Otto-Friedrich-Universität Bamberg

IT-Sicherheitsstrategie der Otto-Friedrich-Universität Bamberg

Beschluss der Universitätsleitung der Otto-Friedrich-Universität Bamberg vom 17.12.2014

Präambel

Der Betrieb einer Universität hängt in hohem Maße von der Qualität ihrer Informationstechnologie (IT)-Infrastruktur und -Dienste ab.

Mit zunehmender Wichtigkeit der IT und angesichts gleichzeitig wachsender Bedrohungen gewinnt die IT-Sicherheit immer größere Bedeutung. Beeinträchtigungen der IT-Sicherheit können erhebliche Auswirkungen auf die Lehre, Forschung und Verwaltung haben und damit hohe materielle und immaterielle Schäden verursachen.

Ein angemessenes IT-Sicherheitsniveau kann nur im Rahmen eines stetigen IT-Sicherheitsprozesses erreicht und aufrechterhalten werden. Mit der vorliegenden IT-Sicherheitsstrategie legt die Universität den organisatorischen Rahmen dafür fest. Die konkreten Regelungen sowie die zu ergreifenden und umzusetzenden Maßnahmen werden in einem IT-Sicherheitskonzept und in operativen Maßnahmenkatalogen der jeweiligen Systembetreiber festgelegt.

1. Geltungsbereich

Die vorliegende IT-Sicherheitsstrategie gilt dem sicheren Betrieb aller an der Universität Bamberg eingesetzten IT-Systeme und –Verfahren und legt die IT-Sicherheitsziele, das IT-Sicherheitsniveau, die Verantwortlichkeiten in der IT-Sicherheitsorganisation und die wesentlichen Parameter der IT-Sicherheitsprozesse fest.

2. IT-Sicherheitsziele

Rechnersysteme, IT-Dienstleistungen und das hochschulinterne Rechnernetz sind zur Unterstützung der universitären Aufgaben in den Bereichen Lernen, Lehre, Forschung und Administration bestimmt. Alle Anwenderinnen und Anwender sind für einen bestimmungsgemäßen Umgang mit dieser IT-Infrastruktur verantwortlich. Gerade wegen der zunehmenden Abhängigkeit von den IT-Systemen verfolgt die IT-Sicherheitsstrategie folgende Ziele:

- Gewährleistung der Verfügbarkeit, Vertraulichkeit und Unversehrtheit von IT-Systemen und Daten,
- Schutz von Datennetzen, Rechnersystemen und Informationen (Hardware, Software und Daten) gegen Missbrauch von innen und außen,
- Gewährleistung der gesetzlichen Vorgaben, insbesondere des Datenschutzes,
- Sicherstellung eines reibungslosen Lehr-, Forschungs- und Verwaltungsbetriebes,
- Erhalt des guten Rufes der Universität in der Öffentlichkeit sowie
- ausgewogenes Verhältnis zwischen potentiell einschränkenden Sicherheitsmaßnahmen sowie einfacher Nutzbarkeit der IT-Systeme.

3. IT-Sicherheitsniveau

Das Mindestsicherheitsniveau für alle IT-Systeme der Universität orientiert sich am IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Es bezieht sich auf Systeme mit normalem Schutzbedarf. Ein System hat einen normalen Schutzbedarf, wenn durch den Verlust an Vertraulichkeit, Verfügbarkeit oder Unversehrtheit des Systems

- nur ein geringfügiger Verstoß gegen Vorschriften und Gesetze möglich ist,
- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des bzw. der Einzelnen nicht möglich ist oder für diesen bzw. diese tolerabel bleibt,
- eine Beeinträchtigung der persönlichen Unversehrtheit des bzw. der Einzelnen nicht möglich ist,
- die Aufgabenerfüllung nur geringfügig beeinträchtigt ist,
- nur eine geringe Ansehens- und Vertrauensbeeinträchtigung zu befürchten ist und
- der finanzielle Schaden tolerabel bleibt.

Für Systeme mit hohem oder sehr hohem Schutzbedarf müssen ergänzende Maßnahmen auf Basis einer differenzierten Sicherheitsanalyse unter Beteiligung des IT-Sicherheitsteams ergriffen werden.

4. IT-Sicherheitsorganisation

IT-Sicherheit lässt sich nur als Gesamtkonzept realisieren. Alle Beteiligten, einschließlich der Endnutzerinnen und Endnutzer, müssen sich der Notwendigkeit von IT-Sicherheit bewusst sein und entsprechend handeln. Demgemäß muss auf unterschiedlichen Organisationsebenen eine entsprechende Verantwortung übernommen werden. Dazu zählen:

4.1. Verantwortung der Universitätsleitung

Die Universitätsleitung trägt die Gesamtverantwortung für die IT-Sicherheit an der Universität Bamberg. Das die Universitätsleitung unterstützende Chief Information Office (CIO) ist unmittelbar für Fragen der IT-Sicherheit zuständig.

4.2. Verantwortung des IT-Sicherheitsteams

Zur Förderung der IT-Sicherheit sowie zur Steuerung und Koordination von IT-Sicherheitsprozessen ist ein IT-Sicherheitsteam eingerichtet. Das IT-Sicherheitsteam setzt sich zusammen aus der Leiterin oder dem Leiter des Rechenzentrums, der Leiterin oder dem Leiter des Dezernats Z/IS, der oder dem Datenschutzbeauftragten der Universität und der oder dem Vorsitzenden des IuK-Beirats.

Das IT-Sicherheitsteam wird bei allen Fragen zur Sicherheit der IT-Infrastruktur beteiligt. Es ist dem Chief Information Office (CIO) unterstellt und berichtet diesem zweimal jährlich.

Bei der permanent erforderlichen Beobachtung der einschlägigen Informationsquellen zu IT-Sicherheit, der praktischen Umsetzung von IT-Sicherheitsmaßnahmen und der Behandlung von IT-Sicherheitsvorfällen wird das IT-Sicherheitsteam vom Rechenzentrum operativ unterstützt. Die dafür erforderlichen zusätzlichen Ressourcen werden bereitgestellt.

4.3. Verantwortung des Leiters bzw. der Leiterin einer Organisationseinheit

Für dezentral betriebene Subsysteme, Arbeitsstationen und Server trägt der Leiter bzw. die Leiterin der entsprechenden Organisationseinheit die Verantwortung. Er bzw. sie ist verpflichtet, sich über geltende Sicherheitsvorgaben zu informieren und für die operative Umsetzung der Sicherheitsstrategie in seinem bzw. ihrem Verantwortungsbereich zu sorgen.

4.4. Verantwortung aller Endnutzerinnen und Endnutzer

Jede Endnutzerin bzw. jeder Endnutzer trägt die Verantwortung für den bestimmungsgemäßen und gewissenhaften Umgang mit den Informationen, die von ihm bzw. ihr genutzt und verarbeitet werden. Er bzw. sie ist verpflichtet, sich über mögliche Sicherheitsrisiken zu informieren und grundlegende Sicherheitsmaßnahmen für seinen bzw. ihren Arbeitsbereich umzusetzen.

Bei Verdacht auf Manipulationen oder missbräuchliche Veränderungen am eigenen Computer ist unverzüglich das Rechenzentrum zu informieren.

5. IT-Sicherheitsprozesse

IT-Sicherheit ist kein Zustand sondern Ergebnis eines stetigen Prozesses. Zum einen werden ständig neue IT-Verfahren eingeführt oder bestehende weiterentwickelt. Zum anderen ändern und vermehren sich die Bedrohungen. Gleichzeitig ist absolute IT-Sicherheit nicht möglich. Der Aufwand für Sicherheitsmaßnahmen und die gegebenenfalls bedingte Erschwernis der Benutzung müssen in ausgewogenem Verhältnis zum potentiellen Schaden stehen. Die Sicherheitsmaßnahmen müssen außerdem Dienste übergreifend betrachtet ausgewogen sein.

5.1. IT-Sicherheitsteam

Das IT-Sicherheitsteam ist daher bei der Einführung neuer IT-Verfahren oder bei grundlegenden Änderungen bestehender IT-Verfahren immer zu beteiligen. Bei neuen Erkenntnissen zur Bedrohungslage gibt es den IT-Verantwortlichen entsprechende Anpassungen der IT-Verfahren vor.

Das IT-Sicherheitsteam berichtet dem CIO zweimal jährlich und zieht dieses bei strategischen IT-Sicherheitsfragen im Zusammenhang mit der Einführung oder dem Betrieb eines IT-Verfahrens hinzu. Datenschutzrechtliche Fragen werden im Rahmen des IT-Sicherheitsprozesses durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten als Mitglied des IT-Sicherheitsteams immer parallel berücksichtigt. Bei mitbestimmungspflichtigen Themen wird der Personalrat hinzugezogen. Die Interessen der Nutzerinnen und Nutzer werden durch die Vertreterin oder den Vertreter des IuK-Beirats im IT-Sicherheitsteam eingebracht.

5.2. Akute Gefahrenabwehr

Zur Abwehr akuter schwerwiegender Störungen und Gefahren, die die IT-Sicherheit gefährden, kann das Rechenzentrum temporär

- Anwender bzw. Anwenderinnen von der Nutzung der IT-Systeme, dem Netzwerk und den IT-Dienstleistungen ausschließen,
- die Verbindung zu Endgeräten oder Subnetzen unterbrechen.

Die Maßnahmen sind auf den Zeitraum beschränkt, in dem die Störung oder Gefahr vorliegt bzw. der für die Abstellung der Ursache erforderlich ist. Die betroffenen Endanwenderinnen oder Endanwender werden umgehend benachrichtigt.

Bei gravierenden Sicherheitsvorfällen sind zudem stets das IT-Sicherheitsteam und das CIO zu informieren.

Bei schwerwiegenden sicherheitsrelevanten Störungen ist die Präsidentin oder der Präsident der Universität Bamberg berechtigt, die verursachenden Anwenderinnen bzw. Anwender zeitweise oder auf Dauer von der Nutzung der IT-Systeme, des Netzwerkes oder der IT-Dienstleistungen auszuschließen.