Editorial

Dr. Marcus Pattloch (DFN-Verein)

Keine Verwaltung kann ihre vielfältigen Aufgaben heutzutage ohne eine leistungsfähige IT-Infrastruktur erbringen. Im Gegenteil: Neue Anforderungen auf der einen Seite und die Forderung nach immer größerer Effizienz sind Gründe für den Einzug neuer Informationstechnologien in die Verwaltung. Das Spektrum der neuen Ansätze ist breit: Es reicht von modernen Web-Anwendungen über die Nutzung von Portalen bis zu neuen Möglichkeiten der Datensicherung. Ganz wichtig ist dabei die Integration aller Verfahren in ein umfassendes Konzept. Dies ist nicht nur für einen stabilen Betrieb erforderlich, sondern auch die Grundlage für zukünftige Erweiterungen.

Ein Thema, das sich durch fast alle dieser neuen Technologien wie ein roter Faden zieht, ist IT-Sicherheit. Nicht zuletzt durch medienwirksame Veröffentlichungen über Hacker und Würmer ist eine sichere IT-Infrastruktur ein allgemein anerkanntes Ziel. Um dieses zu erreichen, werden große Anstrengungen unternommen, und es wird in teure Hard- und Software investiert. Trotzdem verzögert sich die Realisierung oft um Monate oder Jahre, manchmal scheitert sie sogar vollständig. Die Gründe dafür liegen auf der Hand: Es werden elementare organisatorische Fehler gemacht, so dass zwar »die Technik läuft«, aber die Integration der neuen Maßnahmen in die Gesamtprozesse der Hochschule fehlt.

Dass es auch anders geht, zeigt das positive Beispiel der Humboldt-Universität zu Berlin. Dort wird seit Jahren durch die Abteilung »DV in der Verwaltung« im Computer- und Medienservice ein IT-Sicherheitskonzept erfolgreich umgesetzt. Durch Berücksichtigung organisatorischer und betrieblicher Aspekte (neben der erforderlichen Technik) wurden praxistaugliche Ergebnisse erzielt, die aus dem Tagesbetrieb nicht mehr wegzudenken sind und zum Teil neue Dienstleistungen erst ermöglicht haben. Dabei orientiert man sich an drei wesentlichen Aspekten: dem frühzeitigen Einbinden aller relevanten Entscheidungsträger, der intensiven Unterstützung der Nutzer sowie der organisatorischen Integration aller Maßnahmen, bei der anstelle der Technik die langfristige Nutzung im Vordergrund steht.

Wie oft hört man von groß angelegten technischen Planungen, die letztendlich an begründeten Einsprüchen von Personalräten oder Datenschützern scheitern. Gerade der Hang vieler Techniker, grundsätzlich möglichst viele personenbezogene Daten zu sammeln und zu speichern – auch wenn es dafür weder eine technische noch rechtliche Notwendigkeit gibt – führt zu diesen Problemen. An der Humboldt-Universität wurde deswegen frühzeitig eine Steuerungsgruppe »Verwaltungsnetz« ins Leben gerufen, die sich neben technischen Experten aus Personalverantwortlichen und aus Datenschützern zusammensetzt. Durch diese Gruppe wird sichergestellt, dass einmal verabschiedete Planungen auch zügig umgesetzt werden können.

Was für einen Techniker trivial ist, stellt sich für Nutzer oft als Buch mit sieben Siegeln dar. Diese Grenzen zu überwinden und gegenseitiges Vertrauen zu schaffen, ist eine wichtige Basis für die erfolgreiche Einführung von IT-Sicherheit. Wesentliches Ziel muss es sein, frühzeitig auf die Nutzer zuzugehen und ihnen die geplanten Maßnahmen zu erläutern. Bei aller Transparenz der neuen Lösungen werden sich gewisse Änderungen in den etablierten Abläufen nicht vermeiden lassen, aber durch Aufzeigen der Vorteile der neuen Lösungen im Gespräch mit den Nutzern – und nicht über deren Köpfe hinweg – ist das zu schaffen. Diese kommunikative Zusammenarbeit mit »Laien« ist zwar für viele Experten eine schwierige Übung, aber der Aufwand lohnt sich.

Der alte Spruch »erst denken – dann handeln« hat auch im Sicherheitsbereich seine Bedeutung und lässt sich abwandeln in »erst das Konzept – dann die Technik«. Leider wird jedoch immer noch bei vielen IT-Projekten die Technik in den Vordergrund gestellt. Als vor einigen Jahren Firewalls als wichtige Komponente der Sicherheit erkannt wurden, kauften viele Einrichtungen zunächst entsprechende Hardware und Software, aber erst hinterher wurde die Frage gestellt, was denn eigentlich genau abgesichert werden soll. Das Scheitern dieses Vorgehens war vorprogrammiert. Technik darf kein Selbstzweck sein. Sie ist zwar eine wichtige Komponente, aber eben nur ein Teil, der ohne die begleitenden organisatorischen und betrieblichen Maßnahmen nicht zum Erfolg führen kann.

In der Universitätsverwaltung der Humboldt-Universität werden diese »goldenen Regeln« seit langer Zeit umgesetzt. Erste Schritte wurden vor etwa 10 Jahren gemeinsam mit dem DFN-Verein im Rahmen von Forschungsprojekten realisiert. Als Betreuer dieser Projekte war es immer sehr angenehm, mit den sehr motivierten Mitarbeitern zusammenzuarbeiten. Viele, die als studentische Mitarbeiter begonnen haben, sind heute unverzichtbare Mitarbeiter im täglichen Betrieb. Und viele Konzepte, die auf einem Stück Papier begonnen haben, bilden heute – nach intensiver Diskussion mit Steuerungsgruppe und Nutzern – das sicherheitstechnische Rückgrat der IT-Infrastruktur in der Hochschulverwaltung.

Ich bin mir sicher, dass alle Beteiligten die erfolgreichen Arbeiten auch in Zukunft fortsetzen werden und dabei neue Aufgaben lösen, wie sie sich z. B. durch dezentrale Verwaltungsstrukturen oder die neuen Bachelor-Abschlüsse ergeben. Wohl dem, der eine so gute Basis hat wie die Humboldt-Universität zu Berlin.