

## **Elektronische Türsteher sichern Universitäten**

**Wer heute ein Studium absolviert, ist mit seiner Universität verbunden – und zwar über das Internet. Leihfristen für Bücher, Klausurthemen, Recherchen oder Rückmeldungen wickeln Studenten zunehmend online ab. Um eventuellem Missbrauch vorzubeugen, hat die Fernuniversität Hagen, gemeinsam mit mehreren anderen Hochschulen in Nordrhein-Westfalen, nun eine Public-Key-Infrastructure-Lösung erprobt. Mit einem so genannten eToken haben die Studenten dabei von jedem beliebigen PC aus einen sicheren Zugriff auf das Netzwerk der Hochschule.**

Es sind personenbezogene Daten und sensible Informationen, die es unabdingbar machen, das Netzwerk einer Hochschule abzusichern. Gleichzeitig sollen sich alle Studierende aber auch problemlos in die für sie relevanten Bereiche einloggen können, am besten von jedem beliebigen Ort der Welt. Eine große Herausforderung, denn „personenbezogene Daten müssen jederzeit vor unerlaubten Zugriffen, Veränderungen oder Diebstählen bewahrt werden“, wie Robert Dürr, Solution Line Manager für das Thema Security beim Kölner Netzwerkdienstleister NK Networks & Services, betont. Zwar sind die Rechenzentren der Bildungseinrichtungen in der Regel durch Firewalls und Virens Scanner gut gegen Angriffe von außen geschützt. „Doch oft ist es nicht die Bedrohung von außen, sondern die Bedrohung von innen, die den Hochschulen Probleme bereitet“, so der Experte. Das größte Problem ist dabei die hohe Anzahl der Nutzer, die zudem ständig wechselt, etwa wenn die Studenten ihr Studium beenden oder neu beginnen. Hinzu kommt, dass die Nutzer nicht wahllos auf alle, sondern tatsächlich nur auf die für sie bestimmten Daten zugreifen dürfen.

Um diesen besonderen Anforderungen an den Datenschutz gerecht zu werden, setzen immer mehr Bildungseinrichtungen auf eine so genannte Public Key Infrastructure (PKI). Diese Infrastruktur bildet die Grundlage für die Verschlüsselung der vorhandenen Daten und sorgt gleichzeitig dafür, dass jeder Anwender beim Einloggen ins Netz zweifelsfrei identifiziert wird. So ist gewährleistet, dass ein Nutzer auch tatsächlich nur die für ihn bestimmten Informationen lesen oder gar verändern kann. Als „Sesam öffne Dich“ bekommt jeder Nutzer ein Schlüsselpaar zum Codieren und Entziffern der Informationen. Fehlt einer der beiden Schlüssel oder ist ungültig, sorgt der elektronische Türsteher dafür, dass der Nutzer ausgesperrt bleibt.

### **USB-Stick als Lösung**

In Nordrhein-Westfalen haben mittlerweile mehrere Hochschulen diese Lösung getestet und sind dabei bisher auf überwiegend positive Resonanz gestoßen. Zumal die erprobte Lösung mit einem neuen „Zaubergerät“, dem so genannten eToken verbunden ist. Was wie eine neue Spezies von Tamagochis klingt, ist ein USB-Stick, hat die Größe eines normalen Hausschlüssels und den Vorteil einer integrierten Smartcard, auf der ein privater Schlüssel sowie das dazugehörige Zertifikat gespeichert sind. Wird dieser, von der israelischen Firma Aladdin Knowledge Systems entwickelte Speicherstift, in den USB-Anschluss eines beliebigen Computers im Hochschulnetzwerk gesteckt, braucht der Nutzer nur noch das dazugehörige Passwort eingeben, um einen sicheren Zugriff auf die für ihn bestimmten hochschulinternen Anwendungen zu erhalten. Und mit Hilfe eines One-Time-Passwortes, das in Verbindung mit einem persönlichen Code nur wenige Sekunden gültig ist, ist sogar der sichere Zugriff auf das Hochschulnetz über das offene Internet gewährleistet.

Ein Feature, das vor allen Dingen Hochschulen wie der Fernuniversität in Hagen zugute kommt, deren Studenten nicht nur über ganz Deutschland, sondern über die ganze Welt verteilt sind. „Bereits seit 1996 testen wir hier PKI-Lösungen im Rahmen von Förderprojekten und setzen sie im Produktionsbetrieb ein“, berichtet Henning Mohren, Projektleiter an der Fernuniversität Hagen. Allerdings war es der Hochschule zu wenig, damit lediglich die Flexibilität zu erhöhen. Die Verantwortlichen wollten außerdem die Ausstellung der für die PKI-Lösung notwendigen Zertifikate vereinfachen, denn bislang musste dieses Verfahren durch das Administrationspersonal der Hochschule manuell bedient werden. Die Lösung fand sich schließlich mit der Entwicklung eines „Zertifizierungsautomaten“. Er sorgt dafür, dass die Studenten nun nicht mehr persönlich in Hagen erscheinen müssen, um sich zertifizieren zu lassen.

### **Benutzerdatenbank als Grundlage**

Grundlage der Identifikation ist die bestehende Benutzerdatenbank an der Hochschule. Um ein Zertifikat zu erhalten, muss der Student an einem von ihm selbst gewählten, beliebigen internetfähigen

Arbeitsplatz die Website der Fernuni in Hagen aufrufen und seine Matrikelnummer angeben. Der Webserver sucht aus der Benutzerdatenbank den entsprechenden Datensatz heraus, generiert ein Passwort und schickt dieses per Post an die gefundene Adresse. In einem zweiten Schritt wird das Passwort dem Adress-Satz hinzugefügt. Hat der Student das Passwort erhalten, beantragt er über ein weiteres Webformular sein Zertifikat.

„Durch die Ablösung der bisherigen Softwarezertifikate mit dem eToken erreicht die Fernuniversität in Hagen eine sichere Zweifaktor-Authentisierung“, berichtet Mohren. Mit dem Einsatz des USB-Sticks lasse sich die bisherige Arbeitsplatz- und Browser-Bindung aufheben. Auch weitere Nutzungsmöglichkeiten des eToken werden an der Fernuni in Hagen bereits getestet. So ist ein Ziel das Single Sign-on, bei dem sich der Anwender anhand seines eToken und des eToken-Passwortes sicher an verschiedenen Applikationen anmelden kann. „Damit braucht man sich nicht mehr verschiedene Passworte zu merken und hat jederzeit eine Garantie für den Schutz seiner persönlichen Daten“, betont Sicherheitsexperte Robert Dürr. Und auch für Studenten, die bisher keine Erfahrung auf dem Gebiet der PKI-Nutzung hatten, ist das Verfahren einfach durchführbar. In Hagen ist man deshalb davon überzeugt, dass sich der eToken bald in der gesamten deutschen Hochschullandschaft durchsetzen wird.