

6. Zusammenfassung

Mit dem ATM-Backbone-Netz wird der Universität Rostock eine leistungsfähige Grundlage für heutige und zukünftige Kommunikationsanforderungen zur Verfügung gestellt.

In Kapitel 2 wurde ein Überblick über den Stand und die Entwicklung der Normierungen bezüglich ATM gegeben. Dabei wurde festgestellt, daß, obwohl die Normierungs-Entwicklung noch nicht abgeschlossen ist, die für die Belange eines ATM-Backbone-Netzes nötigen Standards verabschiedet und in der Netztechnik der Universität Rostock implementiert sind. Hierzu zählen IP over ATM, UNI 3.1 und 4.0, IISP, PNNI 1.0 (teilweise), TM 4.0 (teilweise) und LANE 1.0.

Die weitere Normierungsentwicklung wird noch im laufenden Jahr Standards wie PNNI 2.0, LANE 2.0 und MPOA spezifizieren, die eine Erweiterung der Verfügbarkeit ermöglichen, mit dem Schwerpunkt der Unterstützung von Dienstgütemerkmalen (QoS). Dies wird ATM zu einer zunehmenden Akzeptanz verhelfen - zur Erweiterung der ATM-Technik bis in den Endbereich und gleichzeitigen Ablösung der bisherigen heterogenen LAN-Strukturen.

Seitens der Universität ist daher auf ein kontinuierliches Upgrade der Netztechnik zu achten.

In Kapitel 3 wurde das ATM-Backbone-Netz der Universität Rostock beschrieben. Der aktive Teil des Backbones mit den ATM- und LAN-Switches, Routern, dem Netzwerkmanagement und der notwendigen Service-Technik wird zur Zeit universitätsweit aufgebaut. An der Planung und Realsierung dieser Elemente ist der Verfasser maßgeblich beteiligt.

Zur Begründung der Produktauswahl wurden umfangreiche Vergleiche mit den Produkten weiterer führender Hersteller angestellt, nach Kriterien wie: Leistungsfähigkeit, Kompatibilität, Erweiterbarkeit, Verwaltbarkeit, Unterstützung von Standards etc.. In diesem Rahmen wurde an Tests des EANTC an der TU Berlin teilgenommen, und deren Ergebnisse in den Produktvergleich einbezogen.

Zur vorhandenen Meß- und Analysetechnik wurden die unterschiedlichen Funktionalitäten der Tools sowie deren Eignung dargestellt. Es wurden Aussagen zu Einsatzmöglichkeiten getroffen und Möglichkeiten der gegenseitigen Ergänzung aufgezeigt. Hinzu kommen Anwendungsbeispiele anhand von Meßszenarien innerhalb des ATM-Backbone-Netzes der Uni Rostock.

Bei den Erörterungen zur Erweiterung und Optimierung des ATM-Netzes wurde dargestellt, welche Möglichkeiten die eingesetzte Netztechnik zur Erhöhung der Ausfallsicherheit bietet, sowohl hardware- als auch softwarebasiert. Diese umfassen Anbindungen der LAN-Switches über Fast Ethernet (Spanning Tree) oder ATM (mittels Dual PHY ATM Interface-Module) und Verknüpfungen der ATM-Switches über ATM (PNNI). Als Hemmnis stellt sich dabei die momentane Sternstruktur des Netzes heraus. Lösungsmöglichkeiten wurden in ATM-Richtfunk-Verbindungen zwischen den

Standorten gefunden und mit Beispielen belegt. Abschließend wurden Redundanzmöglichkeiten von LANE Services sowie Routing-Funktionen dargestellt.

Der zweite Teil der Arbeit befaßt sich mit Sicherheitsmechanismen: allgemein sowie auf das Universitäts-Netz bezogen. Auf dem Gebiet der Netzsicherheit ist ein erheblicher Nachholbedarf zu verzeichnen. Dabei kamen gerade in den letzten Monaten eine Reihe neuer Systeme hinzu, über praktische Erfahrungen auf diesem Gebiet ist bislang kaum etwas veröffentlicht worden. Die vorliegende Arbeit nimmt daher hierauf besonderen Bezug.

Kapitel 4 umfaßt eine ausführliche Darstellung des Stands der Technik bezüglich der IT-Sicherheit.

Es wurde eine allgemeine Bedrohungsanalyse dargestellt und anhand dieser die Notwendigkeit des Einsatzes von Sicherheitsmechanismen nachgewiesen. Es wurden die durch internationale Gremien festgelegten Richtlinien zur Beurteilung der Sicherheit dargelegt.

Die Verfahren zur Encryption wurden beschrieben und anhand von Kriterien wie Grad der Sicherheit, technischer Aufwand, benötigte Rechenleistung und Durchsatz verglichen. Es wurden Angriffsmöglichkeiten gegen Encryption-Systeme aufgezeigt. Die Einsatzmöglichkeiten der Verfahren wurden anhand ausgewählter Beispiele und Produktintegrationen erläutert. Dabei wurde festgestellt, daß es noch Hemmnisse bezüglich des Einsatzes und der Ausfuhr von sicheren kryptographischen Verfahren gibt, z.B. bei Triple-DES.

Bei der Beschreibung der Möglichkeiten der Zugangskontrolle zu Netzen wurden Möglichkeiten der Authentifikation unter Berücksichtigung des Sicherheitsgrades aufgezeigt. Es wurden hierfür entwickelte Protokolle beschrieben und deren Einsatz anhand ausgewählter Beispiele belegt. Es wurde eingeschätzt, daß der Einsatz von permanenten Paßwörtern noch sehr verbreitet ist, sich dadurch jedoch erhebliche Sicherheitsrisiken ergeben.

Im nächsten Abschnitt wurden Firewalls definiert und nach verschiedenen Kategorien unterschieden. Eine Bewertung erfolgte hinsichtlich Funktionalität, Performance, Verwaltbarkeit und Sicherheitsgrad. Es wurden Architekturen unter Einbeziehung unterschiedlicher Firewall-Kategorien beschrieben und bewertet. Für den Einsatz von Firewalls wurden die Empfehlungen des BSI dargelegt, hierbei konnte der Verfasser auf die Unterstützung des BSI in Bonn zurückgreifen.

Beispiele für Implementierungen von Firewalls wurden anhand ausgewählter Produkte beschrieben und hinsichtlich verschiedener Kriterien verglichen. Besonderer Wert wurde auf die Kriterien Sicherheit und Administrierbarkeit gelegt. Dies erfolgte in Auswertung der Ergebnisse aus der Zusammenarbeit mit System-Ingenieuren sowie dem DFN-CERT in Hamburg. Es wurde festgestellt, daß gerade in den letzten Monaten größere Fortschritte in Richtung Funktionalität und Bedienbarkeit gemacht wurden. Die Hersteller werden sich in Zukunft in verstärktem Maße der Implementierung weiterer Funktionen widmen, die Firewalls bislang nicht oder nur unter starken Performance-Einbußen boten, wie beispielsweise Viren-Scanner.

Ein weiterer Abschnitt verfolgt die Entwicklung von Sicherheitssystemen auf ATM-Ebene. Hier ist mit einer Normierung seitens des ATM Forums in frühestens einem halben Jahr zu rechnen. Alle bisherigen „ATM-Firewall“-Lösungen bewirken eine logische Trennung von ATM-basierten geswitchten Netzen und sind daher nicht für den Backbone der Universität Rostock geeignet.

Die abschließende Darlegung von realisierten Sicherheitskonzepten zeigte, daß es noch einer zunehmenden Einsicht in die Notwendigkeit einer sicheren Infrastruktur bedarf. Es steht die einmütige Aussage, daß jeder für seine eigene Sicherheit selbst verantwortlich ist.

In Kapitel 5 wurde Bezug auf die Sicherheitsmechanismen im Netz der Universität Rostock genommen. Die Analyse und daraus abgeleitete Empfehlungen erfolgten getrennt für die drei Teilnetze des RUN, da die Anforderungen der Nutzer in Hochschule, Verwaltung und Medizin bezüglich Sicherheit und Performance unterschiedlich sind.

Es wurden die bereichsspezifischen Funktionalitäten untersucht und deren aktueller Realisierungsstand unter besonderer Berücksichtigung der Sicherheitsanforderungen analysiert. Die Zusammenarbeit mit dem auf Hochschulsicherheit spezialisierten CERT des DFN trug wesentlich dazu bei, die spezifischen Sicherheitsaspekte deutscher Universitäten zu ergründen.

Bei den Sicherheitsempfehlungen wurden verschiedene Sicherheitssysteme an den Forderungen gemessen und an unterschiedlichen Orten im Netz plaziert. Dabei wurden Auswirkungen auf Sicherheit, Performance, Verfügbarkeit, Verwaltung, Investkosten etc. analysiert, in Bezug auf die Sicherheitstechnik und die Netztechnik, und in deren Auswertung Lösungen favorisiert.

Den Abschluß bilden allgemeingültige Empfehlungen.

Im Rahmen dieser Arbeit wurden Empfehlungen zur Erhöhung der Sicherheit innerhalb des Universitäts-Netzes gegeben. Bevor konkrete Schutzmaßnahmen ergriffen werden, müssen im Rahmen einer Sicherheits-Politik Definitionen getroffen werden, welchen Erfordernissen und Beschränkungen die Nutzung des Netzes konkret genügen soll. Hinsichtlich der Benutzergruppen ist genau zu klären, welcher Nutzer welcher Gruppe bzw. Sicherheitskategorie zuzuordnen ist. Hohen Stellenwert hat die Einbeziehung organisatorischer Aspekte in die Sicherheits-Politik. Wenn dies vorliegt, können konkrete Empfehlungen gegeben werden.

Abschließend sei bemerkt, daß die aufwendigsten Maßnahmen keine 100%-ige Sicherheit schaffen können. Zudem werden die wachsenden technischen Anforderungen und steigenden Nutzeransprüche die weitere Optimierung der universitätsumspannenden Informations- und Sicherheitsstruktur notwendig machen.

Mit der vorliegenden Arbeit wurde nachgewiesen, daß die heutigen Kommunikations- und Sicherheitsanforderungen mit einem ATM-Backbone und geswitchtem Netz erfüllt werden können.