AMTLICHE MITTEILUNGEN

Verkündungsblatt der Bergischen Universität Wuppertal
Herausgegeben vom Rektor

Jahrgang 38 | Datum 28.05.2009 | Nr. 14

IT-Sicherheitskonzept

der Bergischen Universität Wuppertal

vom 28. Mai 2009

1
Präambel und Geltungsbereich

Diese Regelungen gelten für die gesamte Informationstechnologie (IT) der Bergischen Universität Wuppertal (BUW), d.h. für alle technischen Kommunikationssysteme, alle Rechner, die als Server oder als Computer-Arbeitsplätze 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.

Diese Regelungen gelten im Kontext und in Übereinstimmung mit der Verwaltungs- und Benutzungsordnung des ZIM (Zentrum für Informations- und Medienverarbeitung der BUW), als deren weitere Spezifizierung und Ergänzung sie zu sehen sind.

Als Server werden nachfolgend Computersysteme bezeichnet, die Dienstleistungen für mehrere Benutzer oder Computer 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. Konkrete Aspekte des Datenschutzes, die für den IT-Bereich relevant sind, werden hier nicht explizit behandelt.

2
Grundsätze

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

IT-Sicherheit ist eine notwendige Voraussetzung für die Datensicherheit, also den Schutz von Daten vor Vernichtung, Verfälschung oder längerer Nichtverfügbarkeit, die wiederum notwendige Voraussetzung für den Datenschutz, also den grundrechtlich garantierten Schutz personenbezogener Daten, ist. Somit ist das IT-Sicherheitskonzept substanzieller Bestandteil der IT-Konzeption der Universität.

2.1
Verantwortlichkeiten

Die Verantwortung für die IT-Sicherheit liegt bei den Leiterinnen und Leitern der Fachbereiche, Zentralen Betriebseinheiten oder der Universitätsverwaltung (die nachfolgend unter dem Oberbegriff „Einrichtungen" ge-

nannt 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 E-Mail-Adresse des Betreuers oder der Betreuerin zu erfassen. Diese Daten werden vom ZIM in einer Datenbank verwaltet und nur zur Benachrichtigung im Störungsfall verwendet. Im Fall einer störenden Beeinflussung anderer IT-Systeme durch ein IT-System innerhalb des Universitätsnetzes kann das ZIM 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 BUW berücksichtigen. Die Einordnung der Systeme in eine dieser Klassen obliegt der Leiterin bzw. 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
Anforderungen an den Betrieb von IT-Systemen im Universitätsnetz

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 ZIM 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 ZIM verpflichtet. Jede Betreiberin bzw. 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 ZIM koordiniert.

Personenbezogene Daten sind gemäß den datenschutzrechtlichen Vorgaben zu behandeln und insbesondere bei der Speicherung und Übertragung besonders zu sichern, z.B. durch die Anwendung geeigneter Verschlüsselungsverfahren. 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 Universitätsnetz festgestellt, so sind diese dem ZIM zu melden, das im Rahmen der rechtlichen Vorgaben auch die Weitergabe von Meldungen an externe CERTs (Computer Emergency Response Teams, z.B. des DFN), 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 ZIM 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 und Nutzer außerhalb eines Instituts- oder Fachbereichsnetzes angeboten werden. Von den Systemverantwortlichen sind dann geeignete Maßnahmen zu treffen, um einen Missbrauch zu verhindern. Vom ZIM angebotene zentrale Dateizugriffsdienste (z.B. Home Directories) werden auf Zugriffe aus dem Universitätsnetz 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 E-Mail wird über die zentralen Mailserver des ZIM abgewickelt; sofern dezentrale Mailserver eingesetzt werden, wird diesen die Mail über die zentralen Server zugestellt. Für ausgehende Mail ist nach dem Stand der Technik sicherzustellen, dass sie frei ist von Computerviren und anderer, für den Empfänger schädlicher Software. Unerbetene Massenmails (sogenannter „Spam") dürfen nicht versandt werden.

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

Die Nutzung von Filesharing (Peer-to-Peer)-Protokollen (P2P) und deren Software-Produkten wie z.B. Gnutella, KaZaA, eDonkey, Bittorrent und andere sind ohne vorherige Absprache mit dem ZIM nicht zu zulässig.

3.5
Regelungen zum Schutz der Netzwerkinfrastruktur

Die Gewährleistung der Funktionssicherheit des Universitätsnetzes ist eine zentrale Aufgabe. Veränderungen der technischen oder logischen Netzstruktur sind nur mit Zustimmung des ZIM 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 ZIM betreibt hierfür zentrale Firewall-Systeme, die für die einzelnen Instituts- bzw. Fakultätsnetze den Schutz in Standardanwendungsfällen zur Verfügung stellen.

4
Sicherheitsprüfungen

Die IT-Systeme werden regelmäßig von den nach 2.1 Verantwortlichen und dem ZIM auf Einhaltung der Bestimmungen dieser Richtlinie überprüft. Häufigkeit, Art und Umfang dieser Überprüfung regelt die Technische Anleitung. Das für IT-Fragen zuständige Gremium der BUW erarbeitet ein Handbuch mit Regeln für Not- und Katastrophenfälle.

5
In-Kraft-Treten

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

Ausgefertigt auf Grund des Beschlusses des Senats der Bergischen Universität Wuppertal vom 29. April 2009.

Wuppertal, den 28.05.2009

Der Rektor
der Bergischen Universität Wuppertal
Universitätsprofessor Dr. Lambert T. Koch