Fachhochschule
Dortmund
University of Applied Sciences

Amtliche Mitteilungen

Verkündungsblatt

28. Jahrgang, Nr. 11, 18.06.2007

Sicherheitsleitlinie der Fachhochschule Dortmund

(Stand: Juni 2007)

Präambel

Die vorliegende Leitlinie bildet die Basis für die Sicherheitsstandards und die Umsetzung der daraus abgeleiteten Sicherheitsrichtlinien und Maßnahmen. Zum Schutz der Informationsverarbeitungs- und Kommunikationsinfrastruktur (IuK) der Fachhochschule Dortmund sind die Sicherheitsleitlinie und die daraus abgeleiteten Richtlinien und Maßnahmen für alle Angehörigen und Mitglieder der Fachhochschule verbindlich.

Eine Hochschule ist heute nur arbeitsfähig, wenn ihre Mitglieder einen möglichst fehlerlosen Zugriff auf die IuK haben. Letztere ist wesentliche Basis aller Arbeitsabläufe. Alle Mitglieder der Fachhochschule sind von der Verfügbarkeit der IuK abhängig. Dies bedeutet, dass absehbare Schäden und Gefahren für die Hochschule und das Land abgewehrt werden müssen, um einen reibungslosen Ablauf des Hochschulbetriebes sicherzustellen. Neben der Sicherstellung von Abläufen muss die Einhaltung rechtlicher Verpflichtungen, z.B. des Datenschutzes, verbindliche Regelungen und organisatorische Maßnahmen zur Gewährleistung der erforderlichen Sicherheit zu treffen, hochschulweit gewährleistet sein. Neben den Interessen der Hochschule sind nicht nur die Beschäftigten, sondern alle Angehörigen der Hochschule durch eine funktionierende Sicherheitsarchitektur zu schützen.

Die Sicherheitsleitlinie ist nicht abschließend. Sie kann ständig überarbeitet und ergänzt werden.

1. Die Sicherheitsarchitektur an der Fachhochschule Dortmund

Um Gefährdungen und Schäden an der IuK vorzubeugen, müssen geeignete Sicherheitsstandards eingeführt werden. Dabei begegnet man der Schwierigkeit, zwischen der Erreichung einer möglichst großen Transparenz der genutzten Infrastruktur und dem Anspruch notwendige Schutzmaßnahmen zur Gewährleistung eines hohen Sicherheitsstandards einen Ausgleich zu finden.

Ziel kann es daher nur sein, den Schwierigkeiten zu begegnen und eine an die Gegebenheiten der Fachhochschule Dortmund angepasste Sicherheitsarchitektur zu erreichen.

Die derzeit angestrebte Sicherheitsarchitektur der Fachhochschule Dortmund soll durch folgende Punkte erreicht werden:

1.1 Sicherheitsleitlinie

Auf oberster Ebene der Sicherheitsarchitektur definiert diese Sicherheitsleitlinie grundlegende Ziele der Datensicherheit und des Datenschutzes. Die Leitlinie legt Verantwortlichkeiten sowie Standards fest und definiert Rahmenbedingungen für ihre Umsetzung.

1.2 Sicherheitskonzept

Zur Erreichung der angestrebten Sicherheitsziele ist eine realistische Abschätzung des Schutzbedarfs einzelner IT-Komponenten oder einzelner IT-Bereiche und die daraus resultierende Festlegung und Einführung von Sicherheitsstandards notwendig. Dabei orientiert sich die Fachhochschule Dortmund grundsätzlich an den aufgeführten Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Erstellung von Sicherheitskonzepten. Diese beinhaltet folgende vier Punkte:

1. Bestandsaufnahme und Strukturanalyse der IT-Geräte, Software, Anwendungen und Daten,
2. Feststellung des Schutzbedarfs einzelner IT-Systeme,
3. Durchführung einer Risikoanalyse und
4. Festlegung von Sicherheitsstandards, Schutzmaßnahmen.

Basierend auf der Bestandsaufnahme erfolgt eine Zuordnung der IT-Komponenten in eine der folgenden Schutzbedarfskategorien, die sich weitestgehend an denen des BSI orientieren.

- **Schutzbedarf Niedrig bis Mittel (nach BSI: Normal)**
  Schäden haben Beeinträchtigungen der Institution zur Folge
- **Schutzbedarf Hoch**
  Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein. Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge
- **Schutzbedarf Sehr hoch**
  Der Ausfall der IT führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

Um den Schutzbedarf zu ermitteln, wird jede IT-Komponente auf den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit geprüft. Die Ermittlung des Schutzbedarfs findet zusammen mit den Nutzerinnen bzw. den Nutzern der IT-Komponente statt.

Für IT-Komponenten bzw. IT-Bereiche, die einen hohen oder sehr hohen Schutzbedarf haben, wird eine individuelle Risikoanalyse durch die administrierende Stelle und dem jeweiligen SIN-Beauftragten durchgeführt, die die Wahrscheinlichkeit für den Eintritt eines sicherheitsrelevanten Schadensfalls ermittelt. Wurde der Schutzbedarf auf niedrig bis mittel festgelegt wird eine gruppenbezogene Risikoanalyse durchgeführt. Für die betroffenen IT-Komponenten werden im Sicherheitskonzept die Sicherheitsstandards festgelegt, aus denen sich die erforderlichen Sicherheitsmaßnahmen und Richtlinien ableiten.

Derzeit wird davon ausgegangen, dass der Schutzbedarf „Sehr hoch“ für keine IT-Komponente bzw. keinen IT-Bereich an der Fachhochschule Dortmund besteht.

1.3 Sicherheitsrichtlinien

Die Sicherheitsrichtlinien sind das Regelwerk, das anhand der im Sicherheitskonzept definierten Sicherheitsstandards Richtlinien und Regeln formuliert und Möglichkeiten der Realisierung aufzeigt.

Es sind proaktive und reaktive Sicherheitsrichtlinien zu unterscheiden. Proaktive Sicherheitsrichtlinien dienen der Erreichung und Überwachung der angestrebten IT-Sicherheitsstandards. Reaktive Richtlinien dienen als Vorgaben für die Bearbeitung sicherheitsrelevanter Vorgänge.

Die Sicherheitsrichtlinien sollen sowohl den Schutz gegen absichtliche Angriffe als auch den Schutz gegen unbeabsichtigte Ausfälle zum Gegenstand haben. Die AG „Erweitertes Sicherheitskonzept“ stellt eine Liste der durch sie erarbeiteten Sicherheitsrichtlinien bereit und aktualisiert diese nach Erforderlichkeit.

2. Leitlinien einer IT-Sicherheitsarchitektur

Die IT-Sicherheitsarchitektur der Fachhochschule Dortmund basiert auf folgenden Grundsatzaussagen:

- Die Fachhochschule Dortmund ist bestrebt, einen offenen Informationsaustausch zu gewährleisten, sofern keine dienst-, urheber- oder datenschutzrechtlichen Belange verletzt werden.

- Die Durchsetzung, Aufrechterhaltung und dauerhafte Fortentwicklung der Sicherheitsstandards wird durch die Tatsache gewährleistet, dass die Hochschulleitung den Sicherheitsprozess initiiert und aktiv unterstützt. Ein rein auf Fachbereichs- bzw. Einrichtungsebene initiierter Sicherheitsprozess kann keine dauerhafte Fortentwicklung der angestrebten Sicherheitsstandards gewährleisten

- Sicherheit kann nur erreicht werden, wenn hochschulweit gültige Sicherheitsstandards definiert werden und diese hochschulweit ggf. gestuft auf Ebene von Fachbereichen, Zentralen Einrichtungen und der Verwaltung erfolgreich umgesetzt werden.

- Sicherheit ist eine Gemeinschaftsaufgabe, die von allen Nutzerinnen und Nutzern der IuK wahrgenommen werden muss. Sie kann nur erfolgreich umgesetzt werden, wenn die Nutzerinnen bzw. Nutzer für Belange der Sicherheit sensibilisiert, geschult und über das Gefährdungspotential und mögliche Gegenmaßnahmen in ihrem Arbeitsumfeld informiert werden.

- Eine absolute Sicherheit der IuK ist nicht realisierbar; viele Beeinträchtigungen der Sicherheit beruhen jedoch auf allgemein bekannten Schwachstellen, die bei sachgemäßer Handhabung und Organisation zu beseitigen sind. Hierfür ist ein dynamischer, sich immer wiederholender Ablauf notwendig.

- Sicherheit ist kein Selbstzweck. Sie muss daher stets die Verhältnismäßigkeit der Maßnahmen und Mittel im Spann-

ungsfeld zwischen Informationsoffenheit, Kosten und Nutzerakzeptanz auf der einen und dem notwendigen Grad von Sicherheit auf der anderen Seite berücksichtigen.

- Der Schutz der in der IuK gehaltenen und verarbeiteten Daten gegen absichtliches Löschen, Verfälschen oder auch unabsichtlichen Verlust ist durch angemessene Maßnahmen der Datensicherung zu gewährleisten.

- Die Sicherheitsstandards sind permanent weiter zu entwickeln und durch Qualitätssicherungsmaßnahmen zu ergänzen, durch die zeitnah neue Risiken erkannt und geeignete Gegenmaßnahmen ergriffen werden können.

3. Die IT-Infrastruktur an der Fachhochschule Dortmund

Das Datennetz der Fachhochschule Dortmund verteilt sich auf drei Standorte, die mittels Richtfunkstrecken miteinander verbunden sind.

Die strukturierte Verkabelung basiert auf Lichtwellenleitern (LWL). Es wird gewährleistet, dass jedem Hochschulbeschäftigten mindestens ein Netzwerk-Anschluss zur Verfügung steht.

An allen drei Standorten steht zur Realisierung der Arbeiten in der Hochschule der Zugriff in das FH Netz über Wireless-LAN (WLAN) zur Verfügung. Der Zugriff im FH-Netz über WLAN erfordert eine vorherige Authentifizierung des Nutzers.

Eine sichere Verbindung von Extern kann mittels einer VPN-Verbindungen realisiert werden.

Weitere Einzelheiten ergeben sich aus dem Papier: „Netzbeschreibung FHDO“, das dieser Leitlinie als Anlage 1 beigefügt ist.

4. IT-Gefährdungslage und Sicherheitsziele

4.1 IT-Gefährdungslage

Die Verfügbarkeit der IuK wird mit zunehmender Häufigkeit einer missbräuchlichen Nutzung und mit einer wachsenden Zahl von Angriffen auf IT-Komponenten wie Rechner, Applikationen und Netze zunehmend bedroht.

Schwachstellen in Betriebssystemen und Anwendungsprogrammen, fehlerhafte Konfiguration von Arbeitsplatzrechnern, Servern und Netzkomponenten, sowie Schwachstellen der Implementation des im Hochschulnetz und Internet verwendeten Datenübertragungsprotokolls TCP/IP stellen ein erhebliches Gefährdungspotential für die IuK der Fachhochschule dar. Angreifer nutzen diese Schwachstellen zur Erlangung eines unberechtigten Zugriffs auf Rechnersysteme und zum Einschleusen von Programmen zum Mitschneiden des Datenverkehrs und zu weiteren Angriffen auf andere Rechner im Bereich der Fachhochschule, aber auch Dritter, aus.

Die Auswirkungen können von der Störung des Betriebs einzelner Komponenten bis zum Ausfall der kompletten IuK führen. Die Vertraulichkeit und Integrität der in der IuK abgelegten Daten ist dabei in höchstem Maße gefährdet. Forschungsergebnisse können z.B. durch unberechtigten Zugriff ausgespäht und manipuliert werden, was nicht nur zu einem erheblichen finanziellen Schaden, sondern auch zu einem nicht bezifferbaren Imageverlust der Wissenschaft an der Fachhochschule führen kann.

Zusätzlich zum Schutz gegen die beschriebenen Angriffe ist es erforderlich, die Sicherheit der IuK vor Ausfällen der IT-Komponenten, die durch Mängel ohne absichtliche Angriffe verursacht werden, zu gewährleisten. Neben diesen Gefährdungen sind ebenfalls die in der IuK genutzten Daten gegen Verlust zu sichern.

4.2 IT-Sicherheitsziele

Die an der Fachhochschule Dortmund angestrebten Sicherheitsstandards dienen dem Schutz der in der IuK der Fachhochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen, insbesondere im Hinblick auf

- **Zugänglichkeit/Verfügbarkeit**
  Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit von jedem Arbeitsplatz bei Bedarf verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren. Zudem müssen Daten regelmäßig gesichert werden.

- **Integrität**
  Daten und Anwendungen dürfen nicht unberechtigt gelöscht/zerstört oder manipuliert werden können.

- **Vertraulichkeit und Datenschutz**
  Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt der einsetzenden Stelle. Wegen der Gestaltung und der Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist die bzw. der behördliche Datenschutzbeauftragte rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der entsprechenden Verfahren.

5. Organisatorische Maßnahmen und Zuständigkeiten

5.1 SIN-Beauftragte der Organisationseinheiten

Auf Organisationsebene (Fachbereich, Zentrale Einrichtung, Verwaltung) sind die Leiter der jeweiligen Einrichtung für den Betrieb und die Sicherheit der vernetzten IT-Systeme verantwortlich. Es existieren Beauftragte für die Sicherheit im Netz (SIN-Beauftragte). Den SIN -Beauftragten soll nach Möglichkeit eine sachkundige Vertreterin bzw. ein sachkundiger Vertreter zur Seite stehen. Es finden regelmäßige Treffen zwischen den SIN-Beauftragten aus allen Bereichen unter Leitung der Sicherheitsbeauftragten bzw. des Sicherheitsbeauftragten der ZIN (Zentrale Einrichtung für IT Netzwerke)/ DVZ (Datenverarbeitungszentrale) statt.

5.2 Arbeitsgruppe „Erweitertes Sicherheitskonzept“ und Umsetzung des Sicherheitskonzepts

Auf der Basis der hier vorgelegten Sicherheitsleitlinie sind ein Sicherheitskonzept gemäß Punkt 2.2 und die darauf aufbauenden Sicherheitsrichtlinien gemäß 2.3 zu erarbeiten. Dies wird eine zweckmäßige Aufgabe der Arbeitsgruppe „Erweitertes Sicherheitskonzept“ sein. Um das Sicherheitskonzept und die Richtlinien hochschulweit umzusetzen und die angestrebten Sicherheitsstandards zu realisieren, sind entsprechende verbindliche Regelungen notwendig. Die Verwaltungs- und Benutzungsordnung der ZIN/DVZ ist den neuen Anforderungen gemäß anzupassen und zu erweitern. Grundsätzlich wird angestrebt, vor allem durch Beratung und in Kooperation von Arbeitsgruppe und den jeweiligen Organisationseinheiten die erforderlichen Sicherheitsstandards zu erreichen. Die Arbeit der AG „Erweitertes Sicherheitskonzept“ findet im engen Austausch mit der Gruppe der SIN-Beauftragten statt.

5.3 Maßnahmen

Eventuell müssen weitere Regelungen, Ordnungen oder Dienstvereinbarungen erstellt werden, um die gewünschte Sicherheit der IuK an der Fachhochschule Dortmund zu erreichen und auch zukünftig zu gewährleisten. Bei allen Maßnahmen zur Gewährleistung der Sicherheit sind zur Priorisierung die Gesichtspunkte der Angemessenheit, Kosten und Wirtschaftlichkeit zu berücksichtigen.

Ausgefertigt aufgrund des Beschlusses des Senats der Fachhochschule Dortmund vom 13.06.2007.

Dortmund, den
Der Rektor
gez.

Prof. Dr. Eberhard Menzel

Netzstruktur der Fachhochschule Dortmund

Das Datennetz der Fachhochschule Dortmund verteilt sich auf drei Standorte und ist mittels virtueller Netze (VLANs) in mehrere Segmente unterteilt. Diese sind logisch einzelnen Einrichtungen zugeordnet. Um diese Segmente in allen Standorten verfügbar zu haben, werden sie über ein ATM-Richtfunk Netz nachgebildet (LANE) . Zur Zeit betreibt die FH drei ATM-Richtfunkstrecken mit jeweils 155 Mbit in einem Dreieck zwischen den Standorten

- Sonnenstr. - Max-Ophüls-Platz ,
- Sonnenstr. – Emil-Figge-Str. und
- Max-Ophüls-Platz - Emil-Figge-Str.

Die strukturierte Verkabelung begann schon in 1998 und erfolgte in mehreren Stufen, ab 2001 jedoch über HBFG-Finanzierung.

Zurzeit stehen

- über 2800 Glasfaserports und
- über 1800 Kupferports (›=Kat5) überwiegend in Labors sowie PC-Pools

zur Verfügung.

Es sind insgesamt ca. 2000 aktive 100 Mbps sowie 150 aktive 1 Gbps switched Glasfaserports und ca. 1500 Kat5-Ports (überwiegend in Labors und PC-Pools) betriebsbereit.

Alle Labore haben im Schnitt vier 100 Mbps. und mindestens einen 1 Gbps Fiber-Anschluss an die zentralen Switches. Die Labore haben zusätzlich eigene dezentrale Switches und gestalten / verändern die Labor-Vernetzung je nach Bedarf. Die Administration der Labore obliegt den Fachbereichen.

Für alle Hochschulbeschäftigten steht mindestens jeweils ein 100 Mbps Netzwerk-Anschluss an die zentralen Switches zur Verfügung.

Derzeit sind über 50 Switches vom CISCO Typ Catalyst 19xx bis Catalyst 65xx, hiervon 18 mit Routingfunktion, im Einsatz.

Seit Mitte des Jahres 2004 steht an allen drei Standorten der Zugriff in das FH Netz über Wireless-LAN (WLAN) der Kategorie 801.11b/g zur Verfügung. Der Zugriff im FH-Netz über WLAN wird mittels eines VPN-Concentrators (VPN-Tunnel) realisiert, über das zurzeit auch die Zugriffe aus dem Internet bzw. über DSL erfolgen

Fachhochschule Dortmund
University of Applied Sciences

Netz der FH Dortmund