Mit Sicherheit offen

Zugang zu Dienstleistungen im Erwin Schrödinger-Zentrum

Lutz Stange
stange@cms.hu-berlin.de

Zugang, Sicherheit, Öffentliche Computerarbeitsplätze, Universitätsbibliothek, Computer- und Medienservice, DV-Dienstleistungen,bibliothekarische Dienste

Das Ziel, den Benutzerinnen und Benutzern die Dienstleistungen des Computer- und Medienservice und der Naturwissenschaftlichen Zentralbibliothek so offen und transparent wie möglich anzubieten, stellt auf der anderen Seite erhöhte Anforderungen an die Sicherheit des Zugangs. Dieser Artikel beschreibt einige organisatorische und DV-technische Maßnahmen, die den Spagat zwischen diesen zwei sich in einzelnen Punkten sicherlich widersprechenden Ansprüche versuchen. Die abschließenden Abschnitte informieren über den derzeitigen Stand der Realisierung.

Anliegen

Idealvorstellung ist, dass Dienstleistungen Benutzerinnen und Benutzern möglichst ohne Einschränkungen angeboten werden können. Für die Kunden entfallen weitestgehend verwaltungstechnische Prozeduren, das Dienstleistungsspektrum steht ihnen im vollen Umfang zur Verfügung und der Zugang gestaltet sich selbsterklärend und ohne großen Aufwand. Der Betreiber kann sich auf die Sicherstellung der Qualität der Dienstleistung beschränken und muss nicht einen Teil seiner Kraft in Verwaltungs- und Abrechnungsprozesse stecken. Dem stehen aber leider die Anforderungen entgegen, die an die Sicherheit der Dienste gestellt werden müssen. Was nützt der freie PC-Zugang, wenn zu einem anderen Standort elektronisch nur eingeschränkt kommuniziert werden kann, weil eine verschlüsselte Datenübertragung nicht möglich ist? Wie kann eine dedizierte Vergabe von Berechtigungen (z. B. Benutzung von Softwarelizenzen und von bestimmten Internetdiensten) organisiert werden, deren Autorisierung für einzelne Benutzergruppen unterschiedlich ist? Welchen Sinn hat ein Zugang in Selbstbedienung, wenn der Computer abhanden gekommen oder sonst nicht benutzbar ist?

Es ist das bekannte Dilemma, dass sich die beiden Zielrichtungen Offenheit und Sicherheit in ihren Auswirkungen im Wesentlichen entgegenstehen. Hier gilt es, Kompromisse zu finden, die sowohl für Betreiber als auch für Benutzerinnen und Benutzer akzeptabel sind. Einige diesbezügliche Realisierungen und Verfahrensweisen im Erwin Schrödinger-Zentrum sollen in diesem Artikel vorgestellt werden.

Zugang und Sicherheit

Vorab sind die beiden für diese Thematik zentralen Begriffe »Zugang« und »Sicherheit« zu erläutern:

Zugang ist die Gesamtheit der technischen und organisatorischen Maßnahmen, Methoden und Einrichtungen zur Steuerung und Abrechnung der Benutzung von DV-Diensten des Erwin Schrödinger-Zentrums. Die Zugangskontrolle sichert Datenverarbeitungssysteme gegen unberechtigte Benutzung. Durch Autorisation und Vergabe von Zugriffsrechten werden Möglichkeiten des unberechtigten Zugangs zu DV-Technik weitestgehend eingeschränkt.

Der Begriff »Zugang« wird klar vom Begriff »Zutritt« unterschieden, welcher die Maßnahmen zur Steuerung sicherheitstechnischer Anlagen bezeichnet (Zutritt zu Räumen, Sicherheitsbereichen, Schließfächern usw.). Der Problemkreis »Zutritt« soll an dieser Stelle nicht weiter betrachtet werden.

Die mit dem Stichwort Sicherheit zusammenhängenden Themen sind sehr umfangreich. Schon ein Blick auf das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genügt, sich eine ungefähre Vorstellung von der Komplexität und Vielschichtigkeit dieses Themas zu machen. An dieser Stelle soll sich im Wesentlichen auf die Aspekte IT-Systeme, Netze und IT-Anwendungen beschränkt werden. Gesichtspunkte wie Infrastruktur, Verfügbarkeit oder sonstige übergreifende Themen werden hier nicht berücksichtigt.

Im Erwin Schrödinger-Zentrum stellt sich der Sicherheitsanspruch in einer neuen Qualität dar. Das ist insbesondere in folgenden Besonderheiten begründet:

- Der schon zu Beginn genannte Anspruch an die Offenheit und Flexibilität gegenüber den Benutzerinnen und Benutzern erfordert in gleicher Weise eine Erhöhung des Sicherheitslevels.

- Die verstärkte Dezentralisierung der Dienstanbieter setzt die Möglichkeit einer sicheren elektronischen Kommunikation voraus (Computer- und Medienservice an zwei Hauptstandorten, die Universitätsbibliothek mit der Naturwissenschaftlichen Zentralbibliothek in Adlershof, der Zentrale in Mitte und etwa 20 weiteren Zweig- und Teilbibliotheken an unterschiedlichen Standorten).
- In gleicher Weise steigen die Ansprüche der Benutzerinnen und Benutzer an eine zeit- und ortsunabhängige Benutzung von Diensten.
- Die quantitative Vergrößerung des Dienstleistungsangebots hat keine entsprechende Personalaufstockung zur Folge, so dass sich der Automatisierungsgrad und der Selbstbedienungsanteil wesentlich erhöhen müssen.
- Der potentielle Kundenkreis wird sich durch die am Standort Adlershof angesiedelten Firmen und Einrichtungen gegenüber Mitte vergrößern.
- Die bisherigen Erfahrungen am etwas abseits gelegenen Campusgelände in Adlershof erfordern zwingend ein intensiveres Nachdenken über Sicherheitsaspekte.

Ein Großteil der Dienstleistungen im Erwin Schrödinger-Zentrum wird computerbasiert angeboten. Für die Benutzerinnen und Benutzer stehen dabei etwa 300 öffentliche Computerarbeitsplätze in zentralen und dezentralen Bereichen zur Verfügung. Wie erfolgt nun die Verwaltung der Benutzerinnen und Benutzer und damit verbunden der Zugang zu den Diensten? Über den aktuellen Stand (zum Zeitpunkt der Eröffnung des Gebäudes) und die Zukunftsaussichten geben die folgenden Abschnitte Auskunft.

Zentrale Benutzermanagement

Die Universitätsbibliothek und der Computer- und Medienservice treten gemeinsam als Dienstanbieter auf. In vorangegangenen Artikeln dieses Heftes wurde bereits ausführlich auf Motivation und Gemeinsamkeiten eingegangen. An dieser Stelle soll sich auf den technologischen Aspekt beschränkt werden.

Aus Sicht der Benutzerinnen und Benutzer sollte der Zugang zu Dienstleistungen unabhängig davon, welche Einrichtung denn nun konkret der Anbieter ist, möglich sein. Das bedeutet, dass es eine zentrale Anlaufstelle gibt (Info-Theke oder elektronische Einwahl), an welcher Anmeldung, Support und sonstige Betreuung erfolgen können. So kann man sich für die Benutzung des Lesesaals in gleicher Weise wie für die Benutzung von DV-Diensten einschreiben lassen. Im Ergebnis erhalten sie ein gemeinsames Authentifizierungskennzeichen (zzt. noch zwei) mit einem einzigen Passwort.

Aus der Sicht der Betreiber wird die gesamte DV-Technik vom Computer- und Medienservice betreut. Das Authentifizierungskennzeichen ist ein (für NIS und ADS identisch aussehendes) Benutzerkennzeichen, wobei die Passwörter automatisch synchron gehalten werden. Für die zahlenmäßig größte Benutzergruppe, die Studierenden, ist darüber hinaus die Anmeldung, Verlängerung und/oder Reaktivierung auch in Selbstbedienung über ein entsprechendes Web-Formular möglich.

In dieser ersten Stufe der Realisierung erhalten die Benutzerinnen und Benutzer von Bibliotheksdienstleistungen noch ein separates Benutzerkennzeichen für das Bibliothekssystem Aleph 500. Dieses kann als Anwendung auf dem Computerarbeitsplatz gestartet werden und erfordert eine eigenständige Authentifizierung.

In einem nächsten Schritt wird ein übergreifendes zentrales Benutzermanagement für den Großteil der angebotenen Dienste konzipiert und eingeführt. Dieses basiert auf dem LDAP-Verzeichnisdienst. Insbesondere werden folgende Systemdienste integriert: Active Directory Service (ADS) von Microsoft, Benutzerverwaltung von Aleph 500, RADIUS und ggf. die Kerberos-Authentifizierung. Dieser LDAP-Verzeichnisdienst ist damit zentraler Verwaltungsdienst für Benutzer von DV- und Bibliotheksdiensten.

Public Key Infrastructure

Mit der Zentralisierung des Benutzermanagements wird einem wesentlichen Ziel beim Betrieb des Erwin Schrödinger-Zentrums näher gekommen: der Vereinfachung technologischer Prozesse. Die Public Key Infrastructure (PKI) charakterisiert nun die Basistechnologie, die die Vorteile der umfassenden Nutzung der Kommunikationsinfrastruktur mit der Wahrung der Sicherheitsinteressen verbindet.

In dem Artikel »Public Key Infrastructure – ein Blick in die nahe Zukunft« wird genauer auf den theoretische Hintergrund sowie unsere Anforderungen an eine Realisierung eingegangen.

Der Aufbau der PKI-Technologie am Erwin Schrödinger-Zentrum erfolgt unter den Bedingungen, dass sie die Grundlage für weitere PKI-Anwendungen der Universität bildet und nahtlos erweitert werden kann. Die durch die PKI erzeugten elektronischen Signaturen entsprechen in ihrer Rechtswirksamkeit der Stufe der fortgeschrittenen Signatur. Die Smartcard ist eine »reine« Zertifikats- und Signaturkarte und wird multifunktional genutzt. Die einzelnen PKI-Anwendungen werden modular aufgebaut und schrittweise auf Smartcard-Nutzung umgestellt.

Erste PKI-Anwendung

Unter der Voraussetzung des Betriebes einer PKI mit einem zentralen Benutzermanagement wird als erste Anwendung der Zugang zu öffentlichen Computerarbeitsplätzen realisiert. Hiermit steht der Zugang zu DV-Dienstleistungen auf der Basis der digitalen Signatur in engem Zusammenhang.

Die technische Grundlage für den Zugang zu Computerarbeitsplätzen sind MS Windows 2000 (Terminal) Server, Windows-PCs, Linux-PCs und Thin-Clients. Für diese Plattformen ist die Funktionalität grundsätzlich verifiziert, die entsprechenden Geräte sind einsetzbar. Ein besonderes Problem stellte dabei die Einbindung von ThinClients dar, für die auf der Basis von Citrix MetaFrame FR2 die PKI-basierte Authentifizierung technisch gelöst wurde.

Der nächste Schritt ist die Einbindung des Zugangs zu den Anwendungen. Mit der Zentralisierung der Benutzerverwaltung (Applikationen können die Authentifizierungsinformationen direkt aus dem Verwaltungs-Verzeichnis lesen) und mit der Möglichkeit der SSL-Verschlüsselung der Passwörter für die Übertragung vom Verwaltungsverzeichnis zur Applikation sind wesentliche Voraussetzungen für einen Single Sign On-Betrieb geschaffen. In diesem Fall ist ein einmaliges Anmelden zu unterschiedlichen Diensten bei einem System-Entry-Service möglich.

Das Procedere der Anmeldung

Die vorangegangenen Abschnitte haben die thematische Einbindung der Benutzerverwaltung in das Gesamtkonzept deutlich gemacht, von denen viele Punkte aber noch Zukunftsmusik sind. Hier soll nun der konkrete Verfahrensweg für die Anmeldung und Benutzung beschrieben werden, wie er sich in der jetzigen Reali-

sierungsform für Kunden des Erwin Schrödinger-Zentrums darstellt.

Es sei mit der Gruppe der an der Humboldt-Universität Studierenden begonnen. Vergleichbar zur Verfahrensweise in der Vergangenheit, jetzt aber mit erweitertem Funktionsumfang, ist ein Großteil der Verwaltungsprozesse Web-basiert unabhängig vom Standort durchführbar. Unter Angabe von Informationen, die eindeutig die Benutzerin bzw. den Benutzer identifizieren, kann die Anmeldung online vollzogen werden. Im Ergebnis werden ein ADS-Benutzerkennzeichen (sofort verfügbar), ein NIS-Benutzerkennzeichen (innerhalb des folgenden Arbeitstages verfügbar) und eine Mail-Adresse bereitgestellt. Bei einem persönlichen Erscheinen an der Info-Theke des Erwin Schrödinger-Zentrums kann sich gleichzeitig an der Universitätsbibliothek angemeldet werden.

Für Mitarbeiter/innen der HU ist die Verfahrensweise vergleichbar, nur dass wegen fehlender eindeutiger Identifikations-Kennzeichen die online-Anmeldung nicht möglich ist. Ein ausgefülltes Antragsformular ist der Benutzerberatung per Hauspost zuzusenden, zwei Tage nach Eingang der Unterlagen stehen die Dienste zur Verfügung. Natürlich ist auch hier die persönliche Anmeldung möglich, in diesem Fall ist das volle Dienstleistungsspektrum von Computer- und Medienservice und Universitätsbibliothek mit Ausnahme von Unix-basierten Diensten und Mail sofort nutzbar.

Die dritte große Gruppe ist die der »HU-Fremden«, also Benutzerinnen und Benutzer von Dienstleistungen des Erwin Schrödinger-Zentrums, die nicht Mitglieder der Humboldt-Universität sind. Zu diesen gehören externe Mitarbeiter/innen, kooperierende Partner, Studierende anderer Hochschulen, Gäste und sonstige Externe. Den Mitgliedern dieser Gruppe ist gemeinsam, dass eine Anmeldung nur persönlich an der Info-Theke vorgenommen werden kann. Grundsätzlich erhalten sie keinen NIS-Account und keine Mail-Adresse. Außerdem gibt es gesonderte Festlegungen zur Gültigkeit der Benutzungsberechtigung.

Zugang zu öffentlichen Computerarbeitsplätzen

Der Zugang zu Dienstleistungen des Erwin Schrödinger-Zentrums erfolgt im Allgemeinen auf der Basis des Zugangs zu öffentlichen Computerarbeitsplätzen. Dieser ist ausschließlich auf der Grundlage einer Anmeldung im ADS möglich, d. h. eine anonyme Benutzung ist bis auf Möglichkeiten der Recherche im Intranet ausgeschlossen. Für weiterführende Dienste ist eine Authentifizierung erforderlich. Zu diesen gehören:

- Benutzung von Standard- und weiterer Windows-Anwendungssoftware
- Benutzung von Peripherie-Geräten (Drucker, Scanner, Brenner usw.)
- Benutzung von Internet- und Intranet-Diensten der Humboldt-Universität (Kommunikationsdienste, Verbindungen zu Unix-Rechnern, Speicherplatz in Home-Verzeichnissen, Erstellung eigener Web-Seiten usw.)
- Anforderung von Dienstleistungen der Universitätsbibliothek
- Benutzung von Internet-Diensten anderer Einrichtungen (z. B. Mail-Boxen anderer Einrichtungen)

Öffentliche Computerarbeitsplätze sind fast ausschließlich ThinClients, die an einem Microsoft Terminal Server mit Citrix MetaFrame angeschlossen sind. Diese sind über den gesamten Parterre-Bereich des Erwin Schrödinger-Zentrums verteilt und benutzbar. Zu den beiden Schulungsräumen ist der Zugang leicht modifiziert: Im Workstation-Pool wird natürlich nur ein NIS-Account zur Anmeldung benötigt. Die PCs im entsprechenden Schulungsraum sind standardmäßig auch als Clients am Terminal-Server angeschlossen, ein Zugriff auf lokale Installationen ist aber möglich. In beiden Fällen ist natürlich eine Windows-Anmeldung Voraussetzung.

Ausblick

Wie in den ersten Abschnitten angedeutet, stellt die derzeitige Ausbaustufe nur einen Zwischenstand dar und kann den Anforderungen an die Sicherheit noch nicht genügen. Auch wenn die Realisierung eines zertifikatsbasierten Zugangs zu DV-Technik und damit zu den Diensten erst einmal einen finanziellen, personellen und technologischen Kraftakt erfordert, führt daran kein Weg vorbei. Der Gedanke ist natürlich attraktiv: Die Anmeldung im Erwin Schrödinger-Zentrum bewirkt die Bereitstellung einer SmartCard, mit der der Benutzerin bzw. dem Benutzer in Form eines Single Sign On der Zugang zu unterschiedlichen Systemen ermöglicht wird und mit der die Sicherheitsfeatures des zertifikatsbasierten Zugangs sowie die Möglichkeiten der digitalen Signatur zur Verfügung stehen. Der jetzt realisierte Stand bildet eine gute Grundlage dafür.

Literatur

[1] Stange, L.: »Zugang und Zutritt zum IKA« in *RZ-Mitteilungen* Nr. 22/November 2001

[2] »IT-Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik«, unter http://www.bsi.de/gshb/deutsch/menue.htm

[3] Schwan, M.: »Verschlüsseln und Signieren von E-Mails – eine einfache Anwendung?« in *RZ-Mitteilungen* Nr. 23/Mai 2002

[4] Olzog, F.: »Einrichtung eines Benutzerkennzeichens für Studierende«, unter https://www.hu-berlin.de/rz/antrag/