

IT-Sicherheit



R | R | Z | N |

Regionales Rechenzentrum für Niedersachsen

Kennen Sie die Gefahren aus dem Netz?

Sicherheitslücken ermöglichen dem Hacker die Kontrolle über Ihr System und eröffnen ihm weitreichende Eingriffsmöglichkeiten, wie

- ➡ unberechtigten Zugriff auf vertrauliche Daten,
- ➡ Beteiligung Ihres Computers an einem Distributed-Denial-of-Service Angriff (DDoS) im Verbund mit anderen Bots (zentral kommandierte, ferngesteuerte Systeme),
- ➡ Einrichten einer Tauschbörse für illegales Datenmaterial,
- ➡ Starten weltweiter Angriffe, die nun von Ihrem Rechner ausgehen, unter Tarnung der wahren Hacker-Identität!
- ➡ Außerdem kann Ihr Rechner als Ankerpunkt im Netz der Universität dazu missbraucht werden, gut geschützte Systeme aus dieser internen Position heraus gezielt anzugreifen. So erreicht der Eindringling nun Rechner, die den Zugriff nur für das interne LUH-Netz erlauben.

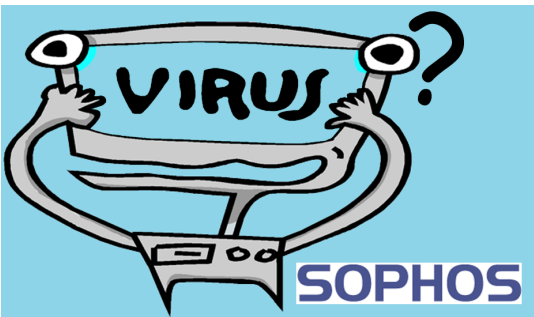


Schützen Sie Ihren Computer!

1 Antivirensoftware installieren und regelmäßig aktualisieren!

Im Rahmen einer Landeslizenz steht der Leibniz Universität Hannover die Antivirensoftware von Sophos zur Verfügung. Das Programm kann kostenlos von Mitarbeitern und Studierenden auf universitätseigenen Rechnern und privat genutzt werden. Programm und automatische Updates werden für die Betriebssysteme Windows 98/ME/NT4, Windows 2000/XP/2003/Vista, Mac OS-X und Linux angeboten.

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



2 Sicherheitskorrekturen (Patches und Service-Packs) für Betriebssystem und Software unbedingt installieren!

Bleiben Sie bei allen Aktualisierungen für Betriebssystem (z. B. Windows, Linux) und Anwendungen (z. B. Acrobat Reader, Mozilla Firefox) auf dem Laufenden!

Mit dem Software-Update-Service (WSUS) des RRZN können Sie Ihr Windows-Betriebssystem und Microsoft-Office auf einfache Weise aktuell halten.

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



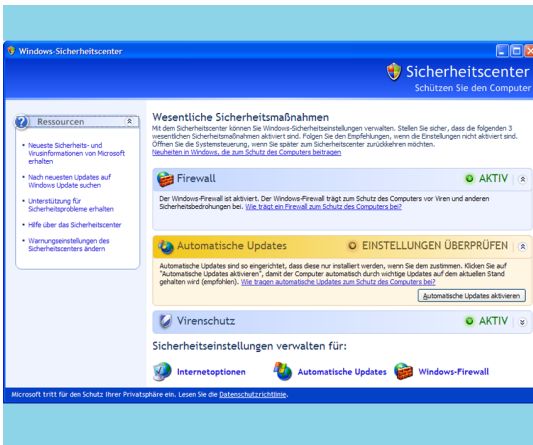
3 Einsatz einer Personal Firewall zur Kontrolle des Datenverkehrs!

Eine Personal Firewall auf Ihrem Rechner erschwert es einem Eindringling, Ihren Computer zu kontaktieren und zu missbrauchen.

Die in Windows XP/Vista mitgelieferte Personal Firewall ist im Sicherheitscenter des Betriebssystems integriert und standardmäßig aktiv.

Ausführliche Informationen dazu und zu anderen Firewall-Lösungen finden Sie unter:

http://www.rzrn.uni-hannover.de/its_p_firewall.html



4 Ins Internet nur mit eingeschränkten Benutzerrechten!

Vermeiden Sie das Arbeiten mit Administratorrechten und melden Sie sich stattdessen nur als Benutzer an. Die Administrator-Option sollten Sie nur dann nutzen, wenn Sie tatsächlich Änderungen am System vornehmen oder neue Programme installieren wollen.

5 Achten Sie auf die Qualität Ihrer Passwörter!

Passwörter sind schwerer zu knacken, wenn bei mindestens acht Zeichen keine Wörter aus Wörterbüchern (auch Fremdsprachen) und keine persönlichen Daten verwendet werden.

Leichter zu merken sind sie mit „Eselsbrücken“, wie Anfangsbuchstaben von Merksätzen oder Liedzeilen unter Beigabe von Zahlen und Sonderzeichen.

Ein Beispiel:

U8!mizAg (Um 8! muss ich zur Arbeit gehen)

Oder aber:

H+Gv!siW (Hänsel und Gretel verlieben! sich im Wald)

Hinweis: Nicht ein und dasselbe Passwort universell für alle Zugänge und Anwendungen einsetzen!

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

Weitere RRZN-Dienste

Funkvernetzung (WLAN)

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

VPN-Nutzung

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

Signieren und Verschlüsseln von E-Mail

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



RRZN-Informationen und Ressourcen im Netz

Unser Informationsangebot zur IT-Sicherheit finden Sie im Netz unter der Adresse

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

Es lohnt sich auch ein regelmäßiger Blick auf die Homepage des RRZN. Hier erhalten Sie einen Überblick über das gesamte Dienstleistungs- und Informationsangebot des RRZN. In den News-Meldungen wird aktuell auf gravierende Sicherheitsprobleme hingewiesen.

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

The screenshot shows the homepage of the Regionales Rechenzentrum für Niedersachsen (RRZN) at Leibniz Universität Hannover. The page features a navigation menu with links for 'A-Z', 'Hotline', 'Kontakt', 'Sitemap', and 'Intern'. A central pop-up window titled 'IT-Sicherheit' lists 'Risiken & Maßnahmen', 'Ernstfall', 'Serviceangebote', 'ITS-Publikationen', and 'CERTs/Links'. The main content area is organized into several columns: 'Betriebsmeldung' (with dates and links for SAP systems, handbooks, and Acrobat/Word), 'Netzbetrieb' (with dates and links for network services), 'Kurse' (with dates and links for Windows Vista, Office 2007, and Acrobat 8), 'Organisation' (with links for 'Über uns', 'Mitarbeiter', 'Nutzungsregeln', 'Stellenangebote', and 'Dienstleistungen'), 'Netz' (with links for 'Datennetz', 'Mail-Service', 'Netzdienste', and 'Netzzugang'), 'Arbeitsplatzrechner' (with links for 'PC/Workstation', 'Server', 'Anwendersoftware', 'Software-Info DB', and 'Gerätebeschaffung'), 'Angebote' (with links for 'Handbücher', 'Kurse', 'Druckausgabe', 'Softwareverteilung', and 'Verkauf & Verleih'), and 'Multimedia' (with links for 'Audio/Video', '3D/Visualisierung', 'Digital Imaging', 'E-Learning', and 'TYPO3'). On the right side, there is a search bar, a 'Suchmaschinenlabor' logo, and a 'Microsoft Vista Business' logo.

„Kennen Sie die Gefahren aus dem Netz?“

Wichtige Hinweise zum sicheren Betrieb von Rechnern im Netz der LUH

Regionales Rechenzentrum für Niedersachsen
Leibniz Universität Hannover
D-30159 Hannover

Telefon 05 11/7 62-28 83

Telefax 05 11/7 62-30 03

E-Mail security@rrzn.uni-hannover.de

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