Ausführungsbestimmungen zur Net-Policy der UHH (erlassen vom Direktor des RRZ am 21.08.2007)

Einleitung

Auf Grundlage von Nr. 2.3 der Net-Policy vom 19.01.2005 erfolgen mit diesem Papier die ersten Konkretisierungen zur Umsetzung der Richtlinien. Zur Strukturierung dieser Richtlinien werden vier Bereiche unterschieden:

1. Personal
2. Endgerätesicherheit
3. Netzkomponenten
4. Dienste

Personal

Es wird davon ausgegangen, dass der IT-Betrieb an der UHH in einer verteilten Form umgesetzt wird. Die zentrale Verantwortung liegt beim RRZ, das Teilaufgaben an Institutionen übertragen kann. Für die Wahrnehmung dieser Teilaufgaben müssen die Institutionen entsprechend qualifiziertes Personal abstellen. Nur so ist es möglich, die hohen Anforderungen an eine sichere IT-Infrastruktur zu erfüllen. Für diese Personen --- im Folgenden Administratoren genannt --- gilt:

1. Diese Administratoren sollten durch die Institutionen dem RRZ benannt werden (offizielle Ansprechpartner).
2. Sie sollten IT-Verantwortungsbereichen in den Institutionen zugeordnet werden (für welche Betriebssysteme, IP-Adressbereiche, Geräteklassen, Dienste zuständig?).
3. Die Administratoren müssen über entsprechende Kenntnisse und Qualifikationen verfügen; eine ständige Fortbildung ist erforderlich.
4. Es besteht die Verpflichtung zur Teilnahme am Informationsaustausch zum Aufgabenbereich (Arbeitstreffen, Verteilerlisten, usw. werden vom RRZ koordiniert).

Aufgrund der Notwendigkeit, Dienste für Forschung, Lehre und Verwaltung mit besonderen Datenschutzanforderungen, Netzsicherheitsanforderungen und Dienstqualitätsanforderungen UHH-übergreifend anzubieten, ist es erforderlich für das RRZ, die Verantwortung für das UHH-Netz und die Richtlinienkompetenz in seiner Funktion/ Rolle als Netzbetreiber eindeutig festzulegen.

Mit dieser Ausführungsbestimmung wird die in der Net-Policy verankerte zentrale fachliche Hoheit der Netzgruppe des RRZ bezüglich des UHH-Netzes dahingehend konkretisiert, dass dem Direktor des RRZ auch die technischen, prozessorientierten und organisatorischen Durchgriffsmöglichkeiten eingeräumt werden, um den Netz-/Datenschutzverpflichtungen und den damit verbundenen Berichtspflichten nachkommen zu können.

Endgerätesicherheit

Ziel ist der Betrieb von ausschließlich sicheren Endgeräten am Netz der UHH. Daher sollen Endgeräte ausschließlich durch hierfür qualifizierte Administratoren (s.o.) verwaltet werden (nicht durch Endnutzer).

1. Folgende Verfahren und Mindestanforderungen gelten für stationäre Endgeräte:
    1. Betriebssysteme: Es sollten nur Betriebssysteme verwendet werden, die von den jeweiligen Herstellern mit offiziellen (Sicherheits-)“Patches“ versorgt werden. Die Betriebssysteme sollten mit diesen „Patches“ regelmäßig aktualisiert werden.
    2. Virenschutz: Es muss grundsätzlich ein aktueller Virenscanner mit automatischer Aktualisierung eingesetzt werden; das RRZ bietet zurzeit eine uniweite Campuslizenz für den Sophos-Virenscanner.
    3. Personal Firewall: Die Endgeräte sollten durch eine „personal firewall software“ derart geschützt werden, dass nur vom Administrator explizit freigegebene Dienste und Verbindungen verwendet werden können. Ein minimaler Satz von Filterregeln wird vom RRZ vorgegeben, um Betriebsstörungen durch „personal firewall software“ auszuschließen. Insbesondere müssen ans Netz angeschlossene Rechner auf ICMP-Echo-Requests antworten. Es wird empfohlen, die im Betriebssystem integrierten Firewall-Funktionen zu verwenden.
    4. IP-Registrierung: Grundsätzlich dürfen nur Geräte am UHH-Netz angeschlossen werden, die beim RRZ oder bei vom RRZ hierfür Beauftragte mit ihren IP- und MAC-Adressen registriert sind.
    5. Rechner, die durch Störungen des Netzbetriebs oder andere Vorfälle auffallen, werden gesperrt und müssen von den Administratoren untersucht und repariert werden, bevor sie wieder am Netz der UHH freigeschaltet werden.

2. Die oben genannten Verfahren gelten ebenso für mobile Endgeräte.

3. Der Betrieb von privaten Notebooks am Netz der UHH ist außerhalb der hierfür explizit vorgesehenen Netze nur gestattet, wenn
    1. der/die Benutzer/in sich bereit erklärt, den Anordnungen der Administratoren in allen Belangen des IT-Betriebs zu folgen, auch bzw. insbesondere wenn die Sicherheit des IT-Betriebs durch das private Gerät beeinträchtigt werden könnte.
    2. Zusätzlich gelten die Regelungen aus „Private Notebooks am Netz der UHH“.

4. Bei der Beschaffung von Endgeräten und Software, die nicht dem Standard entsprechen und Sicherheitsbelange berühren, ist eine Absprache mit dem RRZ erforderlich.

Netzkomponenten

Für den Netzbetrieb gelten die folgenden Regeln:

1. Grundsätzlich dürfen Netzkomponenten nur vom RRZ oder durch vom RRZ beauftragte Administratoren in das Netz der UHH integriert werden.
2. Insbesondere dürfen keinerlei aktive Netzkomponenten zur Einwahl in das Netz der UHH (z.B. WLAN-Access Points, Modem- und ISDN-Geräte, VPN-Geräte) von nicht autorisierten Personen betrieben werden.
3. Sicherheitskomponenten (NAT, Firewall, VPN….) werden auf Antrag vom RRZ bereitgestellt und ggf. betrieben. In Ausnahmefällen kann bei begründetem Antrag eine spezielle Komponente nach Vorgaben/in Absprache mit/des RRZ durch einen Administrator betrieben werden.
4. Bei Beschaffungen von Netzkomponenten durch vom RRZ beauftragte

Administratoren ist eine vorherige Absprache/Abstimmung mit dem RRZ dringend empfohlen (Ziel ist es, eine möglichst kostengünstige (Rahmenverträge) und betriebssichere IT-Infrastruktur für die UHH zu schaffen).

Dienste

Der Zugriff auf IT-Ressourcen der UHH darf nur vom RRZ oder vom RRZ autorisierte Institutionen freigegeben werden.

- Insbesondere ist der Betrieb von Netzbasisdiensten (DNS, DHCP, Radius) ausschließlich durch Administratoren und nach Genehmigung durch das RRZ erlaubt.
- Für die essentiellen Kommunikationsdienste (WWW, E-Mail, FTP, usw.) sollten möglichst zentrale Lösungen angestrebt werden.

Durch dieses Antragsverfahren wird sichergestellt, dass es zu keinen Betriebsstörungen durch unkoordinierte Betriebsmodelle kommt und im Fehlerfall die Zuständigkeiten offen liegen.

Autor: Netzgruppe, Stand: 22.08.2007