X.systems.press

Sicheres Netzwerkmanagement

Konzepte, Protokolle, Tools

Bearbeitet von
Thomas Schwenkler

1. Auflage 2005. Buch. xvi, 454 S. Hardcover
ISBN 978 3 540 23612 2
Format (B x L): 15,5 x 23,5 cm
Gewicht: 865 g

1

Sicheres Netzwerkmanagement: Begriffserklärungen

Seit der Entwicklung von Computern hat der Drang und der Bedarf an Vernetzung dieser Rechner stetig an Bedeutung und Gewicht zugenommen. Bei den ersten mechanischen Rechenmaschinen wurde eine Vernetzung noch dadurch erreicht, dass die errechneten Daten über externe Datenträger an andere Rechenmaschinen übergeben wurden. Der berühmte Physiker Richard Feynman erzählt recht amüsant in seinem biographischen Buch ‚Sie belieben wohl zu scherzen, Mr. Feynman' [67], wie in Amerika zur Zeit des Zweiten Weltkriegs die Forschung an der Entwicklung einer Nuklearbombe vorangetrieben wurde. Zur Lösung der mathematischen Probleme, welche den physikalischen Formeln beispielsweise zur Berechnung der freigesetzten Energie zugrunde lagen, wurden damals im militärischen Forschungszentrum in Los Alamos mechanische Rechenmaschinen eingesetzt. Für jede spezielle Aufgabe gab es eine eigene Maschine; es gab Addiermaschinen, Tabulatoren zum Bilden von längeren Summen, Multipliziermaschinen, Sortierer, Kollationiermaschinen zum Vergleichen und andere mehr. Die Maschinen arbeiteten mit Lochkarten, über welche sämtliche Ein- und Ausgaben abgewickelt wurden. Wollte man nun eine kompliziertere Berechnung mit den Rechenmaschinen anstellen, so mussten die Eingabewerte über Lochkarten in die Maschinen gegeben werden, die daraus Zwischenergebnisse berechneten, welche wiederum wiederholt als Eingabe für die nächste Maschine dienten. Auf der letzten Lochkarte nach dem letzten Rechenschritt war dann das Ergebnis ablesbar. Bei diesen Rechenmaschinen war das Netzwerk noch einfach und mechanisch über Lochkarten realisiert. Im Zuge der Weiterentwicklung wurden dann die Vernetzungen automatisiert, und die angeschlossenen Geräte konnten und mussten entsprechend für das Netzwerk konfiguriert werden. Zu Beginn lief auch dieser Prozess noch statisch. Vor Einführung des Domain Name Service (DNS), der eine dynamische Verwaltung von IP Adressen erlaubt, und des Dynamic Host Control Protocol (DHCP), durch welches Komponenten im Netzwerk dynamisch mit einer IP Adresse sowie Informationen zum DNS und grundlegenden Routing-Informationen versorgt werden können, wurden Netzwerkgeräte einmalig statisch konfiguriert und spätere Änderungen waren selten. Erst mit der steigen-

den Anzahl an Rechnern und dem stetig wachsenden Vernetzungsgrad kam die Notwendigkeit auf, Netzwerkgeräte schneller und dynamisch verwalten zu können. In diesem Zusammenhang spricht man von *Netzwerkmanagement*. Eine genauere Definition des Begriffs ‚Netzwerkmanagement' wurde 1989 von der International Organization for Standardization (ISO) im Open Systems Interconnection (OSI) Managementmodell festgelegt [96]. Die einzelnen dort festgelegten Kategorien des Netzwerkmanagements lassen sich in einer vereinfachten Klassifizierung in zwei grundlegend verschiedene Aufgabentypen zerlegen: die passive, beobachtende Aufgabe der Netzwerküberwachung und die aktive, beeinflussende Aufgabe der Netzwerkkonfiguration.

1.1 OSI Managementmodell

Im Open Systems Interconnection (OSI) Managementmodell werden primär fünf Funktionalitäten des Netzwerkmanagements unterschieden. Diese Funktionalitäten sind das Fehlermanagement, das Abrechnungsmanagement, das Konfigurationsmanagement, das Leistungsmanagement und das Sicherheitsmanagement. Weiterhin sind im OSI Managementmodell die verwalteten Objekte und Systeme näher definiert sowie die Kommunikationswege und Protokolle zwischen den Systemen. Unabhängig vom OSI Managementmodell kann noch eine Zeit-Dimension eingeführt werden, die aus den Phasen Planung, Realisierung, Betrieb und Migration besteht.

1.1.1 Funktionalität

In der Funktionalitäts-Dimension finden sich die Inhalte und Aufgaben des Netzwerkmanagements wieder. Im Vordergrund stehen selbstverständlich Erreichbarkeit und Verfügbarkeit der Systeme, aber auch die Sicherheit und die Abrechnung der vermittelten Daten.

Fehlermanagement

Das Fehlermanagement ist eng mit der Erreichbarkeit eines Systems verknüpft. Gutes Fehlermanagement bietet deshalb Mittel, um auftretende Fehler frühzeitig zu erkennen, zu isolieren und zu beheben. Zum Erkennen der Fehler eignen sich vor allem Maßnahmen wie eine Überwachung der Fehlerprotokolle oder die Entgegennahme von Fehlermeldungen. Dies schließt selbstverständlich eine geeignete Reaktion auf die erkannten Fehler ein.

Gerade im Netzwerkbereich, wo der Ausfall einer einzelnen Komponente eine große Anzahl von Fehlern und Folgefehlern erzeugen kann, stellt das Isolieren eines Fehlers ohne geeignete Hilfsmittel oftmals eine besondere Herausforderung dar. Zur Isolation der erkannten Fehler sollte daher sowohl eine Fehlerverfolgung durchgeführt werden als auch entsprechende Diagnosetests angewendet werden. Der wichtigste Schritt ist aber zweifelsohne die Behebung der erkannten und identifizierten Fehler.

Abrechnungsmanagement

Im Normalfall stellt ein Internet Service Provider (ISP) den Zugang zum Internet nicht kostenfrei zur Verfügung, sondern es fallen Gebühren für die Benutzung der Ressourcen an, welche nach den unterschiedlichen Preismodellen berechnet werden. Oftmals findet man ein volumenabhängiges Abrechnungsmodell, bei dem zusätzlich noch eine Grundgebühr für die Bereitstellung des Dienstes anfallen kann. Ein Teil der Gebühren berechnet sich demnach in Abhängigkeit vom übermittelten Datenvolumen. Nicht nur für den ISP ist deshalb die Erfassung von Abrechnungsdaten existenziell; auch die Endkunden besitzen ein berechtigtes Interesse an der Nachvollziehbarkeit und Überprüfbarkeit der erhobenen Gebühren. Abrechnungsdaten werden idealerweise am Übergang zwischen den Kunden und dem Dienstleister ermittelt, wobei dies an beiden Seiten gleichermaßen möglich ist. Das Abrechnungsmanagement beschäftigt sich mit der Verarbeitung und Verwaltung der anfallenden Abrechnungsdaten. Dazu zählt auch das Verwalten und Überwachen eventueller Kosten- und Ressourcenlimits sowie die Konfiguration der Netzwerkkomponenten bezüglich der Datenerfassung und Datenaggregation.

Konfigurationsmanagement

Die allgemeine Verwaltung der zu überwachenden Komponenten und Systeme fasst man unter dem Konfigurationsmanagement zusammen. Die darunter vereinten Funktionalitäten sind äußert vielschichtig und verfolgen gleichzeitig die unterschiedlichsten Ziele. Im OSI Managementmodell findet sich eine prägnante Beschreibung des Konfigurationsmanagements. Demnach ist es die Aufgabe des Konfigurationsmanagements, die am Management beteiligten Systeme zu identifizieren, Kontrolle über sie auszuüben, Daten von ihnen zu sammeln und ihnen Daten zur Verfügung zu stellen. Die möglichen Ziele dabei können das Vorbereiten von Verbindungen im Netzwerk sein, das Initialisieren und Starten dieser Verbindungen, das Sicherstellen einer kontinuierlichen Verbindung und das abschließende Beenden der Verbindungen. Typische Beispiele für Aufgaben des Konfigurationsmanagements sind:

- Die eindeutige Zuweisung von Namen für verwaltete Objekte und Objektgruppen.
- Konfiguration der Systeme und deren normale Betriebszustände.
- Starten, Stoppen und Konfigurieren der verwalteten Dienste und Objekte des Systems.
- Bedarfsorientierte Ermittlung von Informationen über das System und seinen aktuellen Zustand.
- Entgegennahme von Meldungen über Zustandsänderungen und außergewöhnliche Ereignisse bei den überwachten Systemen und Komponenten.
- Änderung der allgemeinen Konfiguration eines verwalteten Systems.

Leistungsmanagement

Über die Aufgaben des Fehlermanagements hinaus befasst sich das Leistungsmanagement insbesondere mit der Auslastung eines Systems. Hier zeigen sich die Unterschiede zwischen der einfachen Erreichbarkeit und der tatsächlichen Verfügbarkeit eines Systems. Typischerweise werden nicht nur aktuelle Werte bezüglich der Auslastung einer Komponente erfasst, sondern auch eine Historie über die Verfügbarkeit erstellt. So lassen sich beispielsweise Abweichungen vom Normalzustand (der „Baseline") erfassen. Außerdem ermöglicht gutes Leistungsmanagement das Vorhersagen über die zukünftige Verfügbarkeit von Systemen, so dass man frühzeitig auf die sich ändernde Nutzung der Systeme reagieren kann. Schließlich enthält das Leistungsmanagement auch Aufgaben zur Konfiguration des Systems mit dem Ziel der Verbesserung der Verfügbarkeit.

Sicherheitsmanagement

Sicherheit ist heutzutage eines der zentralen Themen in Datennetzen. Nahezu alle Geschäfts-, Verwaltungs- oder Entwicklungsprozesse hängen zumindest teilweise von der Netzwerkinfrastruktur ab. Neben einer hinreichenden Verschlüsselung stehen hier vor allem Faktoren wie Zugangskontrolle oder effektive Abschirmung von der Außenwelt zum Schutz vor Angriffen im Vordergrund. Das Sicherheitsmanagement beinhaltet vorrangig die Überwachung und das Errichten oder Abbauen dieser Sicherheitsmechanismen. Außerdem fällt die Identifizierung und das Propagieren von Sicherheitsverstößen ebenfalls in den Bereich des Sicherheitsmanagements.

1.1.2 Management Information Base

Ein wichtiger Teil der Definition des OSI Managementmodells ist die klare Definition der Management Information Base (MIB). Unter der MIB ist die Gruppe der verwalteten Objekte innerhalb eines verwalteten Systems zu verstehen. Diese Objekte unterliegen grundsätzlich den beiden Funktionen Netzwerkverwaltung und Netzwerküberwachung. Daraus ergeben sich die verschiedenen Informationsflüsse im OSI Managementmodell. Bei der Netzwerküberwachung wandern die Informationen von den Objekten der MIB zu den Managementstationen. Bei der Netzwerkverwaltung sind es die Managementstationen, welche Informationen mit dem Ziel der Administration der MIB zu den verwalteten Geräten senden. Zu diesem Zweck muss nach dem OSI Managementmodell ein entsprechendes Managementprotokoll implementiert sein, welches die verschiedenen Aufgaben erfüllen kann.

1.1.3 Zeit-Dimension

Unabhängig vom OSI Managementmodell lassen sich die verschiedenen Funktionalitäten in unterschiedliche Zeit-Dimensionen eingruppieren. Jede der drei

chronologisch hintereinander angeordneten Phasen besitzt dabei andere Anforderungen an die fünf Funktionalitäten. Zu Beginn des Netzwerkmanagements steht die Planung, gefolgt von der Realisierung oder Umsetzung der Pläne. Zum Schluss steht die Überwachung des Betriebes in der Produktivphase. Eine weitere besondere Phase findet sich noch in der Migration innerhalb eines Netzwerkes, die eine Zyklus von Betrieb zurück zur Planung zur Folge hat.

Planung

In der Planungsphase eines Netzwerks sollte idealerweise auch das Netzwerkmanagement geplant werden. Hier müssen wichtige Entscheidungen getroffen werden, die einen unmittelbaren Einfluss auf die verschiedenen Funktionalitäten des Netzwerkmanagements haben. Dies gilt im Speziellen auch für die Sicherheit des Netzwerkes und des Netzwerkmanagements. Planungsfehler lassen sich häufig nur schwer oder mit großem Aufwand wieder beseitigen. Zusätzlich entstehen weitere Risiken bei der notwendigen Migration. Aus diesem Grund ist der Planungsphase besondere Aufmerksamkeit zu widmen.

Realisierung

Nach abgeschlossener Planung müssen Netzwerk und Netzwerkmanagement im Unternehmen installiert werden. Häufig zeigen sich gerade bei der Umsetzung unberücksichtigte Detailprobleme, die es zu lösen gilt. So kann es durchaus vorkommen, das mitten in der Realisierungsphase eine neue Planungsphase notwendig wird. Die Realisierungsphase ist mit der Umsetzung aller funktionalen und nicht-funktionalen Anforderungen abgeschlossen.

Betrieb

Das installierte Netzwerk muss für einen reibungslosen Betrieb ständig überwacht, angepasst und administriert werden. Das Netzwerkmanagement ist demnach ein zentraler Bestandteil der Produktivphase. Typische Aufgaben sind die Überwachung, Fehlerbeseitigung oder auch das Durchführen präventiver Maßnahmen zur Sicherstellung des laufenden Betriebs.

Migration

Eine Migration ist nicht nur bei der Bereinigung von Planungsfehlern notwendig. Auch das Angleichen der Netzwerkkomponenten und der Netzwerkinfrastruktur an die ständig steigenden Anforderungen macht regelmäßig eine Migration sowohl der Hardware als auch der Software notwendig. Die Migrationsphase vereint alle anderen Phasen der Zeit-Dimension in sich. Während der laufende Betrieb sichergestellt werden muss, müssen die Neuerungen gründlich geplant und eventuell im Produktivbetrieb umgesetzt werden.

1.2 Netzwerkmanagement = Konfiguration + Überwachung

Die im OSI Managementmodell definierten fünf Aufgaben der Funktionalitäts-Dimension lassen sich noch weiter in zwei Kategorien unterteilen, die sich durch die Richtung ihres Informationsflusses unterscheiden. Netzwerkmanagementaufgaben, bei denen Informationen ausschließlich von den administrierten Geräten zu den Managementsystemen übertragen werden, können als Netzwerküberwachung bezeichnet werden. Fließen die Informationen jedoch von den Managementsystemen zu den überwachten Komponenten, so lässt sich diese Aufgabe als Netzwerkkonfiguration bezeichnen. Oft geht die Netzwerkkonfiguration direkt mit einer Netzwerküberwachung einher, vor allem zur Überprüfung der korrekten Umsetzung der Konfigurationsanweisungen an die Netzwerkgeräte. Unter dem Begriff Netzwerkmanagement schließlich versteht man die Kombination aus einer Netzwerküberwachung und einer Netzwerkkonfiguration. Prinzipiell sind alle fünf Funktionalitäts-Kategorien des OSI Managementmodells sowohl mit einer Netzwerküberwachung als auch mit einer Netzwerkkonfiguration verbunden. Zur Verdeutlichung lassen sich die Informationsflüsse jedoch noch weiter gewichten. Abbildung 1.1 veranschaulicht die vereinfachten Zusammenhänge zwischen Informationsfluss und den fünf Funktionalitäten des OSI Managementmodells.

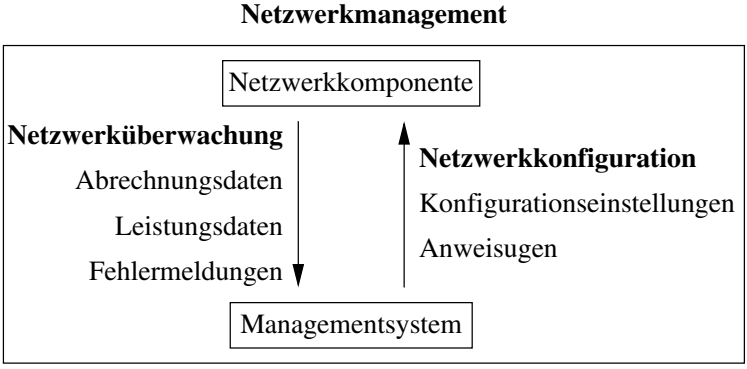

Abb. 1.1. Informationsfluss zu und von den überwachten Geräten eines Netzwerks.

Beim Netzwerkmanagement werden von einer oder mehreren Managementstationen, die von den Administratoren bedient werden, sowohl Lesezugriffe (Netzwerküberwachung) als auch Schreibzugriffe (Netzwerkkonfiguration) getätigt. Im Folgenden soll gezeigt werden, wie das Simple Network Management Protocol (SNMP) beide Aufgaben übernehmen kann. Deshalb wird sich Kapitel 4 ausführlich mit SNMP Rahmenwerk in seinen verschiedenen Versionen beschäftigen.

1.2.1 Netzwerkkonfiguration

Unter Netzwerkkonfiguration versteht man die Durchführung von Aufgaben im Netzwerk, bei denen die Einstellungen und Konfigurationen von Netzwerkkomponenten beeinflusst und verändert werden. Eine manuelle Konfiguration aller Netzwerkgeräte ist bei den heutigen komplexen Netzwerken nur noch schwer möglich. Hier kann eine vereinheitlichte Schnittstelle wie das Simple Network Management Protocol (SNMP) die Arbeit wesentlich erleichtern und vereinfachen. Zur Verdeutlichung soll an dieser Stelle das Beispiel einer typischen Netzwerkkonfigurationsaufgabe betrachtet werden. Konkret soll in diesem Beispiel die IP Adresse einer Netzwerkschnittstelle eines Cisco Routers umkonfiguriert werden. Diese Administrationsaufgabe wurde früher (und wird es heute noch sehr häufig) manuell über eine bequeme TELNET Verbindung zum Gerät durchgeführt. Abbildung 1.2 veranschaulicht die notwendigen Schritte zur Erledigung dieser Aufgabe. Die entstehenden Sicherheitsprobleme bei Verwendung des TELNET Dienstes werden später in Abschnitt 9.2.2 behandelt und sollen hier zunächst unberücksichtigt bleiben.

```
nms$ telnet 172.17.2.1
Login: root
Password: ******
Router> enable
Password: ******
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# interface fastethernet 0
Router(config-if)# ip address 10.29.11.1 255.0.0.0
Router(config-if)# exit
Router(config)# exit
Router# disable
Router> exit
nms$
```

Abb. 1.2. Administration eines Cisco Routers über eine TELNET-Verbindung.

Um diesen Prozess – vor allem bei einer deutlich größeren Anzahl an Netzwerkgeräten – zu vereinfachen und damit die Administrierbarkeit des Netzwerkes weiterhin gewährleisten zu können, wurden im Laufe der Zeit verschiedene Netzwerkmanagementprotokolle entwickelt und etabliert, von denen das Simple Network Management Protocol (SNMP) das bekannteste und verbreitetste ist. Dieselbe administrative Aufgabe der Umkonfiguration der IP Adresse einer Netzwerkschnittstelle eines Cisco Routers kann man mittels SNMP mit zwei Befehlen über die Kommandozeile erledigen. Grafische Netzwerkmanagement-Werkzeuge machen sogar die Textkonsole überflüssig, und die Konfiguration

von Netzwerkgeräten erfordert nur wenige Mausklicks. Abbildung 1.3 zeigt die zur Erledigung der Administrationsaufgabe notwendigen Befehle auf der Konsole.

```
nms$ snmpset -c private 172.17.2.1 ipAdEntAddr.4 a 10.29.11.1
ipAdEntAddr.4 : IpAddress: 10.29.11.1
nms$ snmpset -c private 172.17.2.1 ipAdEntNetMask.4 a 255.0.0.0
ipAdEntNetMask.4 : IpAddress: 255.0.0.0
nms$
```

Abb. 1.3. Administration eines Cisco Routers mittels SNMP.

1.2.2 Netzwerküberwachung

Ein zweiter wichtiger Aspekt bei der Administration von Netzwerken ist die Überwachung der Netzwerkkomponenten. Die stetig steigende Anzahl an vernetzten Systemen erlaubt es einem Administrator heute kaum noch, jedes Gerät einzeln anzusprechen und sich Informationen über seinen Status anzueignen. Außerdem hat die ständig wachsende Abhängigkeit vom einwandfreien Funktionieren der Netzwerke und der daran angeschlossenen Systeme einen großen Einfluss auf die Netzwerküberwachung. Verfügbarkeit, Auslastung und weitere Parameter der einzelnen Systeme sind heute möglichst zeitnah zu erfassen, damit entsprechende Reaktionen auf Störungen schnell und zielgerichtet durchgeführt werden können. Dazu ist nicht nur die Überwachung der einzelnen Komponenten, sondern manchmal auch des Netzwerkes als Ganzes wünschenswert. Ein hilfreiches Konstrukt zur Ermittlung von Statistiken ganzer Netzwerke ist beispielsweise das Remote Monitoring (RMON). Der deutliche Unterschied zur Netzwerkkonfiguration liegt in der Passivität der Netzwerküberwachung. Die Aufgabe der Netzwerküberwachung liegt einzig im Sammeln und gegebenenfalls Auswerten von Daten über das Netzwerk und seine Komponenten.

Wieder soll an dieser Stelle ein Beispiel den Sachverhalt verdeutlichen. Eine mögliche administrative Aufgabe aus dem Bereich der Netzwerküberwachung ist das Ermitteln der Zeitspanne seit der letzten Neuinitialisierung eines Systems („Uptime“). In diesem Fall handelt es sich um denselben Cisco Router wie in den vorhergehenden Beispielen. Abbildung 1.4 veranschaulicht die zur Erfüllung der Aufgabe mittels einer TELNET-Verbindung notwendigen Schritte. Die Ausgabe wurde für eine bessere Lesbarkeit auf die relevante Zeile mit der Angabe zur Uptime gekürzt.

Auch diese Administrationsaufgabe lässt sich mit Hilfe von SNMP deutlich einfacher erledigen. Dazu ist lediglich ein einziger Befehl in der Textkonsole notwendig. Abbildung 1.5 zeigt den notwendigen Schritt, der allerdings eine

```
nms$ telnet 172.17.2.1
Login: root
Password: ******
Router> show version
...
Router uptime is 27 days, 13 minutes
...
Router> exit
nms$
```

Abb. 1.4. Überwachung eines Cisco Routers über eine TELNET-Verbindung.

weniger gut lesbare Form der Uptime enthält. Angezeigt werden die Hundertstelsekunden seit der letzten Neuinitialisierung des Gerätes.

```
nms$ snmpget -c public 172.17.2.1 system.3
system.sysUpTime : TimeTicks: 233359456
nms$
```

Abb. 1.5. Überwachung eines Cisco Routers mittels SNMP.

1.3 Sicheres Netzwerkmanagement

Dieses Buch beschäftigt sich mit dem Thema „Sicheres Netzwerkmanagement", das nicht mit dem „Sicherheitsmanagement" des OSI Managementmodells verwechselt werden darf. In den vergangenen Jahren ist Sicherheit zu einem zentralen Gegenstand der Informations- und Kommunikationstechnologie avanciert. Sicherheit als nicht-funktionale Anforderung ist ein Querschnittsthema, das nicht nur jeden einzelnen Internet-Nutzer betrifft, sondern vor allem auch Organisationen und Unternehmen, die größere Netzwerke betreiben und zu betreuen haben. Während das Sicherheitsmanagement die Administration und Verwaltung der Sicherheitsmechanismen im Netzwerk zur Aufgabe hat, darf dabei die Sicherheit des Netzwerkmanagements selbst nicht vernachlässigt werden.

Zu Beginn der Netzwerktechnik, als die ersten Managementfunktionen direkt über das Netzwerk erledigt wurden, hat sich kaum jemand ernsthafte Gedanken über die Sicherheit des Netzwerkmanagements gemacht, wie es in der heutigen Zeit geboten wäre. Frühere Zielsetzungen lagen primär in der Funktionalität; wichtig war also vorrangig das einwandfreie Funktionieren der

Netzwerkmanagement-Lösungen. Dies spiegelt sich vor allem in der ursprünglichen Version des Simple Network Management Protocols (SNMPv1) wider. Sicherheitsfunktionalitäten sind dort nur in minimalstem Umfang berücksichtigt worden. In der Nachfolgeversion SNMPv2[1] wurde das Thema Sicherheit zwar weiter angegangen, jedoch fehlte es an der letzten Konsequenz, die Sicherheitsfunktionalitäten auch bindend umzusetzen.

Das Problem der mangelnden Sicherheitsfunktionalitäten ist kein spezifisches Problem des Netzwerkmanagements. In vielen anderen Bereichen der Informations- und Kommunikationstechnologie findet sich dasselbe Problem der Vernachlässigung von Sicherheitsmechanismen. Auch die obigen Beispiele aus Abbildung 1.2 und Abbildung 1.4 arbeiten mit dem ebenfalls unsicheren *Telnet* Protokoll (siehe Seite 271). Auch das File Transfer Protocol (FTP) [164], welches eine einfache Möglichkeit zur Datenübermittlung zwischen zwei Rechnern bietet, unterstützt nur rudimentäre Sicherheitsfunktionalitäten. Parallel dazu existierten über einen langen Zeitraum die gleichermaßen unsicheren „r-Werkzeuge“ („r-Tools“) RCP (remote copy), RDIST (remote distribution), RLOGIN (remote login) und RSH (remote shell), die nur mit primitivsten Sicherheitsfunktionen ausgestattet waren. Erst viel später wurde das sicherere SSH (secure shell) mit den Ergänzungen SCP (secure copy) und SFTP (secure file transfer program) entwickelt, bei denen die gesamte Kommunikation verschlüsselt abläuft. Trotz der freien Verfügbarkeit von SSH durch „OpenSSH“ [146] finden sich viel zu häufig noch Bereiche, in denen – oftmals aus Bequemlichkeit – TELNET Verbindungen über unsichere Kommunikationswege zu sicherheitskritischen Komponenten aufgebaut werden.

Mit SNMPv3 wurden schließlich die dringend benötigten Sicherheitsmechanismen in das bewährte Netzwerkmanagementprotokoll auch praktisch eingeführt und umgesetzt. Bis zu diesem Zeitpunkt hatten sich allerdings die beiden ersten Versionen SNMPv1 und SNMPv2 in der Praxis derart etabliert, dass die Umstellung auf die sicherere SNMPv3 Version teilweise sträflich vernachlässigt worden ist. Noch heute existieren Netzwerkgeräte, welche das SNMPv3 Protokoll unzureichend oder gar nicht unterstützen. Die Management-Werkzeuge in der Praxis arbeiten nicht zuletzt aus diesem Grund oftmals in einer der älteren SNMP Versionen, da Funktionalität aus gutem Grund noch immer eine große Rolle spielt.

In diesem Buch soll vorrangig ein tieferes Verständnis und Bewusstsein für die Sicherheitsprobleme in heutigen Netzwerken geschaffen werden, die sich zwangsweise auch auf das Netzwerkmanagement ausweiten. Dazu wird das sichere Netzwerkmanagementprotokoll SNMPv3 im Kontext mit seinen Vorgängerversionen erläutert sowie dessen Vorteile hervorgehoben und näher beschrieben. Einen weiteren Schwerpunkt bilden die verschiedenen Bedrohungsformen und Angriffsformen aus dem Internet, die gleichermaßen für Netzwerke wie auch für das Netzwerkmanagement bestehen. Dabei soll ver-

[1] Abschnitt 4.5 beschäftigt sich mit den verschiedenen SNMP Versionen und deren Namensgebung.

deutlicht werden, dass gerade die Netzwerkmanagementinfrastruktur besonders schützenswert ist. Ziel soll es schließlich sein, dass die verfügbaren Sicherheitsmechanismen des Netzwerkmanagements entsprechend den heutigen Bedürfnissen angepasst und vor allem auch eingesetzt werden. Nur so kann in letzter Konsequenz von einem „Sicheren Netzwerkmanagement“ gesprochen werden.