



# Positionspapier des BSI zur Förderung der IT-Sicherheit an Hochschulen

Stand: 08.11.2004



## Förderung der IT-Sicherheit an Hochschulen

Hochschulen stehen auf dem Gebiet der IT-Sicherheit vor den gleichen Herausforderungen wie Unternehmen und Behörden. Forschung und Lehre sind in hohem Maß vom sicheren Betrieb der Informations- und Kommunikationstechnik abhängig. Um auf veränderte Rahmenbedingungen und neue Anforderungen zu reagieren, ist mehr und mehr in allen Bereichen der Universität unternehmerisches Denken gefragt.

### 1. Gefährdungslage

Universitäten haben viele Gründe, Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationen sicher zu stellen. Die Bedrohungslage einer Hochschule kann dabei aufgrund der Vielzahl von Gefährdungen kritischer als die der meisten Unternehmen sein:

- ▶ In vielen Bereichen werden vertrauliche oder personenbezogene Daten wie Prüfungsergebnisse, Daten von Testpersonen oder medizinische Daten verarbeitet. Diese Daten müssen besonders geschützt werden, um **unbefugte Kenntnisnahme** oder **Manipulationen** zu verhindern. Denn wenn Prüfungen von Kandidaten vorab eingesehen oder Ergebnisse und Noten nachträglich verändert werden können, verstößt dies massiv gegen die Prüfungsordnung. Und auch wenn Unbefugte die Daten einsehen können, kann den Betroffenen schwerer Schaden zugefügt werden. Hat die Hochschule die vertraulichen Daten nur unzureichend geschützt, kann dies einen Verstoß gegen Datenschutzgesetze bedeuten. Von der Integrität medizinischer Daten kann unter Umständen sogar das Leben von Patienten abhängen.
- ▶ Viele Forschungsdaten sind das Ergebnis jahrelanger Arbeit und repräsentieren große finanzielle und persönliche Investitionen. **Datenverluste** können daher immense Schäden verursachen. Datenverluste werden nicht immer vorsätzlich herbeigeführt. Auch gegen menschliches oder technisches Versagen sowie gegen die Auswirkungen von Elementarschäden (wie Feuer oder Wasser) müssen Vorkehrungen getroffen werden.
- ▶ Aufgrund hervorragender Forschungsergebnisse und Erfolg versprechender Patente können auch Universitäten Opfer von **Industriespionage** werden.
- ▶ Ein angemessenes IT-Sicherheitsniveau an Universitäten ist unabdingbar, um als Kooperationspartner für die Wirtschaft attraktiv zu sein. Die Entwicklung von Hochtechnologien oder neuen medizinischen Verfahren geschieht vielfach in enger Zusammenarbeit zwischen Universitäten und Wirtschaftsunternehmen. Und die wichtigste Voraussetzung für eine erfolgreiche Kooperation ist **Vertrauen**.

- ▶ Universitäten gewähren sehr unterschiedlichen Personengruppen **Zugang** zu ihren Netzen und Forschungseinrichtungen – ohne dass eine strenge Kontrolle wie in Unternehmen oder Behörden möglich ist. Viele Hochschulrechner sind in der Vergangenheit durch Viren attackiert worden. Sie wurden zum Senden von Spam-Mails, zur Durchführung von Denial-of-Service-Angriffen oder zur Verbreitung von Raubkopien oder Dateien mit kriminellen Inhalten missbraucht.
- ▶ Die **Verfügbarkeit** der IT-Systeme ist in Universitäten sehr häufig unabdingbar: Der Lehr- und Forschungsbetrieb sowie die Verwaltung können merklich behindert werden, wenn IT-Systeme durch Sicherheitsvorfälle nicht wie gewünscht zur Verfügung stehen.
- ▶ An einer typischen Universität sind die gewachsenen Strukturen und technischen Anforderungen vielfältiger als in den meisten Wirtschaftsunternehmen. Dadurch ist die Systemlandschaft sehr heterogen. In der Regel sind auch die Verantwortlichkeiten verteilt und werden nicht zentral gesteuert. **Heterogene Systemlandschaften** sind aber sehr viel schwerer abzusichern und daher größeren Gefahren ausgesetzt als weitgehend standardisierte Umgebungen.
- ▶ Gerade Hochschulen werden häufig **Ziel von Sabotageakten oder gezielten Angriffen**. Die Motive für einen Angriff sind dabei höchst unterschiedlich: Immer wieder kommt es zu Racheakten von Studierenden oder Doktoranden, die mit ihren Prüfungsergebnissen nicht zufrieden sind. Zum anderen schmeichelt es jedem Hacker, wenn er die Sicherheitsvorkehrungen einer Universität überlisten kann. Aufgrund vielfältiger Forschungsaktivitäten besteht für Universitäten aber auch ein höheres Risiko als für die meisten Unternehmen, zur Zielscheibe ideologischer oder politischer Extremisten zu werden.

## 2. Rahmenbedingungen

Die organisatorischen Randbedingungen an Universitäten sind bei der Umsetzung von IT-Sicherheit außerordentlich schwierig. Sie sind zudem nicht immer mit denen von Unternehmen vergleichbar.

Unternehmen	Universität
In Unternehmen gibt es in der Regel klare Hierarchien und geregelte Verantwortungsbereiche. Unternehmen und Mitarbeiter regeln ihre Zusammenarbeit durch Arbeitsverträge und Arbeitsanweisungen, die Rechte und Pflichten benennen (inklusive Kontrollen und Maßnahmen bei Regelverletzungen). Für IT-Sicherheit können zentral Ressourcen zur Verfügung gestellt und Maßnahmen angeordnet werden. Auch die Fachkompetenz für Informationstechnik und Sicherheit kann zentral für alle Bereiche einer Institution bereit gestellt werden.	Führungsstrukturen und soziale Beziehungen an Hochschulen sind wesentlich vielschichtiger und facettenreicher als in den meisten Unternehmen. Institute, Lehrstühle, Wissenschaftler und Studenten sind darauf angewiesen, weitgehend unabhängig und eigenständig zu arbeiten. Alle Regelungen müssen so gestaltet werden, dass die Freiheit von Forschung und Lehre möglichst wenig beeinträchtigt wird. Auch die Bedürfnisse an Informationstechnik und technischer Unterstützung sind äußerst vielfältig.

**Konsequenz:** Die in der Wirtschaft etablierten Methoden zum IT-Sicherheitsmanagement können zwar wertvolle Hilfe leisten, werden aber den Anforderungen von Hochschulen nicht immer gerecht. Sie können daher nicht ohne kreative Anpassungen übernommen werden. Zudem ist die zentrale Administration der Informationstechnik nicht ohne weiteres möglich. Die Verteilung von Zuständigkeiten muss umso mehr intelligent geregelt werden.

### 3. Empfehlungen zur Förderung der IT-Sicherheit

Aufgrund ihrer großen Bedeutung für die Gesellschaft und den Wirtschaftsstandort Deutschland sind Hochschulen auf ein hohes IT-Sicherheitsniveau angewiesen. Arbeits- und Geschäftsprozesse basieren dabei immer stärker auf IT-Lösungen. Die Abhängigkeit von diesen Prozessen führt zu einer wachsenden Verwundbarkeit und der Gefahr massiver wirtschaftlicher Schäden infolge von IT-Risiken. Die Rolle der Hochschulrechenzentren (HRZ) als zentrale IT-Dienstleister erfordert zwangsläufig eine enge Einbindung der Rechenzentren in das hochschulweite IT-Sicherheitsmanagement.

Das BSI unterstützt daher den *Arbeitskreis der Leiter von Rechenzentren an wissenschaftlichen Hochschulen des Landes NRW* (ARNW) bei der Optimierung des IT-Sicherheitsmanagements an Hochschulen. Das BSI und der ARNW haben dazu unter Mitwirkung der Netzentur NRW als ersten Schritt fünf wichtige Eckpunkte identifiziert und Umsetzungsempfehlungen ausgearbeitet:

#### ■ Eckpunkt 1

##### **Regelung der Verantwortlichkeiten**

*Die Verantwortung für IT-Sicherheit muss an jeder Hochschule eindeutig geregelt werden. Die Gesamtverantwortung trägt die Hochschulleitung. In den einzelnen Organisationseinheiten sind die jeweiligen Leiter für die IT-Sicherheit ihrer Systeme verantwortlich.*

- ▶ Jede Hochschule sollte eine "IT-Sicherheitsleitlinie" verfassen, in der die Bedeutung der Informationstechnik, die angestrebten Schutzziele und die wichtigsten übergeordneten IT-Sicherheitsmaßnahmen dargestellt werden. Die Sicherheitsleitlinie wird von der Leitung verabschiedet und allen Mitarbeitern und Studenten, die die Informationstechnik nutzen, bekannt gegeben. Sie ist verbindlich zu beachten.

## ■ Eckpunkt 2

### **Identifikation der Geschäftsprozesse**

*Für jede IT-Sicherheitsstrategie ist es essentiell erforderlich, dass die Hochschule die Sicherheitsanforderungen ihrer Geschäftsprozesse identifiziert*

- ▶ In einer Risikobetrachtung sollten unter Einbeziehung der für die Geschäftsprozesse Verantwortlichen Gefährdungen identifiziert und mögliche Schadensauswirkungen abgeschätzt werden. Darin fließen gesetzliche Anforderungen - beispielsweise aus dem Datenschutz und aus vertraglichen Regelungen - ebenso ein wie bisherige Prinzipien und Verfahrensweisen der IT-Organisation, die zur Unterstützung von IT-Prozessen etabliert sind und fortgeschrieben werden können.

## ■ Eckpunkt 3

### **Bereitstellung von Ressourcen**

*Ein erfolgreiches IT-Sicherheitsmanagement und die konsequente Umsetzung von IT-Sicherheitsmaßnahmen kann nur von qualifizierten Experten mit großer Erfahrung sichergestellt werden. Auch aus Kostengründen ist die Bündelung von Kompetenzen und Ressourcen dringend notwendig.*

- ▶ Die Hochschulrechenzentren besitzen bereits umfangreiches Know-how zur IT-Sicherheit. Ihre Kompetenz sollte unbedingt genutzt und ihre Stellung als zentrale IT-Sicherheitsdienstleister der Hochschulen gestärkt werden.
- ▶ Es reicht aber nicht aus, das Wissen um IT-Sicherheit nur in den Rechenzentren zu konzentrieren. Jede Organisationseinheit, die IT-Systeme betreibt, sollte so schnell wie möglich ihre Mitarbeiter weiterbilden und konsequent IT-Sicherheit in ihre Geschäftsprozesse integrieren.

## ■ Eckpunkt 4

### **Hohes IT-Sicherheitsniveau**

*Das von den Hochschulrechenzentren betreute Netz muss ein hohes IT-Sicherheitsniveau gewährleisten.*

- ▶ Netze sollten so geplant werden, dass Bereiche mit unterschiedlichem Schutzbedürfnis klar voneinander getrennt werden können.
- ▶ Die Hochschulrechenzentren als Netzbetreiber sollten ein IT-Sicherheitskonzept erstellen, das sich an gängigen Methoden und Standards der IT-Sicherheit (wie zum Beispiel dem IT-Grundschutzhandbuch des BSI) orientiert.
- ▶ Wenn neben dem Hochschulrechenzentrum noch dezentrale Servicezentren Teile des Netzes betreuen, müssen die Servicezentren den gleichen Qualitätsanforderungen wie das Hochschulrechenzentrum genügen. Die Zusammenarbeit zwischen Hochschulrechenzentren und dezentralen Servicezentren muss klar geregelt sein.

## ■ Eckpunkt 5

### **Eindeutige Regelungen**

*Die Beziehung zwischen Dienstleistungsanbieter (z. B. HRZ) und den Nutzern (Verwaltung, Institute, Mitarbeiter, Studenten) muss klar geregelt werden.*

- ▶ Die Hochschulrechenzentren sollten einen definierten Katalog von Dienstleistungen erstellen.
- ▶ Alle Nutzer, die Zugang zu geschützten Bereichen des Netzes wünschen, müssen die Sicherheitsvorgaben des Netzbetreibers kennen, akzeptieren und umsetzen. Die Hochschulrechenzentren müssen jederzeit die vollständige Kontrolle über ihr Netz haben. Das schließt die Möglichkeit ein, potentiell unsichere oder verbotene Aktivitäten zu unterbinden.
- ▶ Die Hochschulrechenzentren unterstützen ihre Kunden nach Kräften. Dazu gehören eine umfangreiche Sensibilisierung aller Nutzer in IT-Sicherheitsthemen und die Beratung von Organisationseinheiten bei der Planung von IT-Projekten, um IT-Sicherheitsaspekte möglichst frühzeitig zu berücksichtigen. Umgekehrt unterstützt die Anwenderseite ihre IT-Dienstleister. Dazu gehören zum Beispiel die Regelung von Verantwortlichkeiten und die Bestellung von technisch Verantwortlichen und Administratoren.

#### **4. Fazit: Ein zentrales IT-Sicherheitsmanagement**

IT-Sicherheit zum Nulltarif gibt es nicht. Einige IT-Anwender werden lieb gewonnene Funktionalitäten vermissen, die aus technischer Sicht in einer sicheren Umgebung nicht länger zu verantworten sind. Auch wird es Kritik geben, wenn der Zugang zum Hochschulnetz für unsichere IT-Systeme eingeschränkt wird.

Intelligente Konzepte, die kooperativ von IT-Sicherheitsexperten und IT-Anwendern entwickelt werden, bieten aber bei weitem mehr Vor- als Nachteile. Die Bündelung und zentrale Verwaltung von Ressourcen und Know-how bringt einen großen Sicherheitsgewinn und verhindert Schäden, die für Einzelpersonen oder eine Hochschule als Ganzes dramatische Auswirkungen haben können.

Ein nachgewiesenes, hohes IT-Sicherheitsniveau verhindert nicht nur mögliche Schäden, sondern erhöht auch die Attraktivität von Hochschulen für Kooperations- und Forschungspartner aus der Wirtschaft.

Nicht zuletzt ist ein zentrales, systematisches IT-Sicherheitsmanagement wesentlich kostengünstiger als eine verteilte Administration, wie sie heute noch oft betrieben wird. Die einzelnen Lehrstühle und Organisationseinheiten werden so von Tätigkeiten entlastet, die nicht zu ihren eigentlichen Lehr- und Forschungsaufgaben gehören.

Da die Randbedingungen an den Hochschulen in ihren Grundzügen durchaus vergleichbar sind, lassen sich durch eine gemeinsame und koordinierte Vorgehensweise der Hochschulen Synergieeffekte erzielen, die es allen Universitäten erlaubt, ihr IT-Sicherheitsmanagement nachhaltig zu verbessern.

#### **5. Kontakt zum BSI**

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200363

53133 Bonn

Telefon: +49 (0) 1888 9582-0

Telefax: +49 (0) 1888 9582-400

E-Mail: [bsi@bsi.bund.de](mailto:bsi@bsi.bund.de)

Internet: [www.bsi.bund.de](http://www.bsi.bund.de)

[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)