

Universität Hannover, Postfach 60 09, 30060 Hannover

Das Präsidium

Der zentrale IT-Sicherheitsbeauftragte

bearbeitet von:

Herrn Harnisch

Tel + 49(0)511.7 62-79 46 63

Fax + 49(0)511.7 62-30 03

e-mail: **harnisch****@rrzn.uni-hannover.de****Rundschreiben A Nr. 35/2005**Universitätseinrichtungen
gem. Verteiler 1 2 3 4 5hier**27.10.2005**

Mein Zeichen:

02031-1-2

(bitte bei Antwort angeben)

Ihre Nachricht vom:

Ihr Zeichen:

Vermeidung von Schadsoftware auf Rechnern im Netz der Universität Hannover

Durch den Befall von Rechnern mit Schadsoftware (d. h. Virus, Wurm oder Trojaner) drohen u. a. der Verlust, die Manipulation und der Diebstahl von Daten und die Zweckentfremdung der Rechner zum rechtswidrigen Gebrauch. Zur Vermeidung von Arbeitsaufwand, Kosten und rechtlichen Problemen sowie von Unterbrechungen und Störungen in der Nutzung von informationstechnischen Anlagen sind die Rechner, die im Netz der Universität betrieben werden, vor Schadsoftware und ihren Auswirkungen zu schützen. Da die Informationstechnik einem ständigen Wandel unterliegt, sind die Schutzmaßnahmen immer wieder zu überprüfen und neueren Gegebenheiten anzupassen. Derzeit sind die im Folgenden beschriebenen Maßnahmen empfehlenswert bzw. zu ergreifen.

Antivirensoftware

Daten und Programme müssen auf Viren untersucht werden, um den Rechner vor Virenbefall zu schützen und eine weitere Verbreitung von Schadsoftware zu verhindern. Zwar werden ein- und ausgehende E-Mails, die die zentralen Mailserver durchlaufen, auf Viren untersucht, es gibt aber weitere Infektionswege: Ein Rechner kann z. B. über Programme oder Daten aus dem Internet, Abruf von E-Mail aus anderer Quelle über Webmail oder durch Datenträger infiziert werden. Eine besondere Gefährdung besteht für Notebooks, die auch außerhalb des Universitätsnetzes betrieben werden. Daher ist auf jedem Rechner eine ständig aktualisierte Antivirensoftware einzusetzen. Für Microsoft-Windows bietet das RRZN die für die Einrichtungen und Angehörigen der Universität kostenfreie Software von Sophos mit automatischem Update an, vgl.

<http://www.rrzn.uni-hannover.de/sru.html>.

Firewall

Beim Anschluss des Computernetzes einer Einrichtung oder eines Standortes an das Netz der Universität empfiehlt sich der Einsatz einer Firewall, die die Zugriffsmöglichkeiten in beide Richtungen auf das nötige Maß beschränkt. Für die Institute besteht dabei die Möglichkeit, ihre

Der zentrale

IT-Sicherheitsbeauftragte

Prof. Dr. M. Breitner

Institut für Wirtschaftsinformatik

Dienstgebäude

Königsworther Platz 1

30159 Hannover

Stadtbahnlinie 4 und 5

Haltestelle Königsworther Platz

Tel + 49(0)511.7 62-49 78

Fax + 49(0)511.7 62-40 13

www.iwi.uni-hannover.de

Netzwerke hinter eine vom RRZN bereitgestellte und individuell konfigurierte Firewall schalten zu lassen, auch der Einsatz einer einrichtungseigenen Firewall ist möglich. Näheres dazu unter

<http://www.rrzn.uni-hannover.de/netzschutz.html>.

Als zusätzliche Maßnahme ist die Absicherung jedes einzelnen Rechners mit einer in Software implementierten so genannten Personal Firewall ratsam. Derzeit bereitet das RRZN eine eindeutige Produktempfehlung vor, mehr Informationen bietet

www.rrzn.uni-hannover.de/fw_produkte.html.

Softwareaktualisierung

Betriebssysteme und Anwendersoftware sind nicht fehlerfrei, weshalb immer wieder Sicherheitslücken darin entdeckt werden. Eingesetzte Software muss durch das Verfolgen von Warnmeldungen und das Einspielen von Korrekturen (Patches) daher regelmäßig gegen das Ausnutzen bekannt gewordener Probleme abgesichert werden. So ein auch als Update bezeichnetes Verfahren kann zum Teil automatisiert erfolgen und wird z. B. vom RRZN für Microsoft-Windows 2000, XP und Server 2003 angeboten:

http://www.rrzn.uni-hannover.de/its_sus.html.

Aktualisierung kann auch bedeuten, dass die Software als Ganzes, z. B. gegen eine neuere Version, ausgetauscht werden muss, wenn der Hersteller die Unterstützung durch Sicherheitsupdates einstellt. Beispiele hierfür sind u. a. im Rundschreiben A Nr. 34/2005 (Migration von Betriebssystemen Windows NT und Windows 2000) zu finden.

Anwenderverhalten

Neben den oben beschriebenen technischen Maßnahmen ist ein verantwortungsvolles Verhalten der Anwender unerlässlich. Auf die Verwendung von Dateien und Programmen sowie den Aufruf von Internet-Seiten und E-Mail-Anhängen sollte verzichtet werden, wenn die Quelle als nicht vertrauenswürdig erscheint. Von Daten ist regelmäßig in geeigneter Weise eine Sicherungskopie anzulegen, und der Zugriff auf personenbezogene Daten ist zusätzlich zu beschränken und zu kontrollieren, um die etwaigen Auswirkungen von Schadsoftware zu begrenzen.

Neben diesen Schutzmaßnahmen sei auch auf § 15 (3) und (7) sowie § 16 der vorläufigen Netzbetriebsordnung für das allgemeine Datenkommunikationsnetz der Universität Hannover und § 7 (1) und (2) des Niedersächsischen Datenschutzgesetzes (NDSG) hingewiesen. Nähere Informationen zu den angesprochenen Themen und Maßnahmen sind einer RRZN-Broschüre zur IT-Sicherheit und in ausführlicherer und fortlaufend aktualisierter Form den Webseiten des RRZN zur IT-Sicherheit zu entnehmen:

http://www.rrzn.uni-hannover.de/it_sicherheit.html

Im Auftrage

gez. Breitner