Hochschule RheinMain

AMTLICHE MITTEILUNG

Nr.: 897

Veröffentlicht am: 09.02.2024

Richtlinie für die IT-Systembetreibende an der Hochschule RheinMain

Herausgeber:

Präsidentin

Hochschule RheinMain

Postfach 3251

65022 Wiesbaden

Redaktion:

Abteilung VIII

Rainer Scholl

E-Mail: rainer.scholl@hs-rm.de

BEKANNTMACHUNG

Nach § 1 der Satzung der Hochschule RheinMain zur Bekanntmachung ihrer Satzungen vom 04. Juni 2013 (StAnz. vom 29.7.2013, S. 929) wird die Richtlinie für die IT-Systembetreibende der Hochschule RheinMain hiermit bekanntgegeben.

Wiesbaden, 09.02.2024

Prof. Dr. Eva Waller

Präsidentin

Hochschule RheinMain

Richtlinie für IT-Systembetreibende an der Hochschule RheinMain

Inhalt

PRÄAMBEL

Die Hochschule RheinMain, ihre Fachbereiche und Einrichtungen betreiben eine Informationsverarbeitungs- und Kommunikations (IuK)-Infrastruktur, bestehend aus Informationsverarbeitungssystemen (Rechenanlagen) und einem Multiservice-Kommunikationsnetz zur Übertragung von Daten und Sprache (darunter fallen auch Bild- und Videoübertragungen). Diese IuK-Infrastruktur ist an das weltweite Internet angeschlossen.

Diese Richtlinie regelt die Bedingungen, unter denen das Leistungsangebot betrieben wird. Sie wird entsprechend dem Fortschreiten der Technik und des Informationssicherheitsprozesses der Hochschule fortlaufend aktualisiert und ergänzt.

1 ALLGEMEINES

(1) Geltungsbereich

Diese Richtlinie gilt für die Systembetreibenden aller an der HSRM betriebenen IuK-Infrastrukturen, bestehend aus Informationsverarbeitungssystemen, Kommunikationssystemen und weiteren Hilfseinrichtungen, z.B.:

- alle im Netz vorhandenen Computer (Clients und Server), aktive Netzkomponenten, Netzdrucker,
- industrielle Steuerungen (Industrial Control Systems, ICS),
- Telekommunikationsgeräte, Mobiltelefone oder andere mobile Geräte.

(2) Infrastruktur für Forschung und Lehre

IT-Systeme und Netze, die ausschließlich für Zwecke von Forschung und Lehre genutzt werden, in denen keine personenbezogenen oder sonstige vertrauliche Daten verarbeitet werden und die nicht mit dem Hochschulnetz, einem dezentralen Netz, dass mit dem Hochschulnetz vebunden ist, oder dem Internet verbunden sind, können durch Beschluss des jeweiligen Dekanats oder der:des Kanzler:in von den Bestimmungen nach Nr. 3 bis 6 (außer Nr. 3.6) ausgenommen werden. Der Beschluss ist dem ITMZ mitzuteilen.

(3) Definitionen

1 Systembetreibende

Systembetreibende ist die Organisationseinheit, die den Betrieb eines IT-Systems verantwortet. Dies ist für das Hochschulnetz, zentrale Systeme und Dienste das IT- und Me-dienzentrum (ITMZ) der Hochschule RheinMain. Das ITMZ regelt den Zugang der einzelnen Systeme zum zentralen Hochschulnetz. Dies betrifft insbesondere die Vergabe der hierzu benötigten Ressourcen (Netzzugänge, IP-Adressen, DNS- Domänen-Namen, Firewall-Freigaben), für dezentrale Systeme oder Netze die jeweils zuständige Organisationseinheit der Hochschule (Fachbereich, Arbeitsgruppe, Einrichtung oder andere Untereinheit der Hochschule), in den Fällen von 1.2 der jeweilige Fachbereich.

2 Systemadministrator:in

Ein:e Systemadministrator:in ist eine Person, die von Systembetreibenden beauftragt wurde, die zum Systembetrieb gehörigen Aufgaben für die Beschäftigten der jeweiligen Organisationseinheit wahrzunehmen.

3 Netz

Ein Netz ist die Gesamtheit der aktiven und passiven Komponenten, die die Kommunikation zwischen IT-Systemen ermöglicht. Dies umfasst insbesondere Verkabelung, Switches, Router sowie W-Lan Access-Points.

4 Server

Ein Server ist ein IT-System, das Dienste für andere IT-Systeme über ein Netzwerk bereitstellt. Systeme, die ausschließlich kurzfristig im Rahmen von Forschung, Studium und Lehre (z.B. bei Lehrveranstaltungen oder Vorführungen) eingesetzt werden, sind von den Regelungen unter Nr. 6 ausgenommen. Über weitere Ausnahmen entscheidet auf Antrag die:der Kanzler:in.

(4) Systemadministrator:innen

1 Benennung von Systemadministrator:innen

Alle Systembetreibenden sind verpflichtet, für jedes betriebene System ein:e Systemadministrator:in und in der Regel ein:e Stellvertreter:in zu benennen und diese dem ITMZ als Systemverantwortliche zu nennen. Die Beendigung der Tätigkeit ist ebenso dem ITMZ mitzuteilen.

2 Anforderungen an Systemadministrator:innen

Systemadministrator:innen und Stellvertreter:innen müssen zuverlässig und fachlich geeignet sein.

Systembetreibende und Systemadministrator:innen sind zur Vertraulichkeit verpflichtet.

3 Entzug von Rechten

Bei Beendigung der Tätigkeit in der IT-Administration sind den betroffenen Personen die entsprechenden Rechte zu entziehen.

4 Professor:innen wissenschaftliches und technisch-adminsitratives Personal

Die Pflichten der Systemadministrator:innen aus den Nr. 3.2, 3.3, 3.4, 3.6 und Nr. 5. gelten entsprechend für Professor:innen, wissenschaftliche und technisch-adminsitrative Beschäftigte, wenn sie eigenständig Software auf Hochschulrechnern installieren.

2 GRUNDSÄTZE DES SYSTEMBETRIEBS

(1) Nutzer:innenverwaltung

1 Zentrales Identity- und Access-Management (IAM)

Das ITMZ führt eine Übersicht über die Nutzungsberechtigten und die an einzelnen Nutzer:innengruppen erteilten Berechtigungen für zentrale Systeme. Bei Bedarf werden

Sonderberechtigungen für einzelne Nutzer:innen hinterlegt. Die Nutzung zentraler und dezentraler IT-Systeme der HSRM setzt den Eintrag im zentralen IAM voraus.

2 Dezentrale Rechteverwaltung

Wenn die dezentralen Systembetreibenden für einzelne Systeme eigene Nutzungsregelungen festlegen, so führen diese Systembetreibenden eine Übersicht über die so erteilten Nutzungsberechtigungen.

(2) Datenschutz und Informationssicherheit

Die Systembetreibenden sind verpflichtet, alle gültigen Rechtsvorschriften zur Wahrung der Integrität, Vertraulichkeit und Verfügbarkeit der Daten der Nutzer:innen einzuhalten. Ferner ist er verpflichtet, die Nutzer:innen durch entsprechende Vorkehrungen vor missbräuchlicher Datenverarbeitung zu schützen und regelmäßig die getroffenen Maßnahmen zu evaluieren. Die Regelungen der Leitlinie Datenschutz an der Hochschule RheinMain (AM798) sind zu beachten.

3 ALLGEMEINE PFLICHTEN VON SYSTEMBETREIBENDEN

(1) Zugang zu zentralen IT-Services

Der Zugriff auf nicht öffentlich zugängliche zentrale IT-Services setzt die Einhaltung dieser Richtlinie voraus. Das ITMZ kann den Zugriff durch technische Maßnahmen beschränken. Je nach Schutzbedarf kann das ITMZ zusätzliche Einschränkungen einrichten.

(2) Absicherung des Systemzugangs

IT-Systeme müssen gegen unbefugte Benutzung gesichert werden. Daher ist zur Nutzung eine Anmeldung am System (Login) erforderlich und es sind Maßnahmen gegen unbefugten physischen Zugang zu treffen.

Ausnahmen sind möglich bei Systemen, die ausschließlich zu Forschung oder Lehre dienen, in nicht allgemein zugänglichen Räumen aufgestellt sind, nicht mit dem Hochschulnetz oder dem Internet verbunden sind und außer von den Administrator:innen nur unter Aufsicht benutzt werden (z.B. Messaufbauten, Laborrechner).

(3) Information über Sicherheitslücken und Patches

Systemadministrator:innen müssen sich regelmäßig über die Sicherheit der von ihnen betreuten IT-Systeme informieren (z.B. durch Abonnement der entsprechenden Herstellerinformationen).

(4) Behebung von Sicherheitslücken

Sicherheitspatches sind unverzüglich zu installieren. Systemkonfigurationen, die die Informationssicherheit beeinträchtigen, sind unverzüglich zu ändern.

(5) Überprüfung von Zugriffsrechten

Alle vergebenen Zugriffsrechte müssen regelmäßig überprüft und entzogen werden, wenn sie nicht mehr erforderlich sind.

(6) Meldung von Vorfällen

Sicherheitsvorfälle und Datenschutzverstöße sind dem CISO und dem:der Justiziar:in für Datenschutzmanagement zu melden.

(7) Dokumentation des Standortes

Die Standorte aller ortsfesten Komponenten sind zu dokumentieren und Namen und/oder Adressen sichtbar am Gerät anzubringen

(8) Multi-Homing

Der Anschluss eines IT-Systems an verschiedene Subnetze erfordert die Zustimmung des:der Netzbetreibenden.

4 PFLICHTEN BEI BETRIEB EINES NETZES

(1) Sichere Aufstellung der Komponenten

Die aktiven Netzkomponenten (Switches, Router, Firewalls etc.) und Patchfelder müssen vor unbefugtem Zugang geschützt sein (verschlossener Raum oder Schrank).

(2) Login zu Netzkomponenten

Der administrative Zugang zu aktiven Netzkomponenten muss sowohl netzseitig (Firewall) als auch durch Login und Rechteregelung auf die zuständigen Administrator:innen beschränkt sein.

(3) Zugang zum Hochschulnetz

Netzanschlüsse müssen gegen unbefugten Zugriff gesichert sein. Bei öffentlich zugänglichen Netzanschlüssen (Netzwerkdosen in allgemein zugänglichen Bereichen, WLAN) ist daher eine Anmeldung am Netz erforderlich.

(4) Einrichtung von Subnetzen

Im Netz müssen entsprechend der Sicherheitsanforderungen Subnetze eingerichtet werden. Dabei ist zu beachten:

a) Arbeitsplatzrechner und Server müssen in verschiedenen Subnetzen platziert werden.

b) Bei Arbeitsplätzen müssen Rechner, die ausschließlich von Beschäftigten genutzt werden, von solchen getrennt werden, die (auch) von Studierenden genutzt werden. Studentische Hilfskräfte gelten als Beschäftigte.

c) Das ITMZ ist über die eingerichteten Subnetze und ihren Verwendungszweck zu informieren.

(5) IP-Adressen

Das ITMZ vergibt die zu verwendenden IP-Adressen und regelt deren Verwendung. Bei der Nutzung öffentlicher IP-Adressen sind außerdem die Regeln des RIPE NCC zu beachten.

Bei der Vergabe von IP-Adressen ist sicherzustellen, dass nachvollziehbar ist, wer bzw. welches Gerät eine IP-Adresse zu einer bestimmten Zeit hatte.

(6) NAT

Zur effizienten Nutzung von IP-Adressen und um die interne Netzstruktur vor möglichen Angreifer:innen zu verbergen kann für Zugriffe auf das Internet NAT eingesetzt werden. NAT in Richtung des Hochschulnetzes kann dazu führen, dass zentrale IT-Services nicht genutzt werden können.

5 PFLICHTEN BEI DER AUSWAHL UND INSTALLATION VON SOFTWARE

(1) Planung und Auswahl von Software

Für jede Software ist der Verwendungszweck und die Art der damit verarbeiteten Daten festzulegen. Bei der Auswahl sind die daraus folgenden Sicherheitsanforderungen zu beachten.

Das ITMZ stellt eine Liste bereits geprüfter und für Anwendungen mit normalem Schutzbedarf freigegebener bzw. nicht freigegebener Software bereit (White- bzw. Blacklist).

(2) Verwendung sicherer Installationsquellen

Bei der Installation sind ausschließlich Quellen zu verwenden, bei denen gewährleistet ist, dass die Software nicht verändert wurde.

(3) Abschaltung sicherheitsgefährdender oder datenschutzverletzender Funktionen

Optionen und Funktionen, die die Sicherheit von Hochschulsystemen oder des Hochschulnetzes gefährden oder die zu Datenschutzverletzungen führen, müssen bei der Installation deaktiviert werden.

(4) Sicherstellung der Verfügbarkeit von Updates

Bei der Auswahl von Software ist sicherzustellen, dass die Verfügbarkeit von Sicherheitsupdates gewährleistet ist.

6 PFLICHTEN BEI BETRIEB EINES SERVERSYSTEMS

(1) Sichere Aufstellung

Server müssen vor unbefugtem physischem Zugriff geschützt sein, z.B. durch Aufstellung in einem verschlossenen Raum oder Schrank.

(2) Trennung von Servern und Arbeitsplätzen

Server dürfen nicht als Arbeitsplatzrechner verwendet werden. Dies gilt auch umgekehrt.

(3) Sichere Einrichtung

Bei der Einrichtung von Servern sind nicht benötigte Funktionen und Dienste zu deaktivieren.

7 RECHTE DER SYSTEMBETREIBER

(1) Passwortüberprüfung

Die Systembetreibenden sind berechtigt, die Sicherheit der in den eigenen IT-Systemen gespeicherten Nutzendenpasswörter und der Nutzendendaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, z.B. Änderungen leicht zu erratender oder veralteter Passwörter, durchzuführen, um die IuK-Ressourcen und Nutzendendaten vor unberechtigten Zugriffen Dritter zu schützen. Bei erforderlichen Änderungen der Nutzendenpasswörter, der Zugriffsberechtigungen auf Nutzendendateien und sonstigen nutzungsrelevanten Schutzmaßnahmen ist der:die Nutzer:in unverzüglich in Kenntnis zu setzen.

(2) Verwendung von Diagnosetools

Bei Störungen oder Verdacht auf missbräuchliche Nutzung können von den Systembetreibenden Diagnosetools (z.B. Netzwerk-Sniffer) verwendet werden. So gespeicherte Daten sind unverzüglich zu löschen, sobald die Störung behoben oder der Verdacht aufgeklärt ist, vorbehaltlich weiterer rechtlicher Schritte.

(3) Einschränkung der Nutzung der Ressourcen

Die Systembetreibenden können die Nutzung ihrer Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren, soweit es zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutze der Nutzendendaten erforderlich ist. Sofern möglich, sind die betroffenen Nutzer:innen hierüber unverzüglich zu unterrichten.

Betreibende von Netzen können entsprechend an ihr Netz angeschlossene Dienste, Ports, Systeme oder Subnetze sperren. Die betroffenen Systemadministrator:innen bzw. Nutzer:innen werden in diesen Fällen informiert.

(4) Protokollierung

1 Zweck der Protokollierung

Der Systembetreiber entscheidet über die Protokollierung der Nutzung der von ihm betriebenen IT-Systeme für nachfolgende Zwecke.

Die Protokolldaten dienen dabei

- der Sicherstellung eines ordnungsgemäßen Betriebes des Systems,
- der Kapazitätsplanung sowie
- der Aufklärung bei Verdacht rechtswidriger Handlungen.

Im Übrigen dürfen sie nicht zur Verhaltens- und Leistungskontrolle der Beschäftigten herangezogen werden.

2 Inhalt der Protokollierung

Die Protokolle enthalten i.d.R. folgende Informationen:

- Zeit des Vorgangs
- Angaben zum:zur Nutzer:in (z.B. Nutzendenkennung, IP- oder E-Mail-Adresse)

- Art der Nutzung
- Ressourcen, auf die zugegriffen wurde.

3 Geräte ohne eigene Protokollierung

Bei Systemen, die keine automatische Protokollierung ermöglichen (z.B. Mikrocontroller oder Messgeräte), können die Nutzungsdaten wie Name der:des Nutzenden und der Zeitraum der Nutzung auch manuell festgehalten werden.

4 Aufbewahrung der Protokolldaten

Die Protokolldaten werden höchstens sechs Monate aufgehoben, es sei denn, dass eine längere Aufbewahrungsdauer vorgeschrieben ist.

8 RECHTE DES ITMZ

(1) Einschränkung der Nutzung

Das ITMZ kann zur Verbesserung der Informationssicherheit oder des Datenschutzes, zum Schutz der Nutzer:innen und der Reputation der Hochschule oder aus Gründen des betrieblichen Ablaufs oder der Wirtschaftlichkeit die Nutzung der IuK-Infrastruktur einschränken.

Dies umfasst insbesondere Verweigerung der Annahme, Nichtzustellung oder Kennzeichnung von E-Mails, die mit hoher Wahrscheinlichkeit Schadsoftware oder unerwünschte Massenmails (SPAM) enthalten.

Sofern von Diensten oder Systemen eine wesentliche Beeinträchtigung der IuK-Infrastruktur oder anderer Nutzer:innen ausgeht, ist das ITMZ berechtigt, eine Sperrung im angemessenen Umfang durchzuführen. Der Systembetreiber ist– außer in dringenden Fällen – vorher anzuhören. Die Sperrung ist unverzüglich wiederaufzuheben, wenn der Systembetreiber dem ITMZ den Wegfall der Beeinträchtigung mitgeteilt und das ITMZ dies verifiziert hat.

Die Rechte des:der Informationssicherheitsbeauftragten bleiben unberührt.

(2) Protokollierung von E-Mail- und Internet-Nutzung

Die Protokollierung von E-Mail und Internetnutzung erfolgt nach den Regeln von Nr. 7.4. Eine Trennung in private und dienstliche Nutzung findet hierbei nicht statt.

9 LIZENZMANAGEMENT

Die Hochschule entwickelt eine Richtlinie zum Lizenzmanagement, die bei Auswahl, Beschaffung und Einsatz von Software zu beachten ist.

10 ÜBERGANGSREGELUNGEN

(1) In-Kraft-Treten

Diese Richtlinie für Systembetreibende tritt am Tage nach der Veröffentlichung in den Amtlichen Mitteilungen der Hochschule RheinMain in Kraft. Sie wird mindestens alle drei Jahre überprüft und bei Bedarf aktualisiert.

(2) Netzmigration

Die Regelungen in Nr. 4.4 bis 4.6 sind innerhalb von 18 Monaten nach Inkrafttreten dieser Richtlinie umzusetzen. Das ITMZ initiiert dazu ein Migrationsprojekt mit den betroffenen Fachbereichen.

(3) Evaluation

In der Runde der IT-Beauftragten wird die Umsetzung der Richtlinie regelmäßig besprochen. Sie kann im Einvernehmen mit der:dem Kanzler:in, der:dem CIO und der:dem CISO vorläufige Maßnahmen beschließen, die die Regelungen dieser Richtlunie ergänzen oder ersetzen. Sie werden in den Amtlichen Mitteilungen veröffentlicht und fließen in die nächste Überarbeitung ein.