

Anwenderbericht: Wie Studentenausweise und Secure Logon von digitronic den Zugriff auf öffentliche Rechner sicher machen

Hochschule für Musik Dresden: Bei der Sicherheit ist Musik drin

Die Sicherheit von öffentlichen oder halb-öffentlichen Rechnersystemen ist seit Jahren ein heikles Thema. Gerade an Schulen, Hochschulen oder Bibliotheken gehen die Benutzer wenig sorgsam mit Daten wie Benutzername und Passwort um. Doch oftmals reichen diese wenigen Daten, die etwa untereinander getauscht werden oder beim Anmelde- und Abmeldevorgang an den Rechner nicht zuverlässig gespeichert bzw. wieder gelöscht werden, aus, um unbefugt an personenbezogene, sensible Daten zu kommen.

Vor der Herausforderung, dieses Problem zu lösen, stand Ende 2007 auch die Hochschule für Musik Dresden Carl Maria von Weber. Die Hochschule gehört zu den ältesten Einrichtungen ihrer Art in Deutschland. Ihr Ursprung im Jahre 1856 ist mit den Namen Carl Maria von Weber, und Richard Wagner verbunden. Heute studieren dort mehr als 600 junge Menschen aus aller Welt Musik. In dem von der Hochschule betriebenen Internet-Pool, meldeten sich die Studenten über Jahre bei Windows XP lediglich mit Benutzername und Passwort an. „Es stellte für uns ein enormes Sicherheitsproblem dar, dass die Benutzer ihre Logindaten untereinander einfach austauschen konnten“, sagt Ina Wolf, IT-Betreuerin der Hochschule für Musik. Die Hochschule stellt ihren rund 200 zur Nutzung zugelassenen Studenten mehrere „Thin-Client“-Arbeitsplätze, zur Verfügung, die von den Studenten für PC-Arbeiten und Recherchen im Internet verwendet werden können. „Daher suchten wir nach einer Lösung, die idealerweise die Verwendung der schon im Umlauf befindlichen Mifare-Karten der Studenten zur sicheren Anmeldung an die PCs ermöglichen sollte“, so Ina Wolf weiter. Die Mifare-Studentenausweise wurden zuvor bereits in Verbindung mit einer PIN für die Nutzung des Rückmeldeterminals, den bargeldlosen Zahlungsverkehr und ähnliche Dienste genutzt.

Bei der Suche nach einer passenden Lösung empfahl die Bechtle AG, die die Hardware der Hochschule betreut, die Lösung Secure Logon der digitronic GmbH. Secure Logon ist ein Sicherheitssystem zur Anmeldung an PCs und anderen Geräten, das Besitz und Wissen voraussetzt. Besitz meint die Verwendung eines USB-Token oder einer Smartcard, während Wissen die Verwendung einer speziellen PIN-Nummer bedeutet. Diese als

Zwei-Faktor-Authentifizierung bezeichnete Lösung Secure Logon ist Teil der digitronic Security Suite, die die Chemnitzer Firma digitronic sowohl Firmen- als auch Privatkunden anbietet.



Nach der Entscheidung für die Lösung von digitronic mussten einerseits Anpassungen an der Software vorgenommen und andererseits Hardware-Komponenten gekauft werden. „Zentrale Anforderung an die Erweiterung der Software war die Ergänzung des Token Management Systems um eine Protokollierungsfunktion“, berichtet Wolf. Das Token Management System, kurz TMS, hilft bei der Überwachung aller mit Zugriffsrechten am System ausgestatteter Benutzer von einem zentralen Administrationspunkt aus. Die angepasste Software konnte zusätzlich folgende Inhalte protokollieren: Den Zeitpunkt des An- und Abmeldens eines Token am jeweiligen PC, die Token-spezifische ID sowie Token-spezifische Informationen wie Besitzer, Beschreibung und Berechtigungen. Um den Studierenden die Nutzung des neuen Systems so einfach wie möglich zu gestalten, übernahm digitronic auch die Anpassung der Software im Hinblick auf die Nutzung der bereits vorhandenen PIN-Nummern. „Unsere Studierenden verwenden also jeweils die selbe PIN-Nummer, um sich an die öffentlichen Rechner anzumelden einerseits und am Terminal die Studiengebühren zu bezahlen oder das Kopiersystem zu nutzen“, beschreibt Wolf. Über die Anschaffung der Hardware schließlich war schnell entschieden: Die Thin Clients wurden um USB-Kartenlesegeräte der Firma Baltech ergänzt, die kontaktlose Speicherkartensysteme unterstützen.

Die Implementierung des Token-Managers sowie von Secure Logon nahm die IT-Leiterin

zusammen mit der Bechtle AG vor. Seit Januar 2008 ist das neue System nun im Einsatz und erfüllt die Anforderungen der Hochschule für Musik zur vollen Zufriedenheit: „Wir sind bisher sehr zufrieden, weil das Sicherheitsproblem behoben werden konnte“, berichtet Wolf: „Die Kontrolle der Internetnutzung der eingetragenen (berechtigten) Benutzer, exmatrikulierter Studenten sowie unberechtigter Benutzer ist dank des Token Management Systems wesentlich einfacher geworden.“ Nur einen kleinen Wermutstropfen sieht Wolf mit der neuen Lösung: „Der Verwaltungsaufwand beim Beschreiben und Löschen der Mifare-Karten ist tendenziell etwas größer geworden – aber das ist eben der Preis, den die Sicherheitslösung von uns allen abverlangt.“



Kurzporträt digitronic

Die im Jahre 1991 gegründete und in Chemnitz ansässige digitronic computersysteme gmbh entwickelt in enger Kooperation mit der Polizei mehrerer Bundesländer die Softwarelösung WinTelex EP. Dieses universelle Verfahren ermöglicht die Teilnahme an der bundesweiten formellen Kommunikation nach PDV 810.1 und gewährleistet den adressatengerechten, schnellen und sicheren Austausch von Informationen im Behördenumfeld.

Neben dem Softwaregeschäft, welches inzwischen auch innovative Standardlösungen im Bereich Zugriffsschutz und Datensicherheit für Client-PCs umfasst, hat sich digitronic kontinuierlich zu einem leistungsstarken Lösungsanbieter im deutschen Markt etabliert, der umfassende Service- und Beratungsdienstleistungen anbietet. Mit einer professionellen, zuverlässigen und auf den Kundennutzen ausgerichteten Arbeitsweise unterstützt digitronic Kunden in der Konzeptionierung und Implementierung von IT-Lösungen und verantwortet deren Betrieb und Service.

Ansprechpartner:

digitronic computersysteme gmbh

Sabrina Wilhelmi
Oberfrohnauer Str. 62
D-09117 Chemnitz
Tel.: +49 (0) 371 81539-242
Fax: +49 (0) 371 81539-900
E-Mail: sw@digitronic.net
Internet: www.digitronic.net

Agentur Frische Fische

Jan Eppers
Martin-Luther-Platz 9
D-01099 Dresden
Tel.: 0351/56 33 87-0
E-Mail: jep@frische-fische.com
Web: www.frische-fische.com