



In Theorie und Praxis die Nase vorn Das neue WLAN-Sicherheitskonzept an der Universität Rostock

Universitäten stellen in mancher Hinsicht besondere Anwender von informationstechnischen Systemen dar. Etwa immer dann, wenn die angehenden Akademiker darangehen, Rechner oder Peripherie auf die Grenze ihrer Leistungsfähigkeit hin zu überprüfen. Aber auch im täglichen Einsatz können Hochschulen außergewöhnliche Anforderungen an das IT-Equipment stellen: Hohe Nutzerzahlen mit noch höherer Fluktuationsrate, fragmentierte Campus oder häufig auch altherwürdige Gebäude sind nur einige der zu lösenden Aspekte.

Die Universität in Rostock ist in bezug auf ihre Wireless LAN-Installation gleich in mehrfacher Hinsicht ein untypischer Nutzer: Einerseits wollen die rund 14.000 Studenten ganz simpel die Vorzüge eines drahtlosen Zugangs zu Mailsdiensten oder Internet nutzen, andererseits treiben die involvierten Institute die Weiterentwicklung des Netzwerkes auch kontinuierlich voran. Einerseits wird in Forschungsprojekten die Herstellerindustrie bei der Fortentwicklung der Produkte unterstützt, andererseits stellt die Cleverness der Studenten schon auch mal die Verantwortlichen des universitären Rechenzentrums vor neue Herausforderungen, etwa in punkto Zugangssicherheit. Daher verwundert es nicht, dass die Uni Rostock nicht nur federführend bei der Entwicklung des Projektes „Notebook University“ für das Bundesministerium für Bildung und Forschung war, sondern nach wie vor

Trends setzt, z.b. mit einem für Deutschland völlig neuen Sicherheitskonzept.

Erste Hochschule in Europa

Die Ära der WLAN-Kommunikation begann in Rostock bereits im Jahre 1999, als die Hochschule als erste in Europa und weltweit mit zwei anderen Universitäten ein flächendeckendes WLAN-Netzwerk installierte, getrieben im wesentlichen vom Institut für Informatik unter der Leitung von Professor Tavangarian. In kurzer Zeit wurde der gesamte Campus mit Zugängen für die drahtlose Kommunikation ausgestattet. Schon allein dies war keineswegs eine triviale Aufgabe, schließlich sind dabei über 300 Gebäude an 34 verschiedenen Standorten bis hin zum 15 Kilometer entfernten Warnemünde zu versorgen.

Zum Einsatz kamen dabei Access Points von

Enterasys, die teilweise über hochperformante LWL-Verbindungen an das zentrale Datennetz herangeführt werden. Alle wichtigen Bereiche wie Hörsäle, Mensa, Cafeteria oder Aufenthaltsräume mit Sitzcken sind mit WLAN-Zugängen ausgestattet. „Zumindest alle Bereiche, die nicht mit einer konventionellen Datendose für den Netzwerkzugang ausgerüstet sind,“ betont Gunter Frisch, im Rechenzentrum für die Betreuung des WLAN zuständig. Denn hinsichtlich der Bereitstellung von Services für Studenten und Mitarbeiter stellt das WLAN zunächst einfach ein Element des gesamten Datennetzes dar.

Die in Rostock bereits frühzeitig gesammelten Erfahrungen mit dem Einsatz mobiler Kommunikationssysteme sollten schon bald beispielgebend für die gesamte deutsche Hochschullandschaft werden. Eine im wesentlichen von Prof. Tavangarian erstellte Studie wurde die Basis für das BMBF-Förderprogramm „Notebook-University“, auf dessen Grundlage bis heute eine Vielzahl von Hochschulen mit einer WLAN-Infrastruktur ausgestattet wurden.

Allerdings: die frühzeitige Adaption neuer Technologien bringt nicht nur einen Wissensvorsprung, sondern führt gelegentlich auch dazu, an erste Produktgenerationen gebunden zu sein, deren Funktionalität oder Konzeption durchaus noch Fragen offen lassen.

Sicherheit als Praxisanforderung

Mit der Übergabe des WLAN-Projektes, zunächst als Referenz für den Informatikbereich selbst ins Leben gerufen, an das Rechenzentrum und den Echtbetrieb zeigte sich schon bald, dass das zugrundeliegende Sicherheits- und Managementkonzept für die produktive Nutzung des Netzes durch einige Tausend User nicht ausreichen würde. „Das war WLAN von Hand,“ beschreibt Gunter Frisch die damalige Situation. Alle MAC-Adressen mussten von Hand erfasst und in den zentralen Router eingetragen werden. Rechner, die nicht eingetragen waren, konnten

dann zwar das WLAN nutzen, aber sich beispielsweise nicht in das Uninetzwerk einloggen, weil das WLAN als eigenes Virtuelles LAN geführt wird. Neben dem Management zeigt sich vor allem die Zugangskontrolle als nicht ausreichend.

„Wireless LAN ist gerade auch für Universitäten eine großartige Technologie, aber ohne Sicherheit geht es heute einfach nicht mehr,“ beschreibt Peter Eschholz, Systemingenieur am Lehrstuhl für Rechnerarchitektur die Situation. „Mit im Access Point vorgehaltenen MAC-Adressen wäre es langfristig nicht mehr gegangen.“



Also machte man sich auf die Suche nach einem geeigneten Konzept zur Erhöhung der Zugangssicherheit und wurde fündig beim Hersteller Bluesocket. Nach einigen Produkttests mit Wettbewerbslösungen entschied man sich in Rostock für den Einsatz der Wireless Gateways des Unternehmens, um den Sicherheitsbereich durch spezielle Hardware vom WLAN zu trennen.

Bluesocket Wireless Gateways sind eine Familie speziell für die Sicherheit und das Management in WLANs konzipierter Geräte mit Durchsatzraten von 100 Mbps bis hin zu 1 Gbps. Die Gateways wurden speziell für den Einsatz in existierenden WLAN-Infrastrukturen entwickelt. Sie arbeiten mit allen 802.11 a/b/g standardkonformen WLAN-Komponenten zusammen. Zur Erhöhung der Netzwerksicherheit oder zur Vereinfachung des

WLAN-Managements werden sie ohne weitere Hardwareänderungen einfach in das vorhandene Netzwerk integriert. Auch eine spezielle Client-Software ist nicht erforderlich. Mit diesem herstellerunabhängigen Ansatz sind die Bluesocket Produkte dazu prädestiniert, Sicherheits- und Managementschwachstellen auch in vorhandenen Netzwerken zusätzlich oder nachträglich zu beseitigen.

Wireless Gateways als Lösung

Die Grundfunktionalität der Wireless Gateways umfasst die Authentifizierung von Nutzern, die rollenbasierte Zugangskontrolle zu Ressourcen, eine starke Verschlüsselung, ein komfortables und wirksames Management der WLAN-Infrastruktur sowie das Management von Bandbreiten und Servicequalitäten (QoS).

In der Praxis hat sich die Administration der WLANs und seiner Nutzer deutlich entspannt. Die vor gut einem Jahr vor der Gateway-Installation prägenden Probleme, etwa die Umgehung der Zugangsbeschränkungen durch findige Studenten oder die manuelle Pflege der MAC-Adressen wurden durch die automatische und konsequente Authentifizierung aller Nutzer sowie die Anbindung an die RADIUS Nutzerdatenbank ausgeräumt.

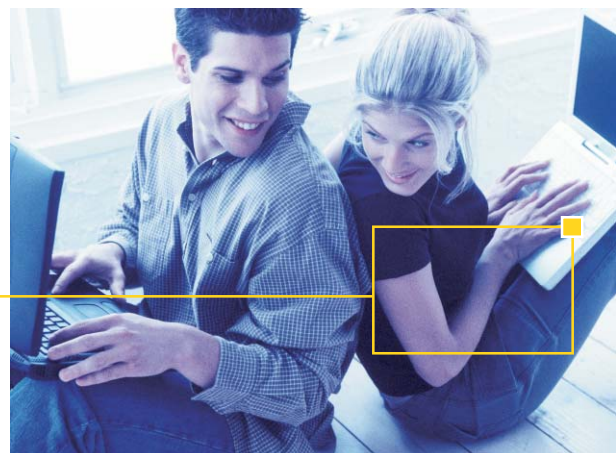
Jeder neue Student bekommt heute einen Account zugewiesen, der ihn zur Nutzung der öffentlichen Einrichtungen, etwa den PC-Pool, berechtigt. Dieser Account gilt auch für die Nutzung des WLAN. Sobald der Anwender eine Webside öffnet, die sich außerhalb des WLAN befindet, muss er sich gegenüber dem Gateway authentifizieren und erhält einen Tunnel geöffnet. Der Datenzugang kann dann wahlweise über ein VPN oder aber unverschlüsselt erfolgen, wobei für die meisten genutzten Anwendungen wie Browser oder Dateidownload die unverschlüsselte Variante genutzt wird.

Neben den Sicherheitsfunktionen der Bluesocket Gateways kommen in Rostock auch die Policy Management und Quality of Service Funktionen

zum Einsatz, wenn auch nicht mit der gleichen Bedeutung wie die Authentifizierung. Vor allem wohl auch deshalb, weil reine Bandbreite im Universitätsnetzwerk nicht ausgesprochen knapp bemessen ist. Trotzdem hat man sich etwa entschieden, Bandbreite pro User bis zur DSL Geschwindigkeit bereitzustellen und nicht wie bis dato mit bis zu 10 Mbps. Diese Limitierung auf 1Mbps dürfte jedoch nicht als allzu große Einschränkung empfunden werden, es sei denn bei Nutzern, die sich extensiv dem File-Sharing verschrieben haben.

Alles in allem ist die Nutzung jedoch frei von Kapazitätsproblemen. Auch wenn an der Universität rund 14.000 Studenten immatrikuliert sind, so beträgt die durchschnittliche Zahl der parallel eingeloggtten User lediglich zwischen 130 und 150, wobei natürlich Spitzenwerte zu Ballungszeiten deutlich darüber liegen.

In Rostock kommen derzeit ein Wireless Gateway Bluesocket WG 2000 sowie ein WG 2100 zum Einsatz. Der unverschlüsselte Datendurchsatz eines WG 2100 beträgt bis zu 400 Mbps. Encrypted werden bis zu 150 Mbps erreicht. Damit ist eine ausreichende Kapazität sichergestellt. Der Entscheidung für den Einsatz zweier Systeme lagen wiederum Sicherheitsüberlegungen zugrunde. Beide Systeme werden redundant betrieben, so dass im Falle des Ausfalls eines Gerätes dessen Funktion unmittelbar vom zweiten übernommen wird.



Praxistest bestanden

Nach gut einjährigem Echtbetrieb des neuen Sicherheitskonzeptes zeigt man sich zufrieden mit der getroffenen Wahl. Derzeit steht die Umstellung der Software auf die neue Version 4.0 an. Die neue Version zeichnet sich durch erweiterte Sicherheitsaspekte, Skalierbarkeit, Durchsetzung von Policies und verbessertes Management aus. Als erster Hersteller unterstützt Bluesocket mit der Version 4.0 das EAP-FAST Protokoll für 802.1x sowie WPA. Zusammen mit anderen EAP Methoden wie LEAP, PEAP, TTLS, TLS und MD5 stellen die Wireless Gateways das umfangreichste Spektrum an Authentifizierungs- und Security-Methoden bereit.

Bei allem Wissensvorsprung, den man sich in Rostock auf dem Gebiet der mobilen Kommunikation erarbeitet hat, gibt man sich mit dem Erreichten doch nicht zufrieden. Neue, spannende Projekte sind bereits in Arbeit. Und die Ideenschmiede von Professor Tavangarian

wartet wieder mit kreativen Ansätzen auf. ‚Mobile Systeme für Mobile Systeme‘ ist ein solches Projekt, bei dem die Eignung von Wireless LANs etwa im Zug, auf der Autobahn oder gar in einer Boeing 747 erforscht wird. Hier gibt es bereits Kooperationen mit Auftraggebern aus der Wirtschaft. Ein anderes Projekt mutet dagegen eher idyllisch an: Hier kommen Fesselballons zum Einsatz, um die WLAN Abdeckung verschiedener Stadtteile aus der Luft auszuleuchten. Auf jeden Fall wird man im Hinblick auf den Einsatz von Wireless LANs aus Rostock noch einiges erwarten können.

WG-2100
Wireless Gateway



KONTAKTANGABEN

Wenn Sie herausfinden möchten, welche Vorteile der Bluesocket Wireless Gateway Ihrer Organisation bringen kann, kontaktieren Sie uns unter sales@bluesocket.com und wir organisieren einen Termin mit einem unserer geschätzten Vertriebs- und Supportpartner in Ihrer Nähe.

Oder holen Sie sich weitere Informationen auf unserer Website: www.bluesocket.com

Das Bluesocket-Logo, Secure Mobility und WG-2100 Wireless Gateway sind Marken von Bluesocket, Inc. © 2004 Bluesocket, Inc. Alle Rechte vorbehalten. Alle anderen Marken, Warenbezeichnungen und Unternehmen, auf die in diesem Text verwiesen wird, dienen ausschließlich zu Identifizierungszwecken und sind Eigentum der jeweiligen Unternehmen.