basel, URL: http://www.bis.org/publ/bcbsc136.pdf, Stand: 13.08.2007.

BJÖRN, M.(2004) Analyse, Entwurf und Implementierung eines System- und Applikationsmonitor für das Betriebsleitsystem (RBL) des Öffentlichen Personennahverkehrs (Ö-PNV) MOBILE. Fachhochschule Karlsruhe – Hochschule für Technik, Karlsruhe

BLUMENTHAL, U. & WIJNEN, B. (1998) RFC 2274: User-based Security Model (USM) for version 3 of the Simple Network-Management Protocol (SNMPv3).

BREITBART, Y., DRAGAN, F. & GOBJUKA, H. (2004) Effective network monitoring. Proceedings of 13th International Conference on Computer Communications and Networks, 394-399, Chicago.

BSI (2002) Einführung von Intrusion-Detection-Systemen. URL: http://www.bsi.bund.de/literat/studien/ids02/dokumente/Grundlagenv10.pdf, Stand: 28.11.2007.

CA (2008) Unicenter Learning Paths. URL: http://ca.com/files/LearningPaths/nsm_learning_path.pdf, Stand: 13.1.2008

CASE, J., MUNDY, R. & PARTAIN, Stewart, D. (2002) RFC3410: Introduction to Version 3 of the Internet-standard Network-Management Framework

CASE, J. D., FEDOR, M., SCHOFFSTALL, M. L. & DAVIN, J. (1990) RFC1157: Simple Network-Management Protocol (SNMP)

CCITT (1988) Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN. 1). Rec. X.

CHIU, M. & SUDAMA, R. (1992) Network monitoring explained: design and application, Prentice Hall PTR, Upper Saddle River

COUHEN, L.(1995) Quality Function Deployment: How to Make QFD Work for You: How to Make It Work.Addison-Wesley, Boston

DISTRIBUTED MANAGEMENT TASK FORCE (1997) Desktop Management Interface. URL: http://www.dmtf.org/standards/dmi/, Stand: 5.11.2007

DISTRIBUTED MANAGEMENT TASK FORCE (1997) DMI to SNMP Mapping Specification. URL: http://www.dmtf.org/standards/documents/DMI/DSP0002.pdf, Stand: 5.11.2007

DISTRIBUTED MANAGEMENT TASK FORCE (2007) Web Based Enterprise Management. URL: http://www.dmtf.org/standards/wbem/, Stand: 5.11.2007

DOD (2004) The Standard Waterfall Model for Systems Development. URL: http://web.archive.org/web/20050310133243/http://asd-www.larc.nasa.gov/barkstrom/public/The_Standard_Waterfall_Model_For_Systems_Development.htm, Stand: 27.11.2007

EHRINGER E. (2005) Netzwerk - Monitoring, Studiengang für Automatisierungstechnik, Fachhochschule Regensburg, Regensburg

GALSTAD E. (2007) Nagios Version 3.x Documentation. URL: http://nagios.sourceforge.net/docs/nagios-3.pdf, Stand: 7.2.2008

GNU (2007) General Public License. URL: http://www.gnu.org/copyleft/gpl.html, Stand: 13.1.2008

HALL, J. (2003) Multi-layer network monitoring and analysis. University of Cambridge, Cambridge

HERBST, U. & SCHULTHEISS, H. (2008) OpenSmart User Guide. URL: http://opensmart.sourceforge.net/docs/documentation/userguide/, Stand:13.1.2008

HEWLETT-PACKARD(2006) HP OpenView AssetCenter Portfolio module. Hewlett-Packard URL: http://www.managementsoftware.hp.com/products/ovacen/ds/4aa0-6069enw_ovacen_ds.pdf, Stand: 23.09.2007

IBM (2005) IBM eserver Xseries and BladeCenter Server Management. URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg246495.pdf, Stand 24.2.2008

IBM (2006) Tivoli IT & Asset Management, IBM, URL: http://www-306.ibm.com/software/tivoli/solutions/it-asset-management/. IBM Corporation, Stand 23.09.2007

IPSWITCH (2006) WhatsUp Professional - Performance Issues with WhatsUp Gold. URL: http://support.ipswitch.com/kb/WP-20060105-DM02.htm, Stand: 20.1.2008

IPSWITCH (2007) WhatsUp Gold v11 Overview. URL: http://www.whatsupgold.com/products/whatsup_gold_premium/index.asp?k_id=flash, Stand: 13.1.2008

IPSWITCH (2008) WhatsUp Gold v11 Price List. URL: http://www.whatsupgold.com/products/whatsup_gold_premium/buy/, Stand: 13.1.2008

ITU-T Study Group VII (1993) Information Processing Systems - Open Systems Interconnection - Systems Management. ITU-T X.700.

JAMES, D. (1990) Multiplexed buses: the endian wars continue. IEEE Micro Volume 10, 9-21, Los Alamitos

JOSEPHSEN, D. (2007) Building a Monitoring Infrastructure with Nagios, Prentice Hall PTR Upper Saddle River

KECERSKI, M(2005) Best Practice der Kostenrechnung in der IT bei Banken in der Theorie und Praxis. Universität Zürich, Zürich

KRAUSE, M. & TIPTON, H. (1999) Handbook of Information Security Management, Auerbach Publications, Philadelphia

MCCLOGHRIE, K. & ROSE, M. T. (1991) RFC 1213: Management Information Base for Network-Management of TCP/IP-based internets: MIB-II.

MICROSOFT (2007) Windows Management Instrumentation, URL: http://msdn.microsoft.com/en-us/library/aa394582.aspx, Stand: 5.11.2007

MIYAMOTO, M. (2007) Sicherheit im Internet, Ruhr-Universität Bochum, Bochum.

MÜLLER-STEWENS, G. & LECHNER, C.(2005) Strategisches Management. Grundlagen - Prozess - Implementierung. Schäffer-Poeschel, Stuttgart

NAGIOS (2007a) Nagios Plugins. URL: http://nagios.sourceforge.net/docs/3_0/plugins.html, Stand: 15.1.2008

NAGIOS (2007b) Nagios Plugin API. URL: http://nagios.sourceforge.net/docs/3_0/pluginapi.html, Stand: 15.1.2008

OREON (2007) Pre requisits - Oreon 1.3.x / 1.4.x. URL: http://www.centreon.com/Product/Pre-requisits-Oreon-1.3.x-/-1.4.x.html, Stand: 20.1.2008

PEKRUHL, U.(2000) Partizipatives Management: Konzepte und Kulturen. Hampp, Mering

RATHGEBER, I. (2004) Werbung von gestern bis heute. Institut für Wirtschaftspädagogik, Universität Koblenz-Landau, Landau

RECHENBERG, P. et al. (2002) Informatik-Handbuch. Hanser, Wien.

ROSE, M. T. & MCCLOGHRIE, K. (1990) RFC 1155: Structure and identification of management information for TCP/IP-based internets.

RUMMLER, G. & BRACHE, A. (1995), Improving Performance: How to manage the white space on the organizational chart, Jossey-Bass, San Francisco

SOANES, C. (2006) Paperback Oxford English Dictionary Oxford, Oxford University Press, Oxford.

STALLINGS, W. (1998) SNMP, SNMPV2, Snmpv3, and RMON 1 and 2, Addison-Wesley Longman, Boston

STEEDMAN, D. (1990) Abstract Syntax Notation One (ASN. 1): The Tutorial and Reference, Technology Appraisals.

TABAKOFF A. (2006) Service-Monitoring im Netzwerk der Alpine-Mayreder Bau GmbH, Studiengang für Telekommunikationstechnik und -systeme, Fachhochschule Salzburg, Salzburg

WELGE, M. & AL LAHAM A. (2004) Strategisches Management. Grundlagen - Prozess - Implementierung. Gabler, Wiesbaden

WOJTECKI JR, J. G. & PETERS, R. G. (2000) Communicating organizational change: information tachnology meets the carbon-based emploee unit. The consulting, Annual, Volume 2, 207-223, San Francisco

ZIMMERMANN, H. (1980) OSI Reference Model-The IS0 Model of Architecture for Open Systems Interconnection. IEEE Tansactions on communications, Volume 28, 425-432, Norwood

ZWICKY, E. (1998) Enough SNMP to Be Dangrous. :login:, 98.
URL: http://www.usenix.org/publications/login/1998-12/snmp.html, Stand: 5.11.2007