IT-Sicherheitskonzept der
Heinrich-Heine-Universität Düsseldorf
vom 06.12.2004

1 Präambel und Geltungsbereich

Diese Regelungen gelten für die gesamte Informationstechnologie (IT) in der Heinrich-Heine-Universität Düsseldorf (HHU), d.h., für alle technischen Kommunikationssysteme, alle Rechner, die als Server und am Arbeitsplatz genutzt werden, alle eingesetzten Softwareprodukte und alle gespeicherten oder zu bearbeitenden Daten. Sie umfassen auch verpflichtende Verhaltensmaßnahmen aller Nutzerinnen und Nutzer, die wegen der Gefährdung der Betriebssicherheit und aus Gründen des Datenschutzes erforderlich sind.

Im folgenden schließt der Begriff „HHU-Netz" das Netz des Universitätsklinikums ein. Für diejenigen Netzbereiche des Universitätsklinikums und der Universitätsverwaltung, die nur für eingeschränkte Konnektivität zum Internet und zum übrigen HHU-Netz eingerichtet sind, werden gesonderte Regelungen getroffen.

Als *Server* werden nachfolgend Computersysteme bezeichnet, die Dienstleistungen für mehrere Benutzer erbringen; andere werden *Arbeitsplatzrechner* genannt. Die Bezeichnung *IT-System* umfasst Server, Arbeitsplatzrechner und aktive Netzwerkkomponenten wie z.B. Router.

Mindestanforderungen an technische Standards und Dokumentation der Systeme werden in einer Technischen Anleitung getroffen, die separat veröffentlicht und fortgeschrieben wird.

Aspekte des Datenschutzes, die für den IT-Bereich relevant sind, regelt die Datenschutzordnung für die HHU.

2 Grundsätze

Dieses Sicherheitskonzept soll dazu beitragen, dass die IT-Einrichtungen der HHU produktiv und störungsfrei benutzt werden können. Hierzu sind verbindliche Vorschriften für alle Nutzerinnen und Nutzer erforderlich.

2.1 Verantwortlichkeiten

Die Verantwortung für die IT-Sicherheit liegt bei den Leiterinnen und Leitern der Fakultäten, Zentralen Einrichtungen oder Zentralen Verwaltung (die nachfolgend unter dem Oberbegriff „Einrichtungen" genannt werden). Werden Aufgaben, die ihnen nach dieser Richtlinie obliegen, auf andere Mitarbeiterinnen oder Mitarbeiter übertragen, so ist dies unter Namensnennung zu dokumentieren. Für jedes vernetzte IT-System sind Name, dienstliche Adresse und Telefonnummer sowie Email-Adresse des Betreuers oder der Betreuerin zu erfassen. Diese Daten werden vom URZ in einer Datenbank verwaltet und nur zur Benachrichtigung im Störungsfall verwendet. Wenn keine der betreuenden Personen in angemessener Zeit erreichbar ist, kann das URZ das betreffende System erforderlichenfalls vom Datennetz trennen.

2.2 Feststellung der Sicherheitsanforderungen

Für alle IT-Systeme im Geltungsbereich dieses Sicherheitskonzepts sind die Sicherheitsanforderungen unter Berücksichtigung gesetzlicher Vorgaben und dienstlicher Erfordernisse festzulegen. Hierzu werden in der Technischen Anleitung Sicherheitsbedarfsklassen festgelegt, die sich an den vom Bundesamt für Sicherheit in der Informationsverarbeitung (BSI) vorgeschlagenen Sicherheitsniveaus orientieren und die besonderen Gegebenheiten der Hochschule berücksichtigen. Die Einordnung der Systeme in eine dieser Klassen obliegt der Leiterin/dem Leiter der Einrichtung, in der das System betrieben wird. Zum Erreichen eines hohen Schutzniveaus sind Einschränkungen hinsichtlich der Konnektivität und der Einfachheit der Benutzung des Systems in Kauf zu nehmen.

Auf Systeme mit erhöhtem Schutzbedarf darf nur Zugriff haben, wer dies zur Erfüllung seiner Aufgaben benötigt. Diese Zugriffe müssen durch verlässliche Authentisierung und geeignete Protokollierung nachvollzogen werden können.

3 Organisatorische und technische Regelungen

3.1 Allgemeine Anforderungen an den Betrieb von IT-Systemen im HHU-Netz

Alle IT-Systeme sind durch ihre Betreiber/innen in angemessenen Zeitabständen gemäß der technischen Anleitung auf ordnungsgemäßen Betrieb und Einhaltung der Sicherheitsanforderungen zu überprüfen. Sicherheitsrelevante Korrekturen müssen zeitnah eingesetzt werden. Sicherheitsüberprüfungen, Portscans oder Versuche zur Überwindung von Sicherheitsmaßnahmen sind bei fremden Systemen grundsätzlich nur nach Absprache mit den Systemverantwortlichen des fremden Systems zulässig. Das URZ kann zur Abwehr drohender Gefährdungen solche Aktionen unangemeldet durchführen, muss aber die Systemverantwortlichen über Durchführung und Ergebnis informieren.

Soweit die Funktion von Netzwerken und Computern zentral überwacht wird, ist die Betreiberin/der Betreiber eines Systems zur erforderlichen Abstimmung mit den Mitarbeiterinnen und Mitarbeitern des URZ verpflichtet.

Jede Betreiberin/jeder Betreiber muss für alle eingesetzte Software die notwendigen Lizenzen vorweisen können.

Die Vergabe von Host- und Domainnamen sowie öffentlichen und sichtbaren privaten Adressen wird vom URZ koordiniert.

Personenbezogene Daten sind bei der Speicherung und Übertragung besonders zu sichern, z.B. durch geeignete Verschlüsselung. Datenträger mit personenbezogenen Daten sind gegen unbefugten Zugriff in geeigneter Form zu schützen. Im Falle der Entsorgung ist sicherzustellen, dass die Daten nicht

mehr gelesen werden können.

Werden Sicherheitsverstöße im HHU-Netz festgestellt, so sind diese dem CERT (Computer Emergency Response Team) des URZ zu melden, das ggf. auch die Weitergabe von Meldungen an externe CERTs, die Polizei oder die Staatsanwaltschaft koordiniert.

3.2 Pflichten beim Betrieb von Arbeitsplatzrechnern

Jeder Arbeitsplatzrechner ist nach dem Stand der Technik gegen unberechtigten Zugang und gegen die Installation von Schadsoftware (Viren, Würmer, Trojanische Pferde, Dialer) zu schützen und auf die Wirksamkeit des Schutzes zu überprüfen. Für häusliche oder mobile Arbeitsplatzrechner legt die Technische Anleitung gesonderte Sicherheitsanforderungen fest.

3.3 Pflichten beim Betrieb von Servern

Server sind unter Angabe der vorgesehenen zu erbringenden Netzwerkdienste beim URZ anzumelden. Dabei sind eine Administratorin oder ein Administrator und eine Stellvertreterin oder ein Stellvertreter zu benennen.

Die Nutzung eines Servers (z.B. als Proxy-Server) zum Zwecke der Umgehung von Sicherheitsvorkehrungen muss wirksam unterbunden werden.

Dateizugriffsdienste (File Serving, File Sharing, globale oder Netzwerkdateisysteme etc.) dürfen nur in besonders definierten Fällen für Nutzerinnen/Nutzer außerhalb eines Instituts- oder Fakultätsnetzes angeboten werden. Von den Systemverantwortlichen sind dann geeignete Maßnahmen zu treffen, um einen Missbrauch zu verhindern. Vom URZ angebotene zentrale Dateizugriffsdienste (z.B. Home Directories) werden auf Zugriffe aus dem HHU-Netz beschränkt.

Die Nutzung der Serverdienste ist zu protokollieren. Änderungen der Konfiguration müssen über einen angemessenen Zeitraum hinweg nachvollziehbar sein, damit Unregelmäßigkeiten oder Sicherheitsverstöße analysiert werden können. Näheres regelt die Technische Anleitung.

3.4 Regelungen für den Betrieb spezieller Netzwerkdienste

Der Empfang von Email wird über die zentralen Mailserver des URZ abgewickelt; sofern dezentrale Mailserver eingesetzt werden, wird diesen die Mail über die zentralen Server zugestellt. Für ein- und ausgehende Mail ist nach dem Stand der Technik sicherzustellen, dass sie frei ist von Computerviren und anderer, für den Empfänger schädlicher Software. Unerbetene Massenmails (sog. „Spam") dürfen nicht versandt werden; auf eingehende Mail sind geeignete Filterprogramme anzuwenden, die solche Mails markieren und ausfiltern können.

Sonstige von außerhalb der HHU anzusprechende Netzwerkdienste müssen beim URZ angemeldet werden und werden nur in begründeten Fällen freigeschaltet.

3.5 Regelungen zum Schutz der Netzwerkinfrastruktur

Die Gewährleistung der Funktionssicherheit des HHU-Netzes ist eine zentrale Aufgabe. Veränderungen der technischen oder logischen Netzstruktur sind nur mit Zustimmung des URZ zulässig; hierzu gehören die Schaffung von Verbindungen zwischen verschiedenen Netzwerkbereichen und die Herstellung zusätzlicher Außenanbindungen, der Einsatz von Routingprotokollen, die Inbetriebnahme von Funk-LANs und die Einrichtung von virtuellen privaten Netzen über den Bereich eines IP-Subnetzes hinaus.

3.6 Regelungen zum Schutz von Systemen und Netzen durch Firewalls

Arbeitsplatzrechner dürfen mit dem externen Internet nur unter Zwischenschaltung mindestens eines separaten Firewall-Systems verbunden sein. Serversysteme müssen ebenfalls durch Firewalls geschützt werden.

Das URZ betreibt zentrale Firewallsysteme, die für die einzelnen Instituts- bzw. Fakultätsnetze den Schutz in Standardanwendungsfällen zur Verfügung stellen können.

Welche Dienste im Einzelfall durch Firewalls freigeschaltet werden sollen, entscheidet die Leiterin oder der Leiter der Einrichtung. Die Firewall-

Konfigurationen sollen aus einem in der Technischen Anleitung aufgeführten Katalog ausgewählt werden.

Das URZ unterstützt den Einsatz dezentraler Firewalls durch fachliche Beratung und geeignete Netzwerkkonfiguration.

4 Sicherheitsüberprüfungen

Die IT-Systeme werden regelmäßig von den nach 2.1 Verantwortlichen und dem URZ auf Einhaltung der Bestimmungen dieser Richtlinie überprüft. Häufigkeit, Art und Umfang dieser Überprüfung regelt die Technische Anleitung.

Das für IT-Fragen zuständige Gremium der HHU erarbeitet ein Handbuch mit Regeln für Not- und Katastrophenfälle.

5 Inkrafttreten

Dieses Rahmenkonzept für IT-Sicherheit tritt am Tag nach seiner Veröffentlichung in den Amtlichen Bekanntmachungen der Universität in Kraft.

Ausgefertigt auf Grund des Beschlusses des Senats der Heinrich-Heine-Universität Düsseldorf vom 27.07.2004.

Düsseldorf, den 06.12.2004

Der Rektor
Der Heinrich-Heine-Universität
Düsseldorf

Alfons Labisch
Univ.-Prof. Dr.med. Dr.phil. M.A.(Soz.)