Richtlinie: Betrieb von Rechensystemen im Hochschuldatennetz

Arbeitskreis IT-Sicherheit an der UniBwM

Gültig ab: 25.07.2007

Datum	Bemerkung
25.03.2007	Erstfassung
23.04.2007	Einpflege GSHB
02.05.2007	Überarbeitung nach Sitzung AK
04.05.2007	kleine Änderungen in Layout und Formulierungen (TA)
25.07.2007	Zustimmung durch die Hochschulleitung
19.12.2010	Änderung Software-Updates Windows (WSUS), siehe 1.1
26.02.2011	Aktualisierung Verweise auf Grungschutzkataloge des BSI

Zielgruppe: Systemverantwortliche, Anwender

Thematik: Hochschuldatennetz (HDN), Betrieb, Rechensysteme

Zusammenfassung: Am HDN sind Rechner der unterschiedlichsten Hersteller und Systemfamilien angeschlossen, die in der Zuständigkeit der verschiedensten Bereiche der Universität autark betrieben werden. Damit das Rechenzentrum ein möglichst sicheres und stabiles Netzbetriebsverhalten gewährleisten kann, sind nachfolgende Regelungen bei Anschluss dieser Rechensysteme an das HDN einzuhalten.

Inhaltsverzeichnis

1 Rechensysteme und ihre Pflege

1.1 Aktuelles Betriebssystem

Rechensysteme dürfen am Hochschuldatennetz nur betrieben werden, wenn ein aktuelles, gepflegtes Betriebssystem darauf installiert ist. Das bedeutet:

1. Für das Betriebssystem gibt es (noch) Sicherheitsupdates vom Hersteller oder Distributor.
2. Die sicherheitsrelevanten Updates werden umgehend nach Verfügbarkeit eingespielt.
3. Bei Einsatz von Windows-Betriebssystemen ist der automatisierte Windows-Update-Dienst (WSUS) zu nutzen. Optional kann für Rechner innerhalb des Hochschuldatennetzes der zentrale Windows-Update-Service des Rechenzentrums genutzt werden (siehe auch `http://www.unibw.de/rz/gesamt/sicherheit/wsus`.

Das Rechenzentrum stellt Links zu den Sicherheitsupdates der meisten gängigen Betriebssystemhersteller auf seiner Homepage zur Verfügung.

1.2 Tagesaktueller Virenschutz

Ein tagesaktueller Virenschutz ist für alle Rechensysteme zu empfehlen, für die ein solcher auf dem Markt angeboten wird.

Die aufgrund ihrer großen Marktpräsenz besonders gefährdeten MS-Windows-Rechensysteme müssen mit einem tagesaktuellen Virenschutz versehen sein. Die Virenschutzsoftware muss folgende Anforderungen umsetzen:

- Mindestens einmal täglich werden die Virensignaturen automatisch auf Aktualität überprüft und gegebenenfalls aktualisiert.
- Beim Öffnen jeder Datei wird diese automatisch auf Virenfreiheit überprüft.
- Einmal täglich sollen *alle* Dateien des Rechensystems auf Virenfreiheit untersucht werden. Dies gilt insbesondere beim Einbringen von Fremddaten (z.B. über USB-Stick).

Das Rechenzentrum stellt für verschiedene Rechensysteme kostenlos Antiviren-Software für alle Universitätsangehörigen (auch für den Heimgebrauch) zur Verfügung. Nähere Informationen finden sich auf den Seiten des Rechenzentrums `http://www.unibw.de/rz/gesamt/sicherheit/sophosav`.

1.3 Aktuelle Applikationen

Rechensysteme sind nicht nur über ihre Betriebssysteme, sondern auch über die auf ihnen ablaufenden Applikationen angreifbar und missbrauchbar. Aus diesem Grund müssen auch Applikationen analog den Betriebssystemen (siehe 1.1) aktuell gepflegt werden. Unverzichtbar ist dies bei den weit verbreiteten Produkten für E-Mail, Web-Zugriff, Instant Messenger und Bürosoftware (z.B. Internet Explorer, Office, Outlook), da deren Schwachstellen besonders häufig für Angriffe genutzt werden.

Ganz besonders sorgfältig müssen ebenfalls Serverapplikationen wie z.B. Web, Mail und Datenbanken gepflegt werden, da diese über das Netz genutzt werden. Netzstörungen und auch Rechtsverletzungen sind häufig die Folge des Systemmissbrauchs.

2 Ausschluss unsachgemäße gepflegter Rechensysteme vom Netzverbund

Die Umsetzung der Vorschriften gemäß Punkt 1 verlangen eine regelmäßige Betreuung und Funktionskontrolle der ans HDN angeschlossenen Rechensysteme. Wird auch nur eine der Vorgaben gemäß Unterpunkt 1.1, 1.2, 1.3 nicht erfüllt, so ist das betroffene Rechensystem auf Dauer vom HDN zu trennen. Das Rechenzentrum behält sich vor, diese Trennung selbst vorzunehmen bzw. soweit dies technisch für das einzelne Rechensystem nicht möglich ist auch das gesamte betroffene Subnetz vom HDN zu trennen.

3 Betrieb institutseigener aktiver Netzkomponenten am HDN

Die betriebliche Verantwortung des Rechenzentrums endet an der peripheren Datennetzdose. Um Probleme bei der HDN-Nutzung zu minimieren, bietet das Rechenzentrum Beratungsleistung hinsichtlich der Beschaffung institutseigener aktiver Netzkomponenten (z. B. Router, Switches, WLAN-Accesspoints, Firewalls) an und bittet darum, vor Beschaffung solcher Komponenten Rücksprache mit der Betriebstechnik des Rechenzentrums zu nehmen.

4 Anbindung an öffentliche Netze

Der gleichzeitige Anschluss von Rechensystemen an das HDN und an öffentliche Netze (z.B. zusätzlicher DSL- oder IDSN-Anschluss) ist untersagt, da dadurch unkontrollierte Nebenschlüsse in das HDN entstehen.

5 Checklisten

Nachfolgende Checklisten sollen den Betroffenen eine einfache Hilfestellung zur Einhaltung dieser Richtlinie bieten.

5.1 Systemverantwortlicher

- ☐ Für dieses System gibt es noch aktuelle Sicherheitsupdates.

  Referenz: 1.1.

- ☐ Virenscanner ist installiert und konfiguriert.

  Referenz: 1.2.

- ☐ Sicherheitsrelevante Updates (sowie evtl. erforderliche zusätzliche Sicherheitssoftware) werden umgehend nach Verfügbarkeit eingespielt (Betriebssystem, Virenschutz und Applikationen).

  Referenz: 1.1, 1.2, 1.3;

  Allgemein: `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m02/m02273.htm`,
  `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m04/m04253.htm`,
  `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m04/m04249.htm`;

  Virenschutz: `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m02/m02159.htm`,
  `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m02/m02160.htm`.

- ☐ Im Fall eines Windows-basierten Systems wird dieses über einen WSUS-Dienst versorgt.

  Anleitung: `http://www.unibw.de/rz/leistungen/gesamt/sicherheit/wsus`.

- ☐ Die Sicherheit der verwendeten WWW-Browser ist gewährleistet.

  Referenz: 1.3,
  `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05045.htm`,
  `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05093.htm`,
  `http://www.heise.de/security/dienste/browsercheck/`,
  `http://www.heise.de/security/dienste/browsercheck/anpassen/`.

- ☐ Ein sicherer Betrieb von E-Mail-Applikationen ist gegeben.

  Referenz: 1.3, `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05053.htm`,

https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05054.htm,
https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05057.htm,
https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05094.htm,
https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05096.htm,
https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05108.htm.

- ☐ Den besonderen Sicherheitserfordernissen beim Anschluss von Laptops an lokale Netze wird Rechnung getragen.

  Referenz: https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m05/m05122.htm.

5.2 Anwender

- ☐ Sicherheitsrelevante Updates sind auf meinem System aktuell eingespielt.

  Anleitung: `http://www.unibw.de/rz/leistungen/gesamt/sicherheit/wincheck`.

- ☐ Der Virenscanner ist aktuell und aktiviert.

  Anleitung: `http://www.unibw.de/rz/leistungen/gesamt/sicherheit/wincheck`;

  Grundlegendes: `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m04/m04003.htm`;

  Verhaltensregeln: `https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m06/m06023.htm`.

- ☐ Soweit für mich als Anwender erforderlich, habe ich mich mit den Inhalten aus Abschnitt 5.1 vertraut gemacht.