Konzept für die Datensicherheit im

Daten- u. Kommunikationsnetz der Kernuniversität der

Friedrich Schiller Universität Jena (FSU Jena)

1. Zielstellung

Bei Nutzung eines Computers erwartet der Anwender, dass einerseits die Daten vor Verfälschung, Diebstahl, Missbrauch und Verlust geschützt sind und dass man andererseits nicht durch Viren, unerwünschten Mailverkehr u.Ä. in seiner Arbeit beeinträchtigt wird.
Dies wird aber nicht erreicht, wenn Arbeitsplatzrechner, Server oder Netze sich selbst überlassen werden. Eine 100%ige Sicherheit für IT – Systeme wird es nicht geben. Jeder Anwender sollte aber dieser Thematik seine ständige Aufmerksamkeit widmen, um eine optimale Sicherheit zu erreichen.

Diese Ordnung soll Grundregeln für einen sicheren Betrieb von Datenverarbeitungsgeräten und Kommunikationsnetzen in der Friedrich – Schiller – Universität festlegen und wurde entsprechend der Betriebs-/Benutzerordnung für das Datennetz der FSU (http://www.rz.uni-jena.de/allg/betrieb_benutzer.pdf) erarbeitet.

2. Verantwortlichkeiten

Für Betrieb, Wartung und Ausbau der Servertechnik für die angebotenen Dienste als auch der Netzübertragungstechnik der Kernuniversität ist das Universitätsrechenzentrum (URZ) zuständig. Eine Ausnahme bildet hierbei die Tertiärverkabelung, bei der Aufgaben im Zusammenhang mit Ausbau und Wartung kooperativ durch Verwaltung und URZ wahrgenommen werden. Der Betrieb dieser Verkabelung erfolgt arbeitsteilig durch das URZ und die Dezernate 3 - Betriebstechnische Dienste /Bauwesen /Fernmeldetechnik und 4 - Liegenschaften und Vermögensverwaltung. Anschlusspunkte der Inhouse – Verkabelung (Patchfelder) und Netzaktivtechnik sind in den Netzknotenräumen (Datenverteilern) der einzelnen Gebäude/Standorte untergebracht. Diese sind als betriebstechnische Räume im Sinne der Datensicherheit ausschließlich dem URZ und dem Dezernat 3 zugänglich.
Durch die Benennung von Endgeräte- und Anschlussverantwortlichen gemäß Punkt 2 der Betriebs- und Benutzungsordnung für das Datenkommunikationsnetz der Kernuniversität (DKNK) der Friedrich-Schiller-Universität Jena werden die Voraussetzungen geschaffen, damit eine kontinuierliche, qualifizierte Betreuung der Endgeräte erfolgen kann.

3. Generelle organisatorische Maßnahmen zur Datensicherheit

- Zentrale Sicherheitsmaßnahmen des URZ
    - Mail als Hauptvirenquelle: Einsatz eines Virenscanners zum Prüfen von Emails bei deren Eintreffen.
    - Datensicherheit: Zentral im Rechenzentrum gespeicherte Daten werden vor unberechtigtem Zugriff geschützt. Bei fahrlässigem Verhalten des Nutzers (Passwörter (s.u.), Benutzung unverschlüsselter Datenkanäle durch den Nutzer, usw.) kann keine Verantwortung übernommen werden.

- Nutzerdaten werden im Rahmen der Datenverwaltung im Rechenzentrum nur verschlüsselt übertragen.
- Nutzerdaten werden regelmäßig und automatisch gesichert, um diese im Havariefall (z.B. Hardwareausfall) wieder herstellen zu können.
- Es werden für alle kritischen Anwendungen verschlüsselte Verbindungen angeboten: ssh, sftp, scp, pop3s, imaps, https...
- Es liegt in der Verantwortung des Nutzers, diese auch anstelle der unverschlüsselten Verbindungen zu verwenden; die Verwendung unverschlüsselter Verbindungen wird grundsätzlich als fahrlässig eingestuft.

- Zentralserverbetrieb

Das URZ ist verantwortlich für den stabilen und sicheren Betrieb der zentralen Serverdienste, die von allen Einrichtungen genutzt werden.
Das betrifft insbesondere folgende Dienste:

- Server zur zentralen Nutzerverwaltung und zentrale Verzeichnisdienste (z.B. LDAP, RADIUS, NIS, NDS, ADS)
- DNS Server - Domain Name System
- DHCP Server - Dynamic Host Configuration Protocol
- Mail Server
- WWW Server - World Wide Web
- FTP – Server - File Transfer Protocol
- File- und Archivserver
- Backupserver
- Rollendatenbank
- Computeserver
- Lizenzserver
- Downloadserver für Windows Sicherheitsupdates
- Server für die Verteilung von Windows Virensignaturen

Der Betrieb von eigenen Servern in den Einrichtungen ist grundsätzlich mit dem Rechenzentrum abzustimmen. Sie sind entsprechend der geforderten Sicherheitsstufe für die auf diesen Servern laufenden Dienste in die Firewall - Struktur der Universität einzubinden. Server, die bereits vom Rechenzentrum vorgehaltene zentrale Dienste anbieten, werden in der Regel nur genehmigt, wenn deren Notwendigkeit ausreichend begründet werden kann.
Für diese dezentralen Server ist durch den Betreiber ein stabiler und sicherer Betrieb zu garantieren – auch in Krankheits- oder Urlaubszeiten.

- Registrierung von Endgeräten

Die Struktureinheiten - Identifikatoren sind den Kostenstellenummern der entsprechenden Einrichtungen zugeordnet und werden überall dort verwendet, wo
IV - Strukturen mit Universitätsstrukturen in Verbindung stehen (Verzeichnisdienste u. ä.). Eine Pflege der Struktureinheiten - Identifikatoren und interne Veröffentlichung erfolgt durch die Zentrale Universitätsverwaltung (Dezernat 1).
Es erfolgt eine generelle Kennzeichnung aller Endgeräte mit Stations- und Subdomainnamen in Abstimmung mit den entsprechenden Anschlussverantwortlichen. Bezüglich der Arbeitsplatzrechnernamen wurde im Jahr 2000 ein System der Namensgebung eingeführt, das neben Stationsnamen einen Identifikator für die jeweilige Struktureinheit enthält. Die Subdomainnamen werden ebenfalls schrittweise auf diese zentralen Struktureinheiten - Identifikatoren umgestellt. Alle am Netz autorisierten Endgeräte erhalten einen DNS-Namen und werden zentral erfasst.

- Bereitstellung eines Trouble Ticket System (TTS) durch das URZ

  Das URZ stellt den Anschlussverantwortlichen ein Trouble Ticket System bereit. Sie sind autorisiert für die Nutzung des Systems und die Einsicht in die Anschlussdokumentation.
  Aufträge aller Art die Konfiguration von Endgeräten am Netz betreffend (Adressen, Namen, Anschlussparameter, Dosenzuordnung, Umzugsvorbereitungen u. a.) sowie Störungs- und Fehlermeldungen werden von den Anschlussverantwortlichen in der Regel über das zentrale TTS mit Zugangsschnittstellen für WWW, in Ausnahmefällen über Mail oder Telefon an die zuständigen URZ – Bereiche erteilt. Das betrifft auch die Bearbeitung von Sicherheitsproblemen.

4. Maßnahmen zur Datensicherheit im Bereich der Netzübertragungstechnik

a) Organisatorische Maßnahmen

- Der Betrieb sowie die Administration des Netzes wird entsprechend der Verantwortlichkeiten zentral vom URZ wahrgenommen. Dies geschieht unter Zuhilfenahme verschiedener Netzmanagementsysteme.
- Der Betrieb von einrichtungseigener oder privater Netzübertragungstechnik (auch WLAN – Strukturen) am Netz der FSU Jena ist nicht gestattet. Ist eine Finanzierung durch eine Fakultät / Einrichtung erforderlich, so hat die Beschaffung in Abstimmung mit dem URZ zu geschehen, Installation und Betrieb erfolgt durch das URZ.
- Netzadressen werden durch das URZ vergeben und zentral verwaltet
- Anschlüsse für Endgeräte innerhalb dieser Netzstrukturen werden durch autorisierte Personen (Anschlussverantwortliche) auf Anforderung durch die jeweiligen Endgeräteverantwortliche beim URZ beantragt und durch das URZ realisiert und verwaltet.
- zentrale Registrierung aller Endgeräte im Zusammenhang mit Aktivierung entsprechender Zugangsschutzmaßnahmen mit dem Ziel, unbekannte Geräte und Adressen von der Netznutzung auszuschließen
- Unterbringung der Netzaktivtechnik in abgeschlossenen Datenverteilerräumen (betriebstechnische Räume), die nur dem URZ und dem Dezernat Betriebstechnische Dienste/Bauwesen zugänglich sind, wodurch die Technik gegenüber dem physischen Zugriff Unberechtigter weitgehend gesichert ist
- Betrieb eines universitätseigenen LWL-Netzes (dadurch besteht weitest gehende Unabhängigkeit von angemieteten Leitungen)
- Vermeidung der Inanspruchnahme von Fremddiensten

b) Regelungen für den Betrieb von Netzen

- Netzstrukturen (Subnetze/Teilnetze) werden nach Nutzergruppen unter Zuhilfenahme des zentral vorgegebenen strukturabbildenden Kostenstellenverzeichnisses (http://www.uni-jena.de/Kostenstellenverzeichnis.html) für die FSU Jena erstellt. Bei Nutzung gemeinsamer Ressourcen können im Bedarfsfall gemeinsame Netze gebildet werden. Sinnvoll ist dies immer dann, wenn aufgrund erhöhter Sicherheitsanforderungen der Einsatz einer gemeinsamen Firewallösung realisiert wird.
- Die Netze werden als virtuelle Netze (VLAN´s) realisiert und können sich somit bei Bedarf über mehre Standorte erstrecken. Dies ist ausschließlich bei allen Standorten mit dienstoffener Verkabelungsinfrastruktur möglich.

c) Regelungen für den Betrieb der Netzaktivtechnik

- Die Kopplung der Switchsysteme erfolgt mindestens im Distribution-Bereich unter Nutzung entsprechender Redundanz-Techniken über getrennte Lichtwellenleiterfasern (wenn durchführbar, auch über getrennte LWL-Kabel bzw. Kabeltrassen)
- Verwendung redundanter Netzteile
- Einsatz unterbrechungsfreier Stromversorgungen
- Wartungsverträge für die Aktivtechnik garantieren im Fall von Hardwarefehlern einen Austausch in angemessenen Fristen. Im URZ werden darüber hinaus entsprechend den finanziellen Möglichkeiten zusätzliche Ersatzteile vorgehalten
- die Datenübertragung erfolgt auf Basis dynamischer Routingverfahren mit dem Ziel der Nutzung von möglichen Ersatzpfaden beim Ausfall von Komponenten und zur Verringerung des Störungspotentials
- konsequente Nutzung der Wartungs- und Managementfunktionalitäten aller Netzwerkkomponenten stets unter Nutzung von Verschlüsselungstechniken und Berücksichtigung des Sicherheitsaspektes für autorisierte Mitarbeiter
- Überwachung der Datenströme zur Früherkennung von Problem- und Fehlersituationen durch autorisierte Mitarbeiter
- Analyse der Datenströme im Rahmen von Störungs- und Problembeseitigungen durch autorisierte Mitarbeiter sowie im Rahmen von Wartungsverträgen
- LWL-Strecken werden im Backbonebereich auch zur elektrischen Potentialtrennung zwischen den Standorten genutzt

d) Regelungen für den Betrieb der Endgeräteanschlüsse

- Einsatz geswitchter Anschlüsse für Endgeräte
- Nutzung von Sicherheitsmechanismen zur Verringerung des Angriffs- und Fehlerpotentials
- Nutzung von LWL-Technologien bis zum Arbeitsplatz bei technischer Notwendigkeit (z.B. im Bereich StorageAreaNetwork (SAN), im Bereich von Magnetfeldern)

e) Regelungen für den Betrieb von Filtern und Firewalls

- **Filter**
  Zentral erfolgt der Einsatz von Filterregeln am Anschluss zum WissenschaftsInformations-Netz (WIN) und damit am Übergang zum Internet
- **Firewall**
  Den Einrichtungsnetzen wird vom URZ der Betrieb zentraler stateful Firewallösungen angeboten und empfohlen

Die aktuellen Regelungen für Filter und Firewalls sind unter http://www.uni-jena.de/Firewall.html aufgeführt.

5. Empfehlungen zur Verbesserung der Datensicherheit für Endnutzer

Generell gilt, dass der Betreiber eines Endgerätes (Arbeitsplatzcomputer, Drucker,…) unabhängig von der Art des Gerätes die gesamte Verantwortung für dessen sicheren Betrieb trägt und bei durch den Betrieb entstandenen Schäden haftbar gemacht werden kann. Deshalb ist grundsätzlich eine qualifizierte Betreuung erforderlich.
Die Nutzung der Arbeitsplatzcomputer soll nur über einen autorisierten Zugriff erfolgen, um eine unberechtigte Benutzung auszuschließen.

Folgende Grundsätze sollten durch den Endnutzer eingehalten werden:

- Alle an das Datennetz der Universität anzuschließenden Rechner werden über die lokalen Anschlussverantwortlichen (https://tts.rz.uni-jena.de/tts/av/) im Rechenzentrum vor Inbetriebnahme angemeldet.
- Die Computer sollen nur mit vom Hersteller noch unterstützten Betriebssystemen und Anwendersoftware betrieben werden.
- Die auf diesen Rechnern installierten Betriebssysteme müssen durch regelmäßiges Einspielen von Updates und Patches aktuell und sicher gehalten werden.
- Die Anwendersoftware (Browser, Mailprogramme, sonstige Kommunikationssoftware) ist ebenfalls ständig auf einem aktuellen Stand zu halten. Es sollten nur die Komponenten installiert werden, die wirklich benötigt werden. Bei Bedarf werden Anschluss-verantwortliche bzw. deren Helfer Unterstützung geben.
- Die Rechner sind durch Installation von entsprechenden Schutzprogrammen (Virenscanner), die stets aktuell zu halten sind, vor Angriffen zu bewahren. Virenscanner werden vom Rechenzentrum im Rahmen von Hochschul- bzw. Landeslizenzen zum Download (http://www.uni-jena.de/Downloads.html) vorgehalten.
- Bei der Auswahl von Software, die sensible Daten verarbeitet (Passwörter, Kreditkartenkennungen usw.), sollte auf verschlüsselte Datenübertragung geachtet werden (SSL – Web – Server, Secure Shell Client, ...).
- Obwohl die Computer der FSU durch zentrale Firewalls geschützt sind, sollen die Endgeräte durch eigene Firewalls mit einer den speziellen Bedürfnissen entsprechenden Konfiguration zusätzlich gesichert werden.
- Ein ganz wichtiger Punkt ist der Umgang mit den Passworten. Sie sollen schwer zu erraten, aber für den Eigentümer merkbar sein. Vor allem dürfen sie nicht aufgeschrieben und sichtbar hinterlegt werden. Bei der Auswahl eines Passwortes sollte bedacht werden:
    - es sind nur die ersten 8 Zeichen signifikant
    - keine Worte oder Begriffe wählen, die in Wörterbüchern u.Ä. zu finden sind (deutsch, englisch, französisch...)
    - keine Zeichenketten wählen, die aus der Persönlichkeit des Nutzers abgeleitet werden können (Geburtstag,…)
    - gemischte Verwendung aller möglichen Zeichen (Groß/Kleinbuchstaben, Ziffern, Sonderzeichen soweit möglich)
    - neu zugeteilte Passwörter sofort ändern
    - Vorschlag: Ein Satz, von jedem Wort der erste Buchstabe: ESvjWd1B

  Wenn diese wenigen und einfachen Regeln beachtet werden, ist es praktisch nahezu unmöglich, ein Passwort auch mit programmtechnischen Mitteln zu erraten.

Werden durch einen Rechner verursachte Schäden bekannt, wird der AV durch das URZ informiert. Wenn die Ursachen nicht in vom URZ vorgegebenen von der Schwere der Fehlerfolgen abhängigen Fristen beseitigt werden, wird der Rechner vom Datennetz getrennt. Das URZ benennt einen Verantwortlichen für Sicherheitsfragen, der bei Problemen zu kontaktieren ist. Der Name des Ansprechpartners ist der Sicherheitsseite (http://www.uni-jena.de/URZ_Sicherheit.html) des URZ zu entnehmen.
Er betreut die entsprechenden Seiten mit sicherheitsrelevanten Hinweisen und sorgt dafür, dass bei akuten Vorkommnissen Informationen auf diesen Webseiten sowie über die Mailingliste security – l bereitgestellt werden.

Dr. Olaf Götz
Komm. Leiter.
Universitätsrechenzentrum

Jena, 09.November 2007

Anhang

Um Klarheit darüber zu schaffen, in welchem Sinn sicherheitsrelevante Begriffe verwendet werden, folgt hier eine Liste von Begriffen und ihrer Bedeutung.

Informationen sind Daten, denen bestimmte Attribute wie Autor, Erstellungsdatum, Gültigkeitsdauer, etc. zugeordnet werden können

Datensicherheit bezeichnet die Bewahrung der Daten vor ungewollter Beeinträchtigung und bildet eine Voraussetzung für den Datenschutz. Datensicherheit unterteilt sich in die Bereiche:

Vertraulichkeit

Schutz der Daten/Informationen vor unberechtigtem Zugriff

Verfügbarkeit

Zum geforderten Zeitpunkt stehen dem berechtigtem Nutzer entsprechende Dienstleistungen, Funktionen der IT-Systeme sowie Daten/Informationen zur Verfügung.

Integrität

Die Integrität ist gewährleistet, wenn die Daten/Informationen vollständig und unverändert sind.

Datensicherung bezeichnet die Erstellung von Sicherheitskopien der Daten/Informationen zum Schutz vor Verlust

Datenschutz bezeichnet den Schutz von Daten/Informationen mit Bezug zu natürlichen Personen vor dem unberechtigtem Zugriff durch Dritte (siehe Bundesdatenschutzgesetz BDSG)

Authentisierung bezeichnet die Überprüfung der Identität.

Autorisierung bezeichnet den Vorgang der Überprüfung der Berechtigung zur Durchführung einer bestimmten Aktion.

Datennetz wird aus Netzübertragungstechnik und Endgeräten gebildet. Es bestehen Übergänge zu weiteren Datennetzen.

Netzübertragungstechnik besteht aus passiven Komponenten (Verkabelung) und aktiven Komponenten (Netzaktivtechnik) und dient der Übertragung von Daten/Informationen.

Datenverteiler (DV) sind betriebstechnische Räume in den Standorten der FSU Jena zum Auflegen der Inhouse -Verkabelung sowie zur Unterbringung der Netzaktivtechnik.

Verkabelung unterteilt sich in die Bereiche:

Primärverkabelung

Verkabelung zwischen einzelnen Standorten (i.d.R. auf Basis von Lichtwellenleiterkabeln (LWL-Verkabelung))

Sekundärverkabelung

Verkabelung zwischen den Datenverteilern eines Standortes (i.d.R. ebenfalls auf Basis von Lichtwellenleiterkabeln (LWL-Verkabelung))

Tertiärverkabelung

Verkabelung zwischen einem Datenverteiler und den Anschlussdosen in den einzelnen Räumen eines Standortes als Inhouse - Verkabelung auf Basis einer dienstoffenen, strukturierten Kupferverkabelung nach Kategorie 5/ Klasse E oder höherwertig. Historisch bedingt bestehen daneben teilweise noch Verkabelungen auf Basis von Koaxialkabeln RG58.