Amtliche Mitteilungen der

Philipps Universität Marburg

Veröffentlichungsnummer: 01/2023 **Veröffentlicht am: 13.01.2023**

Richtlinie zur Administration von IT-Systemen und IT-Diensten im Netzwerk der Philipps-Universität

Inhaltsverzeichnis

1 Ziele

Entsprechend der Informationssicherheitsleitlinie[1] der Philipps-Universität, sind Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen und IT-Diensten die wichtigsten Schutzziele der Informationssicherheit. Eine nicht ordnungsgemäße Administration von IT-Systemen erleichtert Angriffe auf verschiedene Informationsverbünde und beeinflusst unmittelbar diese Schutzziele. Diese Richtlinie soll IT-Administrierende dabei unterstützen, die ihnen anvertrauten IT-Systeme und Dienste ordnungsgemäß zu administrieren, sodass die Schutzziele der Informationssicherheit und des Datenschutzes erreicht und gewahrt werden. Diese Richtlinie ersetzt keine detaillierteren Regelungen, die beispielsweise in IT-Sicherheitskonzepten von IT-Systemen und IT-Diensten getroffen werden müssen. Die Kennzeichnung der Verbindlichkeit von Anforderungen durch „muss“,

1 https://www.uni-marburg.de/de/hrz/ueber-uns/it-management/inf-sicherheitsleitlinie.

„darf nicht“ bzw. „darf kein“ und „sollte“ richtet sich nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[2].

2 Begriffsbestimmungen und Geltungsbereich

2.1 IT- Administrierende

IT- Administrierende sind Personen, die ein IT-System oder einen IT-Dienst für die Nutzung durch andere Personen einrichten oder betreiben. Personen, die die Betreuung von Fachanwendungen oder Teilsystemen übernehmen, sind ebenfalls IT-Administrierende im Sinne dieser Richtlinie.

2.2 IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.

2.3 IT-Dienst

Ein IT-Dienst ist ein elektronischer Informations- und Telekommunikationsdienst im Sinne des Telemedien- und Telekommunikationsgesetzes[3].

2.4 Authentisierung

Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u.a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen. Die Authentisierung einer Identität kann ebenfalls durch kryptographische Signaturen erfolgen.

2.5 Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

2.6 Geltungsbereich

Diese Richtlinie gilt für alle IT-Administrierenden der Philipps-Universität Marburg.

3 Organisatorische Anforderungen

Administrative Rollen müssen von kontrollierenden Rollen (z. B. Revision) getrennt werden.

Wenn mehrere IT-Administrierende ein System gemeinsam administrieren, muss die Aufgabenverteilung geregelt sein: Die spezifischen Aufgaben der IT-Administrierenden sollten schriftlich dokumentiert werden, um eine gegenseitige Beeinträchtigung sowie Unklarheiten über die Verantwortungsbereiche zu vermeiden. Zudem sollten feste Ansprechpersonen und Kommunikationsschnittstellen definiert werden, um den fachlichen Austausch zu erleichtern.

Für den Krankheits- oder Urlaubsfall sollte eine Vertretung für die Administration benannt und eingewiesen werden.

4 Allgemeine Aufgaben und Verantwortung

IT-Administrierende sorgen für einen möglichst störungsfreien Betrieb der IT-Systeme und IT-Dienste. Die Schutzziele der IT-Sicherheit sowie des Datenschutzes müssen erreicht und die

2 Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Benutzerdefinierte_BS/Autorenrichtlinie.pdf?__blob=publicationFile&v=3.
3 Vgl. § 1, Abs. 2, lit. c der Ordnung der Philipps-Universität für die Nutzung und den Betrieb der Informationstechnologie (IT-Nutzungsordnung, https://www.uni-marburg.de/de/hrz/ueber-uns/it-management/it-nutzungsordnung).

Einhaltung dieser Schutzziele kontrolliert werden können. Die Umsetzung der dafür notwendigen Maßnahmen ist abhängig vom Schutzbedarf der verarbeiteten Daten.

IT-Administrierende sollten sich kontinuierlich und anlassbezogen über sicherheitsrelevante und systemstabilisierende Patches, Updates und sonstige Maßnahmen für die Behandlung von Sicherheitsrisiken informieren und diese umsetzen. Bei der Informationsbeschaffung ist es sinnvoll, auf mindestens zwei Quellen zurückzugreifen. Einige Informationsquellen sind beispielsweise:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) (siehe http://www.bsi.bund.de/)
- Warnmeldungen des CERT Bund – Das Computer-Notfallteam des BSI (siehe https://cert-bund.de/)
- Heise-Security Newsletter (https://www.heise.de/newsletter/manage/heisec-summary)
- Hersteller bzw. Distributoren von Anwendungen und Betriebssystemen

4.1 Sichere Konfiguration von IT-Systemen und IT-Diensten

Vor dem produktiven Einsatz sollten sich IT-Administrierende über die erforderlichen Maßnahmen zur Einhaltung der Schutzziele informieren. Dies gilt insbesondere für Systeme, auf denen Daten mit einem hohen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit verarbeitet werden. Außerdem sollte die Hard- und Software getestet werden.

IT-Administrierende müssen für das System geeignete und angemessene Sicherheitslösungen einsetzen (bspw. Antivirensoftware, Firewalls etc.). Sie sollten ein zentrales Konfigurationsmanagement sowie eine automatisierte Softwareverteilung verwenden. Es sollten nur notwendige IT-Dienste, Ports und Berechtigungen aktiviert sein.

Für die Automatisierung von Administrationsaufgaben sollten Passwörter nur dann hinterlegt werden, wenn es keine andere (technische) Lösung gibt.[4]

4.2 Sicherer Betrieb von IT-Systemen und IT-Diensten

Am universitären Datennetz dürfen nur IT-Systeme und IT-Dienste betrieben werden, für die Sicherheitspatches zur Verfügung gestellt und installiert werden. IT-Administrierende müssen vorgesetzte Personen sowie die Stabsstelle Informationssicherheit über Systeme in ihrem Verantwortungsbereich informieren, für die keine Sicherheitspatches mehr zur Verfügung gestellt oder installiert werden können.

IT-Administrierende müssen regelmäßige Datensicherungen (je nach Schutzbedarf auch auf Offline-Medien) der IT-Systeme durchführen. Dazu sollte ein Datensicherungsplan erstellt werden. IT-Administrierende sollten sicherstellen, dass besonders sensible Sicherungskopien verschlossen aufbewahrt werden. Elektronische Datenträger, die nicht länger benötigt werden, müssen vor der Entsorgung ausgesondert und sicher gelöscht oder zerstört werden.

Um die Ausfallzeiten von IT-Systemen und IT-Diensten gering zu halten und deren Funktionalität zu überwachen, sollten IT-Administrierende ein geeignetes Monitoring einsetzen. Beim Anlegen von Protokolldateien für IT-Systeme und IT-Dienste muss auf Datenschutz- und Mitbestimmungsaspekte sowie auf das Prinzip der Datensparsamkeit geachtet werden. Die Einsichtnahme in Protokolldateien ist nur zur Sicherung des Betriebs und zur Fehleranalyse erlaubt. Die Zugriffsrechte auf und die Aufbewahrungszeiten von Protokolldateien müssen IT-Administrierende auf das erforderliche Maß beschränken.

Zur Vermeidung von Störungen müssen IT-Administrierende regelmäßig Wartungsarbeiten durchführen. Sicherheitsrelevante Wartungen müssen IT-Administrierende umgehend vornehmen. Sind dazu Vorbereitungen nötig, müssen sie damit unmittelbar beginnen. Wartungsarbeiten sollten so durchgeführt werden, dass der laufende Betrieb möglichst wenig gestört wird. Wartungs- und Reparaturarbeiten sollten IT-Administrierende den betroffenen Personen rechtzeitig ankündigen. Wartungen an IT-Systemen sollten dokumentiert werden. Administrative Vorgänge, die einen

4 Die Hinterlegung von Passwörtern vermittelt einen falschen Signalcharakter für den sicheren Umgang mit Passwörtern.

kritischen Einfluss auf IT-Systeme oder IT-Dienste haben können, dürfen nicht vor längeren Abwesenheiten des zuständigen IT-Administrierenden durchgeführt werden.

Die Wartungsarbeiten sollten von fachkundigen Personen ausgeführt werden. Wartungs- und Reparaturarbeiten durch Externe sollten beaufsichtigt werden. Sofern diese Arbeiten als Fernwartung durchgeführt werden, gelten die Regelungen der Fernwartungsrichtlinie für IT-Systeme der Philipps-Universität Marburg[5].

Störungen an IT-Systemen und -Diensten müssen IT-Administrierende umgehend beheben. Gravierende Störungen müssen analysiert und Verbesserungsmöglichkeiten für die künftige Vermeidung der Störungen erarbeitet werden. Diese sollten dokumentiert werden.

4.3 Dokumentation

Änderungen, die an einem IT-System vorgenommen werden, sollten IT-Administrierende in einem Protokoll dokumentieren[6]. Dies erleichtert Vertretungen und Nachfolgenden den Einstieg in ihre Tätigkeiten. Zusätzlich können dadurch Sicherheitsvorfälle besser aufgeklärt bzw. nachverfolgt werden.

Aus der Dokumentation sollte hervorgehen:

- welche Änderungen erfolgt sind,
- wann die Änderungen erfolgt sind,
- wer die Änderungen durchgeführt hat,
- auf welcher Grundlage bzw. aus welchem Anlass die Änderungen erfolgt sind.

Die Art der Dokumentation sollte in einem Sicherheitskonzept festgelegt werden. Vorhandene Protokollierungsmechanismen von Systemen und IT-Diensten sollten dabei in einem geeigneten Umfang genutzt werden. Für die Dokumentation können beispielsweise Systemlogbücher, Ticketsysteme oder ähnliches eingesetzt werden.

4.4 Authentisierung und Autorisierung

Die Authentisierung mit Administrations- und Nutzerkonten an IT-Systemen und IT-Diensten muss über verschlüsselte Netzwerk-Verbindungen erfolgen. Um die Eingabe von Authentisierungsdaten bei betrügerischen IT-Systemen und IT-Diensten zu verhindern, muss die Authentizität des IT-Systems oder des IT-Dienstes vor der Authentisierung eindeutig verifiziert werden. Passwörter müssen mit einem dem Stand der Technik entsprechenden Hash- oder Verschlüsselungsverfahren geschützt werden. IT-Administrierende müssen Zugriffe auf ein Konto durch ein geeignetes Authentisierungsverfahren absichern. Ist die Benutzungsberechtigung eines Kontos abgelaufen, müssen IT-Administrierende den Zugang sperren. Administrations- und Nutzerkonten sollten ausschließlich von einer Person genutzt werden.

Für Administrationskonten gilt:

- Passwörter für Administratoren müssen komplexer (z. B. längere Passwörter, mehr verschiedene Zeichenkategorien, 2-Faktor-Authentisierung) als Passwörter für Nutzerkonten sein.[7] IT-Administrierende müssen voreingestellte Standard-Passwörter des Herstellers von Hard- und Software vor der Inbetriebnahme ändern. Eine Kopie der Zugangsdaten für ein Administrationskonto sollte in einem verschlossenen Umschlag in einem Safe aufbewahrt werden.
- IT-Administrierende müssen für Administrationsaufgaben Konten mit abgestuften Rechten nutzen. Das Administrationskonto darf nur für Administrationsaufgaben genutzt werden.

5 https://www.uni-marburg.de/de/universitaet/administration/recht/satzung/ri_2021_09_30_fernwartung.pdf
6 Darunter fallen beispielsweise Änderungen an der Hardware, der Software, der Konfiguration oder des Standorts.
7 https://www.uni-marburg.de/de/hrz/az/passwortrichtlinie

Insbesondere dürfen keine Alltagsaufgaben wie das Bearbeiten von E-Mails oder das Surfen im Internet ausgeführt werden. Die Anmeldung mit einem Administrationskonto darf nur auf vertrauenswürdigen und von besonders geschützten Systemen erfolgen. Hierfür sollten Systeme, die ausschließlich für die Administration vorgesehen sind, verwendet werden. Insbesondere müssen §5 Abs. 3 und 4 der IT-Nutzungsordnung[8] beachtet werden.

- Wenn ein IT-System oder ein IT-Dienst von mehreren IT-Administrierende betreut wird, sollte jeder IT-Administrierende ein eigenes Administrationskonto nutzen. Sind IT-Administrierende für verschiedene Aufgaben (Datenbank, Systemverwaltung etc.) zuständig, sollten die Berechtigungen dahingehend angepasst werden, dass jeder IT-Administrierende nur die für seine Aufgabe erforderlichen Berechtigungen hat. Bei Übernahme eines Administrationskontos muss das dazugehörige Passwort geändert werden, z. B. bei Beginn und Ende einer Vertretung bzw. bei Austritt von einer Person, die Kenntnis über dieses Passwort hatte.

Für Nutzerkonten gilt:

- Nutzerinnen und Nutzer dürfen nur Zugriff auf Daten haben, die sie für ihre Arbeit benötigen. Dabei sollte auch auf die Zugriffsart (z. B. lesen, schreiben, ausführen) geachtet werden.
- IT-Administrierende sollten Nutzerinnen und Nutzer dahingehend unterstützen, dass unabsichtliche Dateifreigaben und die Datensicherheit gefährdende Einstellungen unterbunden werden.

5 Datenschutzrechtliche Anforderungen

Alle Informationen, die IT-Administrierende aufgrund Ihrer erhöhten Berechtigungen an IT-Systemen im Rahmen Ihrer Tätigkeiten bekannt werden, müssen grundsätzlich vertraulich behandelt werden. Dabei muss eine unbefugte Einsichtnahme durch Dritte[9] verhindern werden. Die Verpflichtung zum Datengeheimnis bleibt auch nach Beendigung der Tätigkeit an der Universität Marburg bestehen.

Für bestehende und neu eingeführte Systeme, die personenbezogene Daten verarbeiten, müssen IT-Administrierende die Notwendigkeit einer entsprechenden Datenschutzdokumentation mit der Rechtsabteilung abstimmen. Sollten personenbezogene Daten durch externe Dienstleister verarbeitet werden, muss zusätzlich ein Auftragsverarbeitungsvertrag abgeschlossen werden.

Personenbezogene Daten dürfen nach Art. 5 DSGVO zu keinem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeitet werden. Die Einsichtnahme in sonstige Inhalte (insbesondere E-Mails) ist ohne eine entsprechende Rechtsgrundlage unzulässig.

Sofern im Rahmen von Garantie- oder Wartungsleistungen elektronische Datenträger an externe Dritte gegeben werden, müssen IT-Administrierende sicherstellen, dass diese nicht auf die Daten zugreifen können.

IT-Administrierende müssen Datenschutzvorfälle unverzüglich der oder dem Datenschutzbeauftragten melden (datenschutz@uni-marburg.de, +49 6421 28-26484).

8 https://www.uni-marburg.de/de/hrz/ueber-uns/it-management/it-nutzungsordnung

9 [Ein] Dritter [ist] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (DSGVO Art. 4, Abs. 10)

6 Verhalten bei Sicherheitsvorfällen

Bei gravierenden Sicherheitsvorfällen, z. B. Ausführen von Schadsoftware, Einbruch in ein System oder unberechtigte Manipulation, müssen IT-Administrierende das betroffene System unverzüglich vom Datennetz der Philipps-Universität trennen.

IT-Administrierende müssen Sicherheitsvorfälle unverzüglich an die Stabsstelle Informationssicherheit melden (it-sicherheit@uni-marburg.de, +49 6421 28-28281).

Die Richtlinie zur Administration von IT-Systemen und IT-Diensten im Netzwerk der Philipps-Universität wurde am 10.01.2023 vom Präsidium der Philipps-Universität genehmigt und tritt mit Veröffentlichung in den Amtlichen Mitteilungen in Kraft.

In Kraft getreten am 14.01.2023