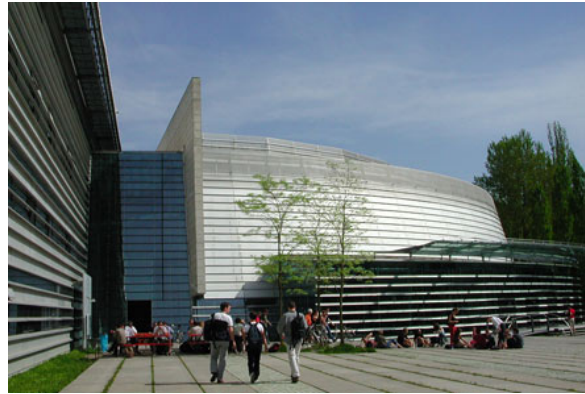


Eine der besten Adressen in Deutschland

Astaro Security Gateway schützt Hochschulnetz der TU München.

Die Technische Universität (TU) München und die Universität Karlsruhe gehören zu den besten Adressen in Deutschland. So lautet das Fachurteil des Centrums für Hochschulentwicklung (CHE) aus dem Mai 2006. Das CHE-Hochschul-Ranking umfasst mittlerweile mehr als 280 untersuchte Hochschulen im deutschen Raum, 30 Fächer, über 250.000 Studenten, 31.000 befragte Professoren und bis zu 34 unterschiedliche Kriterien pro Disziplin. Es enthält systematische Informationen über Studienfächer, Fachbereiche, Hochschulen und deren Standorte, Studienbedingungen und Studienmöglichkeiten, einschließlich der für die Lehre relevanten Forschung. Im Fach Informatik haben es die Universität Karlsruhe und die TU München in die Spitzengruppe geschafft und beide Einrichtungen spielen in den Kriterien IT-Infrastruktur und Forschungsgelder auf höchstem Niveau. Da passt es ins Bild, dass es bei der IT-Sicherheit eine weitere Parallele gibt: Die TU München vertraut bei der Absicherung ihrer IT-Netze auf die Technologie des Karlsruher Spezialisten für Netzwerksicherheit Astaro.



Die Verbindung zwischen München und Karlsruhe ist im Falle der Netzwerksicherheit eine Zusammenarbeit der ersten Stunde. „Wir haben bereits die 3er-Version der Astaro-Sicherheitslösung eingesetzt“, betont Thomas Mayerhofer, Netzwerkverantwortlicher der Fakultät Maschinenwesen, beschäftigt am Lehrstuhl für Informationstechnik im Maschinenwesen. Die Astaro AG suchte von Anfang an nach der Firmengründung im Jahr 2000 den direkten Kontakt zum akademischen Umfeld, schließlich kannte sich das Gründerteam ohnehin über die Universität. Auch die Geschäftsidee, Open-Source-Software unter Sicherheitsaspekten so aufzubereiten, dass sie in puncto Bedienungsfreundlichkeit und Preisgestaltung attraktiv wird, passte zur universitären Umgebung mit engen Budgetgrenzen. Viele Kunden hatten einfach nicht die notwendigen Personalressourcen, um Linux-Software auf dem neuesten Stand zu halten und benötigten Hilfestellung bei Installation und Konfiguration. Astaro bildete deshalb eine komplette Sicherheitslösung auf einer einfach zu bedienenden Oberfläche ab, deren technischer Kern auf Open Source basierte.

„Astaro-Partner erster Stunde“

„Im Universitätsumfeld gab es auf unserer Seite auch keinerlei Berührungspunkte gegenüber linuxbasierter Software“, erläutert Thomas Mayerhofer. „Und das vollkommen zurecht: Mittlerweile ist Open Source ein Qualitätskriterium, nicht nur was die niedrigeren Kosten betrifft.“ Zu den ersten Aufgaben der Firewall gehörte es, das Dateimanagement der Fakultät abzusichern. „Die Installation erfolgte im Jahr 2000 und wir haben als einer der größeren Lehrstühle an der Fakultät Maschinenwesen eine gewisse Vorreiterrolle gespielt“, bemerkt Thomas Mayerhofer nicht ohne Stolz. 2005 folgte dann die Installation der großen Gesamtlösung für die Fakultät. Besondere Komplikationen habe es dabei nicht gegeben: „Astaro ist sehr modular und problemlos von Lehrstuhl bis Fakultätsgröße anpassbar“, so Mayerhofer. Bei der Produktauswahl war auch eine Konkurrenzlösung im Gespräch: „Man läuft ja nicht blind durchs Leben, aber bei vielen großen Hersteller

stimmt das Preis-Leistungsverhältnis in Bezug auf unsere Anforderungen nicht. Wir können nicht einen Drittel unseres Etats für die Firewall ausgeben.“



Inzwischen ist Version 6 von Astaro Security Gateway an der Münchner Hochschule im Einsatz. „Wir wollten eine Lösung, die bedienbar ist und wir wollten einen Dienstleister, der das System auf dem neuesten Stand hält“, so Mayerhofer weiter. Bei der Beratung und Planung des Soft- und Hardwarekonzeptes hat sich die TU München deshalb mit der Münchner MICROSTAXX Gesellschaft für Informations- & Kommunikationslösungen mbH externe Hilfe ins Haus geholt. Martin Reil ist der

Geschäftsführer des Münchner Dienstleisters, der einen seiner Schwerpunkte auf Beratung und Support bei der IT-Sicherheit gelegt hat. „Die Astaro-Software ist günstig, sehr einfach zu installieren und das Web-Interface intuitiv bedienbar“, so Martin Reil über die Stärken der Karlsruher Unified-Threat-Management-Lösung (UTM).

Alle Sicherheitsupdates laufen über den Astaro Up2Date-Service, der eine komfortable Update-Automatik nutzt, um die gesamte Sicherheitsplattform und das Betriebssystem über Software-Patches, Virensignaturen und Linux-Aktualisierungen stets auf dem aktuellsten Stand zu halten. Zur Verwaltung des Systems steht Administratoren die intuitive, grafische Benutzeroberfläche WebAdmin zur Verfügung, mit der sie per Mausklick eine umfangreiche Netzwerkinfrastruktur verwalten können. Astaro Security Gateway bietet einen umfangreichen und effektiven Schutz vor den Risiken der Internetnutzung, wie Hacker, Viren, Würmer, Spam und den damit verbundenen Produktivitätsausfällen. Neun wichtige Sicherheitsanwendungen sind voll integriert in einem einfach zu handhabenden Paket. Astaro-Lösungen sind mittlerweile in über 30.000 Netzwerken in mehr als 60 Ländern im Einsatz und haben bereits viele Auszeichnungen erreicht.

„VPN ist ein großes Thema“

Zum Sicherheitsprojekt an der TU München meint Martin Reil: „Im Rahmen des Consultingvertrages haben wir Angebote auf Wirtschaftlichkeit und Leistungsfähigkeit geprüft und uns um die Projektüberwachung gekümmert. Unsere Aufgabe war es unter anderem, ein Windows-L2TP-IPSec-VPN mit Astaro ohne zusätzliche Clientsoftware zu realisieren.“ Insgesamt 3.000 Endgeräte sind auf dem Universitätsgelände flächen-



Herr Reil und Herr Mayerhofer

deckend über ein 1-GB-Backbone mit 10 GB an das Rechenzentrum angeschlossen. „VPN ist dabei ein großes Thema“, bestätigt Thomas Mayerhofer. „Viele Mitarbeiter nutzen die Option, sich über ein von Astaro geschütztes VPN auf dem Terminalserver einzuwählen oder andere Dienste abzufragen.“ Aktuell nutzen circa 70 Prozent der Mitarbeiter des Lehrstuhls für Informationstechnik im Maschinenwesen diese Funktionalität, Tendenz

steigend. Die Sicherheitstechnologien müssen also nicht nur innerhalb des Campusnetzes, sondern auch außerhalb der Unigrenzen greifen.



An der Fakultät Maschinenwesen der TU München spricht man von mehreren „Sicherheitsringen“, die eine bestmögliche Sicherheit erzielen sollen. Innen sind in der Hauptsache Microsoft-Systeme in Betrieb. Aus dem sicherheitstechnischen Blickwinkel gesehen liegen die Schwerpunkte auf einem konsistenten Patch Management, um bekannte Einfallstore schnell schließen zu können. Die Rechner nutzen Windows XP SP2 sowie die mitgelieferten Sicherheitsfeatures, um Risiken zu mindern. „Ab einem bestimmten Punkt

kommen dann linuxbasierte Systeme zum Einsatz“, erläutert Thomas Mayerhofer. Hier ist nicht nur das Preis-Leistungsverhältnis ausschlaggebend, sondern wirkt sich auch das akademische Umfeld mit traditionell guten Beziehungen zur Open-Source-Community aus. „Astaro ist uns außerdem aus der Presse und Testvergleichen gut bekannt“, analysiert Mayerhofer. „Für uns war wichtig, dass Astaro in Fachkreisen einen sehr guten Ruf hat, was sich beispielsweise an den Auszeichnungen in der Fachpresse ablesen lässt.“

„Schwächen von Monokulturen verhindern“

Zum Teil müssen die Sicherheitsringe auch außerhalb der Campus-Mauern errichtet werden. Im Kollegium nutzen immer mehr Mitarbeiter die Möglichkeit, Home Offices einzurichten. „Vorher musste man mehrere Tage planen und Sachen zusammenpacken, um keine Unterlagen zu vergessen“, blickt Thomas Mayerhofer auf die Zeit vor Astaro zurück. „Jetzt haben wir ein nach außen sicheres Netzwerk und die Möglichkeit, einen sicheren VPN-Tunnel aufzubauen, um darüber eine Vielzahl von Diensten zu nutzen.“ Die TU München verfügt über eine Campus-Lizenz von Astaro Security Gateway, die allen Lehrstühlen den Einsatz von Astarotechnologie

ermöglicht, um die elektronischen Informationen vor fremdem Zugriff zu schützen und digitalen Eindringlingen einen Riegel vorzuschieben. „Allerdings haben nur wenige der 28 Lehrstühle von Anfang an auch Astaro eingesetzt“, räumt Thomas Mayerhofer die bereits erwähnte Vorreiterrolle seines Lehrstuhls ein. Mittlerweile sind an der Fakultät Maschinenwesen der TU München jedoch „die unterschiedlichsten Geräte im Einsatz, auf denen Astaro-Software läuft“. Zusätzlich zu den VPN-Funktionalitäten baut die Hochschule auf E-Mail-Scanning der POP3- und SMTP-Server, Firewall-Schutz und inhaltsbasierte Filterung der HTTP-Dienste.

TU München - www.tu-muenchen.de

Die Technische Universität München ist eine international anerkannte Forschungsuniversität mit mehr als 60 Bachelor- und Master-Kursen. Die zwölf Fakultäten, verteilt auf die Standorte München, Garching und Weihenstephan, erzielen Spitzenergebnisse in Naturwissenschaft und Technik, in Medizin und den Life Sciences. In Zentralinstituten werden Bereiche einzelner Fakultäten zusammengeführt, um sich auf wissenschaftlicher Ebene zu ergänzen und Raum für interdisziplinäre Forschungsprojekte bereitzustellen. Mit rund 20.000 Studierenden, davon 20 Prozent aus dem Ausland, 440 Professorinnen und Professoren und etwa 8.500 Mitarbeiterinnen und Mitarbeitern zählt die TU München zu den größten Hochschulen Deutschlands.



Im universitären Umfeld ist es nicht ganz einfach, eine einheitliche Sicherheitspolicy durchzusetzen. Das liegt an den Besonderheiten bei Forschung und Lehre, denn die Mitarbeiter an der Fakultät sind zur Erfüllung ihrer Aufgaben zumeist auf verschiedenste Dienste und Verbindungen angewiesen. Mayerhofer: „Sie haben keine Einschränkungen, auch wenn es aus sicherheitstechnischer Sicht nicht unbedingt ideal ist.“ Jeder Lehrstuhl ist eigenständig verantwortlich. „Wir haben da immer nur beratende Funktion und geben technische Hilfestellung“, umreißt Thomas Mayerhofer die Aufgabe seiner Abteilung.

Fazit

Anfang 2005 stellte die Fakultät Maschinenwesen der TU München auf Astaro Security Gateway um. Auch wenn die Hochschule manche Funktionen der UTM-Lösung bisher noch nicht nutzt, ist Thomas Mayerhofer als Projektverantwortlicher „mit der Gesamtlösung glücklich“. Nach dem Erwerb der hochschulweiten Campuslizenz wechselten nicht alle Lehrstühle „auf einen Schlag, aber mittlerweile sind 75 Prozent auf unserem Stand“, lautet sein Resümee. Nach einer kurzen Eingewöhnungsphase, die er sich nicht zuletzt mit einer natürlichen Hemmschwelle vor Neuem erklären lässt, „waren die Leute überrascht, wie einfach dieses mächtige Werkzeug zu bedienen ist“. Die Zusammenarbeit mit Astaro verzeichnet er weiteren als Pluspunkt, denn „mit dem Support lassen sich neue Features besprechen und abstimmen, die dann zwei Releases später auch umgesetzt werden. Das geht nicht bei anderen großen Herstellern.“

MICROSTAXX - www.microstaxx.de

Seit 1990 ist MICROSTAXX eines der führenden Systemhäuser für individuelle IT-Lösungen mit deutschlandweiter Ausrichtung und Sitz in München. MICROSTAXX betreut schwerpunktmäßig mittelständische Unternehmen aller Branchen sowie öffentliche Auftraggeber aus den Bereichen Bildung, Wissenschaft, Forschung und Lehre. MICROSTAXX pflegt bewusst exklusive, langfristige Kooperationen mit ausgewählten Herstellern, um professionelle und hochkompetente Services für deren Lösungen anbieten zu können. MICROSTAXX verfügt über Qualifizierungen dieser Key-Partner auf höchstem Niveau. Die regelmäßig durchgeführte ISO-9001-Zertifizierung gewähr-leistet standardisierte und optimierte Geschäftsprozesse als Basis für eine präzise und zuverlässige Zusammenarbeit mit Herstellern und Kunden. Die MICROSTAXX-Kompetenzen umfassen alle Bereiche, die eine qualifizierte Konzeption, Realisierung und Instandhaltung einer anspruchsvollen IT-Lösung sicherstellen. Die Planung und Umsetzung von individuellen Infrastrukturen stehen im Vordergrund der Dienstleistungen und Consulting-Services. Ebenso bietet MICROSTAXX bei Bedarf ein komplettes IT-Outsourcing und die Übernahme des IT-Managements.

