JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

Der Präsident

Mitteilungen der Justus-Liebig-Universität Gießen

09.05.2014 | **2.26.30 Nr. 4**

Richtlinien für die IT-Systemadministration

Richtlinien für die IT-Systemadministration an der JLU Gießen

Fassungsinformationen

Richtlinien: verabschiedet vom Präsidium am 15.04.2014; tritt am 10.05.2014 in Kraft.

Tabellarische Darstellung der Fassungsinformationen

	Genehmigung	*Inkrafttreten/Geltung*
Richtlinien	Präsidium 15.04.2014	10.05.2014

Inhaltsverzeichnis

Zielsetzung

Mit diesen Richtlinien für IT-Systemadministratorinnen und IT-Systemadministratoren werden diesen Verhaltensregeln für ihre tägliche Arbeit an die Hand gegeben. Sie sollen den Administratorinnen und Administratoren dabei helfen, die von ihnen verwalteten Systeme und Dienste so zu betreuen, dass insbesondere die Ziele der IT-Sicherheit und des Datenschutzes beachtet werden.

Begriffsdefinition IT-Administratorin/IT-Administrator

Eine IT-Systemadministratorin beziehungsweise ein IT-Administrator ist jede Person, die ein IT-System oder einen IT-Dienst für die Nutzung durch andere Personen einrichtet und betreibt.

In diesem Text steht der Begriff IT-Systemadministrator im Folgenden sowohl für die weibliche als auch für die männliche Form, im Folgenden kurz als Administrator bezeichnet.

Abgrenzung zu Gastsystemen und -diensten

Für auf den vom Administrator verwalteten Systemen eventuell installierte Gastsysteme und –dienste liegt die Verantwortung beim Auftraggeber/Betreuer der Gastsysteme und -dienste. Für diese Personen gelten die Richtlinien zur IT-Systemadministration entsprechend.

Generelle Anforderungen

Der Administrator hat innerhalb seines ihm zugewiesenen Bereichs für einen möglichst störungsfreien Betrieb der von ihm betreuten IT-Systeme und –Dienste zu sorgen. Er ist dafür verantwortlich, dass die Ziele der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit und Integrität der Daten) sowie des Datenschutzes durch geeignete Maßnahmen erreicht werden und die Einhaltung dieser Ziele kontrolliert werden kann. Die Umsetzung dieser Maßnahmen soll in Absprache mit dem Vorgesetzten in einem wirtschaftlich sinnvollen Rahmen erfolgen. Der Administrator ist verpflichtet, die einschlägigen Gesetze und Vorschriften zu beachten und deren Einhaltung soweit als möglich technisch zu unterstützen.

Allgemeine Aufgaben und Verantwortungen

Jeder Administrator hat nach Absprache mit seinem Vorgesetzten einen Vertreter einzuweisen und so zu informieren, dass dieser während Abwesenheitszeiten (Urlaub, Krankheit) des Administrators die Standardadministrationsaufgaben übernehmen kann. Dazu ist möglichst eine entsprechende Dokumentation zu erstellen und aktuell zu halten.

Der Administrator soll sich regelmäßig über sicherheitsrelevante und systemstabilisierende Patches, Updates oder sonstige Anleitungen zur Behebung von Sicherheitslücken oder Instabilitäten informieren und diese zeitnah umsetzen.

Der Administrator soll mit der oder dem IT-Sicherheitsbeauftragten kooperieren und ist gehalten und berechtigt, jederzeit Vorschläge zur Verbesserung der IT-Sicherheit zu machen.

Auch bei sorgfältigem Arbeiten sind Fehler und Fehlbedienungen nicht vollständig auszuschließen. Der Administrator soll aus solchen Fehlern lernen und transparent mit ihnen umgehen mit dem Ziel, dass dieser Fehler nicht nur vom Administrator selbst, sondern auch von anderen Administratoren zukünftig vermieden wird.

Konfiguration der Systeme und Dienste

Vor dem produktiven Einsatz ist die eingesetzte Hard- und Software nach Möglichkeit zu testen.

Bei der Installation von Software und Bereitstellung von Diensten ist auf die korrekte Lizensierung zu achten.

Voreingestellte Default-Passwörter des Herstellers von IT-Hard- oder –software sind mit der ersten Inbetriebnahme zu ändern.

Je nach Wichtigkeit des vom Administrator bereitgestellten IT-Dienstes sind dieser und die Systeme, auf denen er läuft, möglichst ausfallsicher auszulegen und die Funktionalität durch ein automatisiertes Monitoring zu überwachen.

Auf einem System sollen grundsätzlich nur die Dienste (Softwarekomponenten) und Ports aktiviert sein, die für die beabsichtigte Funktion unerlässlich sind. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren.

Es sind angemessene und geeignete Sicherheitsprodukte (z.B. Virenschutz) einzusetzen. Je nach Sicherheitsbedürfnis kann auch die Einrichtung und Konfiguration einer hostbasierten Firewall notwendig sein.

Beim Anlegen von Protokolldateien für Systeme und Dienste sind Datenschutz- und Mitbestimmungsaspekte sowie das Prinzip der Datensparsamkeit zu beachten. Für Log-Dateien mit personenbezogenen Inhalten bedeutet das in der Regel, dass die Erstellung und Genehmigung eines Verfahrensverzeichnisses notwendig wird. Die Zugriffsrechte auf und die Aufbewahrungszeiten von Log-Dateien sind auf das erforderliche Mindestmaß zu beschränken. Die gegebenenfalls in Dienstvereinbarungen festgelegten Fristen sind einzuhalten.

Umgang mit Daten

Da ein Administrator rollenbedingt meist Zugriff auf alle Daten eines Systems hat, ist hierbei eine besondere Sensibilität gefordert.

Der Administrator muss alle Dateninhalte, die ihm im Rahmen seiner Tätigkeit bekannt werden, grundsätzlich vertraulich behandeln und Verschwiegenheit wahren. Eine Einsichtnahme durch Dritte ist zu verhindern. Das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit als Administrator an der JLU fort.

Der Administrator ist berechtigt, auf alle Daten zuzugreifen, die er zur Erfüllung seiner Aufgaben benötigt. Personenbezogene Daten dürfen nach §9 HDSG zu keinem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeitet werden. Die Einsichtnahme in Protokolldateien ist, soweit zur Sicherung des Betriebs und zur Fehleranalyse erforderlich, erlaubt. Die Einsichtnahme in sonstige Inhalte, insbesondere von Mails, ist nur mit ausdrücklicher vorheriger Erlaubnis des oder der Betroffenen oder aufgrund einer besonderen Rechtsgrundlage nach gesonderter Beauftragung zulässig. Sollten dem Administrator durch eigene Fehlbedienung oder Versehen persönliche Dateninhalte anderer Personen bekannt werden, die er im Rahmen seiner Administratorentätigkeit sonst nicht erlangt hätte, so ist der betroffene Nutzer darüber zu informieren.

Elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden, sind vor der Entsorgung sicher zu löschen. Bei der Aussonderung von IT-Systemen ist ebenfalls darauf zu achten, dass keine vertraulichen Informationen mehr zugänglich sind.

Für defekte Datenträger, die im Rahmen von Garantieleistungen oder Wartungsverträgen nach außen gelangen, ist vertraglich zu vereinbaren, dass die darauf gespeicherten Daten sicher gelöscht werden.

Zugangs- und Zugriffkontrolle

Die Zugangs- und Zugriffsrechte für die Benutzer sind vom Administrator einzurichten, zu dokumentieren und, soweit technisch und funktionell möglich, vor unberechtigten Änderungen zu schützen.

Nach Ablauf der Benutzungsberechtigung ist der Nutzer automatisch vom System zu sperren.

Zugangs- und Zugriffsrechte für die Benutzer sind so einzurichten, dass jeweils nur die berechtigten Personen Zugriff auf die Daten haben. Dabei ist auch nach Zugriffsart (lesen, schreiben, ausführen) zu unterscheiden. Default-Rechte für die Benutzer und für von diesen angelegte Daten sind möglichst restriktiv zu handhaben. Die Benutzer sind bei der Nutzung von IT-Diensten durch sinnvolle Voreinstellungen so zu unterstützen, dass unabsichtliche Datenfreigaben und die Datensicherheit gefährdende Einstellungen möglichst unterbunden werden.

Der Administrator selbst hat seiner Rolle angepasste Zugangsrechte zu nutzen (Trennung zwischen Administratoren- und seinen eigenen Benutzerrechten). Administratorrechte sind nur dort einzusetzen, wo es notwendig ist.

Der Zugriff des Administrators auf die zu administrierenden Systeme soll mittels eines verschlüsselnden Protokolls erfolgen.

Der Zugriff darf nur von vertrauenswürdigen Systemen aus erfolgen.

Das Administratoren-Passwort (für den Zugang zur Administratoren-Rolle) ist in besonderer Weise zu schützen. Es sollte noch höheren Sicherheitsanforderungen als das Benutzer-Passwort genügen. Für den Vertretungsfall

ist das Administratorpasswort möglichst in einem verschlossenen Umschlag in einem Safe aufzubewahren. Das Administrator-Passwort ist in angemessenen Zeitintervallen oder nach Beendigung des jeweiligen Vertretungsfalls zu wechseln.

Der Administrator hat bestehende Regeln für die Passworte der IT-Benutzer umzusetzen und deren Einhaltung technisch zu unterstützen.

Passwörter sind im System zugriffssicher möglichst verschlüsselt zu speichern.

Passwörter sind den Benutzern auf sichere Art zu übergeben.

Datensicherung

Es sind regelmäßige Datensicherungen durchzuführen. Dazu ist die Erstellung eines Datensicherungsplans sinnvoll.

Wartung

Der Administrator hat dafür zu sorgen, dass die Informationsverarbeitung möglichst störungsfrei abläuft. Hard- und Softwarekomponenten sind daher ordnungsgemäß zu warten. Wartungsarbeiten sind so durchzuführen, dass der laufende Betrieb möglichst wenig gestört wird. Daher sind die Wartungsarbeiten im Wartungsfester oder, falls das nicht möglich ist, in betriebsarmen Zeiten durchzuführen. Bei absehbar längeren Ausfallzeiten sind die Benutzer vorab zu informieren.

Verhalten bei Störungen

Eingetretene Störungen an IT-Systemen und –Diensten im Verantwortungsbereich des Administrators sind von diesem möglichst bald mit der den Auswirkungen angemessenen Priorität zu beheben. Die Ursachen von gravierenden Störungen sind zu analysieren und Verbesserungen zur künftigen Vermeidung zu erarbeiten. Dies ist zu dokumentieren.

Bei einem Verlust der Systemintegrität ist das betroffene System unverzüglich vom Datennetz zu trennen.