Realisierung von IT-Sicherheitszonen durch Virtualisierung der Netzwerkinfrastruktur am Universitätsklinikum Erlangen

Wentz B[1], Kaiser J[2], Prokosch HU[3]
[1]*Medizinisches Zentrum für Informations- und Kommunikationstechnik, Universitätsklinikum Erlangen, Deutschland*
[2]*Stabstelle für IT-Sicherheit, Universitätsklinikum Erlangen, Deutschland*
[3]*Institut für Medizininformatik, Biometrie und Epidemiologie, Lehrstuhl für Medizinische Informatik, Universität Erlangen, Deutschland*
bernhard.wentz@uk-erlangen.de

Einleitung und Fragestellung Im Universitätsklinikum Erlangen machen neue Anforderungen von Seiten des medizinischen Personals aber auch von Seiten der Patienten eine Neu-Orientierung der aktuellen Netzwerkstruktur erforderlich. Die Wünsche reichen von einem ausfallsicheren hochverfügbaren Netzwerk für wichtige klinische IT-Anwendungen wie Labor-Systeme, digitale bildgebende Verfahren, OP-Dokumentation, etc. hin bis zur Verwendung mobiler Arbeitsgeräte für die klinische Visite in einem Funknetzwerk sowie der Nutzung von Multimedia-orientierten Diensten für die Information von Mitarbeitern und Patienten. Schutz und Sicherheit der Daten in einem Netz sind nicht nur aus dem gesetzlichen Hintergrund des Datenschutzes motiviert sondern vielmehr aus den Erfordernissen der Anwender, die zum Erreichen der erforderlichen Dienstgüte neben der Ausfallsicherheit auch einen Schutz vor Zugriffen unbefugter Anwendergruppen und Vermeidung der Verbreitung von sog. Malware wie Computerviren erwarten. Wenngleich klinische Anwender ein Netzwerk eher als Gesamtheit aller Rechnersysteme, die über eine Netzwerk-Infrastruktur zusammengeschlossen sind, verstehen, ermöglicht genau diese Infrastruktur der aktiven und passiven Netzwerkkomponenten, also das eigentliche Local Area Network (LAN), den wichtigsten Ansatzpunkt für Maßnahmen zur Ausfallsicherheit und Kontrollmechanismen zur Unterstützung der IT-Sicherheit. Die Realisierung der unterschiedlichen Anforderungen resultiert in der Einrichtung von Sicherheitszonen durch neue voneinander getrennte LANs. Durch eine Neugestaltung der Netzwerkinfrastruktur durch Anschaffung zusätzlicher aktiver Komponenten ist eine physische Trennung zwar umsetzbar aber sehr kostenintensiv. Alternativ besteht die Option, getrennte logische Netze durch eine Virtualisierung der Netzwerkkomponenten einzurichten – also durch die Konfiguration virtueller LANs (VLANs) auf ein und derselben Infrastruktur. Somit wird es Zeit für ein Umdenken in Richtung neuer Konzepte und Lösungen, die nicht nur über die Netzwerktechniken auf den unteren Ebenen des OSI-Referenzmodells für die Datenkommunikation realisiert werden sollten [1]. Vielmehr fordert die Betrachtung der Netzwerkinfrastruktur und der darauf aufsetzenden Dienste und IT-Anwendungssysteme die Einbeziehung von IT-Sicherheitsmaßnahmen auch auf den oberen Ebenen des OSI-Referenzmodells.

Historie und Umfeld Seit 1993 wurde im Rahmen des sog. Netzwerk-Investitionsprogrammes (NIP) die gesamte Universität Erlangen inklusive des Universitätsklinikums verkabelt [2]. Zur Überbrückung der größeren Strecken zwischen den Gebäuden, die im gesamten Erlanger Stadtgebiet verteilt sind, wurden Glasfaserkabel verlegt, ebenso zwischen den Verteilern innerhalb der Gebäude. Von diesen Verteilern führen Kupferkabel sternförmig bis hin zu den Netzwerkdosen in den einzelnen Räumen. Durch geeignete aktive Netzwerkkomponenten (Switches, Router, etc.) wurde die Verkabelung in den medizinischen Einrichtungen zum sog. *Medizinischen Versorgungsnetz* zusammengeschaltet und im übrigen Bereich der Universität Erlangen-Nürnberg zum sog. *Wissenschaftsnetz* verbunden. Die Forderungen der Anwender im Medizinischen Versorgungsnetz nach Diensten wie E-Mail und Internet-Zugang resultierten in der Umsetzung eines geschützten Überganges zum Wissenschaftsnetz der Universität durch ein Firewall-System, das für Bedrohungen von außen eine wirksame Schutzmaßnahme darstellt [2]. Sicherheitsrisiken innerhalb des Netzwerkes - z.B. durch Computer-Viren, aber auch durch bestimmte Aktionen weniger verantwortungsbewusster Anwender - machten zusätzliche organisatorische und technische Maßnahmen erforderlich. Neben dem obligatorischen Anschluss an das *Medizinische Versorgungsnetz* wurden in einigen Kliniken des Universitätsklinikums zusätzlich auch Zugänge für das *Wissenschaftsnetz der Universität* zur Verfügung gestellt. Beide LAN-Infrastrukturen sind völlig voneinander getrennt, d.h. ein Endgerät, das an einer Netzwerkdose des Wissenschaftsnetzes angeschlossen ist, hat keinen Zugriff auf das Medizinische Versorgungsnetz.

Konzepte und Realisierungen Die künftigen Anforderungen lassen sich mit dem vorhandenen hochsicheren Netz für die Patientenversorgung auf der einen Seite und dem weniger sicheren Wissenschaftsnetz der Universität auf der anderen Seite nicht umsetzen. Das Ziel ist ein ausgewogenes Sicherheitskonzept mit unterschiedlichsten Anforderungen, was in der Einrichtung mehrerer Netzwerke für unterschiedliche Aufgaben mit jeweils eigenen Sicherheitsrichtlinien resultieren wird.

Mit der heutigen Maßgabe der Kostenreduktion im Gesundheitswesen lässt sich eine Multiplikation der Netzwerkinfrastruktur für IT-Anwendungen mit unterschiedlichen Sicherheitsanforderungen zumindest aus betriebswirtschaftlichen Gründen nicht mehr verantworten. Hierbei sind nicht nur die Kosten für die aktiven Komponenten wie Router und Switches zu betrachten, sondern ebenso die weiteren Aufwendungen für Glasfaserverkabelung zwischen Gebäuden, der zusätzliche Platz in Verteilerräumen und der deutliche höhere Aufwand für das Management der geschaffenen Strukturen, der mit der Anzahl der Geräte ansteigt.

Die Methode der Wahl stellt daher die Virtualisierung auf Netzwerkebene dar: Die gängigen für die Netzwerkinfrastruktur verwendeten aktiven Hardware-Komponenten erlauben die Konfiguration verschiedener logisch voneinander getrennter virtueller Netze (VLANs), denen unterschiedliche Funktionalitäten und Dienste zugewiesen werden können. Mehrere virtuelle Netze können auf eine physische Infrastruktur abgebildet werden, also auf denselben Kabeln und aktiven Komponenten umgesetzt werden. Eine Netzwerkdose wird einem definierten virtuellen Netzwerk und damit auch der in diesem Netz definierten Sicherheitszone zugewiesen. Dadurch lassen sich einerseits - abhängig von den unterschiedlichen Sicherheitsanforderungen der Anwendungen und Dienste - verschiedene IT-Sicherheitszonen realisieren, andererseits aber auch bevorzugte Wege für wichtige Anwendungen - z.B. bei Performance-Problemen - definieren.

Mögliche Sicherheitszonen richten sich nach den Anforderungen des Klinikums:

- In einem Netzwerk für die medizinische Versorgung der Patienten werden nur zertifizierte und durch die zentrale IT-Abteilung administrierte Geräte eingesetzt. Das entspricht quasi dem Status Quo im Medizinischen Versorgungsnetz, das aktuell als VLAN umstrukturiert wird.
- Wissenschaftler, die zwar Angehörige der Universität sind, aber selbst aus Datenschutzgründen nicht auf Patientendaten direkt zugreifen dürfen, können in einem Netzwerk für die medizinisch-wissenschaftliche Datenverarbeitung im Rahmen von Kooperationsprojekten im Klinikum medizinische Forschung betreiben. Diese VLANs werden sich als klinikumsweite Alternative für die wenigen direkten Zugänge zum Wissenschaftsnetz im Universitätsklinikum etablieren.
- Mobile Systeme sollen über funkgestützte Infrastrukturen (WLAN) auch schützenswerte Patientendaten sicher kommunizieren können. Dafür müssen zur Verbindung und Verkabelung der sog. WLAN Access Points sichere WLAN-Backbones eingerichtet werden. Dieses Konzept wird am Universitätsklinikum Erlangen derzeit in der Chirurgischen Klinik und der Medizinischen Klinik I pilotiert und über ein VLAN umgesetzt.
- Ein weiterer interessanter Bereich ist das Feld der Telemedizin. Hier sieht sich ein Netzbetreiber in der Rolle, nahe am Patienten und Arzt leitungsfähige Infrastrukturen für Multimedia-Anwendungen zur Verfügung zu stellen. Diese gehen Kommunikationsbeziehungen nach außen ein und dürfen daher nicht im hochsicheren medizinischen Versorgungsnetz eingesetzt werden. Für die an der Kommunikation mit anderen Arztpraxen und Krankenhäusern beteiligten Geräte ist daher eine weitere Sicherheitszone zu schaffen, mit der eine sichere Kommunikation nach außen über Technologien wie Virtual Private Networks (VPN) umgesetzt werden kann.
- Im Rahmen der sog. Hoteldienstleistungen für Patienten treten immer mehr elektronische Angebote in den Vordergrund. So ist heute davon auszugehen, dass ein Patient auch während seines Krankenhausaufenthalts sowohl elektronisch kommunizieren als auch unterhalten werden möchte. Für diesen Zweck sind besondere Vorkehrungen zu schaffen, welche ein Eindringen der Nutzer in geschützte Bereiche verhindert. Dieses Konzept wird derzeit am Universitätsklinikum Erlangen in der Geburtshilfe der Frauenklinik über den Zusammenschluss von ca. 50 Multimedia-Terminals für Patienten mit Zugang zum Internet in einem VLAN pilotiert.

Diskussion und Ausblick Um die Integrität der Virtualisierung der LANs zu gewährleisten, muss über die Sicherheit der beteiligten Komponenten diskutiert werden. Es ist prinzipiell möglich, dass durch eine vorsätzliche Fehlnutzung von Endgeräten innerhalb eines virtuellen Netzes andere Endgeräte gestört oder auch Daten ausgespäht werden [3]. Zunächst müssen die Risiken der zwischen den aktiven Komponenten automatisch ablaufenden Verfahren bewertet werden. Diese Verfahren übernehmen in modernen Netzwerken Steuerungs- und Koordinierungsfunktionen. Durch

gezielte Manipulation dieser Verfahren kann ein Angreifer seine Sicherheitszone verlassen und in eine andere eindringen. Ebenso sind Fehler in der Konfiguration der aktiven Netzkomponenten nicht auszuschließen, einerseits verursacht durch Kommunikationsprobleme, die zwischen den Netzwerkbetreuern und den Anwenderbetreuern vor Ort auftreten können, andererseits aber auch bedingt durch direkte Konfigurationsfehler der Netzbetreuer. Somit müssen technische Verfahren gefunden werden, die solche Konfigurationsfehler aufdecken. Eine Möglichkeit besteht darin, den tatsächlichen Ist-Zustand mit einem vorher definierten Sollzustand zu vergleichen, was automatisch durch periodische Abfragen der beteiligten Komponenten realisierbar ist. Auf einer höheren Abstraktionsebene können sogar Richtlinien mit Aktionen verglichen werden. Verbindungen zwischen den unterschiedlichen Sicherheitszonen lassen sich durch Firewalls und Application Gateways realisieren und schützen [3]. Ein mögliches Verfahren ist das Einsetzen eines verteilten Systems zur Richtlinienüberwachung, das zwischen den Übergabepunkten der einzelnen Sicherheitszonen Verstöße gegen zuvor definierte Richtlinien analysiert und bewertet.
Das Universitätsklinikum Erlangen befindet sich auf dem besten Weg zu einem der führenden modernen Medizin-Dienstleister bei dem die beschriebenen Konzepte aus den Bereichen der IT-Sicherheit und der Netzwerktechnologie eine wichtige Rolle spielen werden, um die neuen Anforderungen der Patienten und Mitarbeiter umzusetzen.

Literatur

[1] Dickson G, Lloyd A. Open Systems Interconnection. New York, London, Toronto, Sydney, Tokyo, Singapore: Prentice Hall, 1992

[2] Hefler T, Beier E, Wentz B. Anbindung sensibler medizinischer Netze an internationale Netze. Allergologie 1994, 17/1:26.

[3] Wentz B, Kaiser J. Migration von herkömmlichen Sicherheitsmaßnahmen hin zu einer Service-orientierten IT-Sicherheit im verteilten Netzwerk des Universitätsklinikums Erlangen – ein notwendiger Paradigmenwechsel? In Rexer H, Friedrich M, Fankhänel A, Thorn K, Hrsg. Medizinische Dokumentation wichtig oder nichtig? Tagungsband 9. DVMD-Fachtagung. Alius Verlag 2006: 365-370