Leibniz Universität Hannover

# Sicherheitstage

im Wintersemester 2011/2012

21./22. November 2011

Die Sicherheitstage werden am 21. und 22. November 2011 (Montag und Dienstag) vormittags im Gebäude 1210, Schloßwender Straße 5 in Hannover stattfinden.

Die Sicherheitstage sollen zu einigen Sicherheitsthemen in der Administration einen tieferen Einblick geben. Zudem sollen die Vormittage Gelegenheit zum Gespräch und Erfahrungsaustausch bieten, auch zu unseren Serviceleistungen.

Die Sicherheitstage richten sich in erster Linie an Administratoren sowie die IT-Sicherheitsbeauftragten der Fakultäten und zentralen Einrichtungen der Leibniz Universität Hannover. Dabei sollen auch Mitarbeiter, die die Computerverwaltung als zusätzliche Aufgabe ausüben, und studentische Hilfskräfte, die mit IT-Aufgaben betraut sind, angesprochen werden.

## Anmeldung

Sie können sich ab dem 7. November für die Sicherheitstage anmelden. Die Anmeldung erfolgt wie bei anderen Kursen online. Näheres dazu finden Sie unter `https://www.rrzn.uni-hannover.de/organisatorisches.html`. Die Anmeldung erfolgt dabei zwar für beide Vormittage, bitte melden Sie sich aber auch dann an, wenn Sie nur an einigen Vorträgen teilnehmen wollen.

Die Plätze werden bevorzugt an Teilnehmer aus der Leibniz Universität Hannover vergeben, externe Teilnehmer anderer Hochschulen sind aber willkommen. Bei Anmeldeproblemen wenden Sie sich bitte (bevorzugt per E-Mail) an uns: `http://www.rrzn.uni-hannover.de/kontakt.html`.

Leibniz Universität Hannover

## Terminplan

| Montag, 21.11.2011 | Dienstag, 22.11.2011 |
|---|---|
| 09:15–09:45 **IT-Reorg-Umsetzungsprojekt** G. von Voigt | 09:15–10:00 **Archiv und Backup** A. Gerdes |
| 09:45–10:45 **Aktuelle Sicherheitslage** H. Harnisch | 10:00-10:45 **Web-Single-Sign-On** S. Klopp |
| 10:45–11:15 Pause | 10:45–11:15 Pause |
| 11:15–12:00 **Sophos** H. Harnisch | 11:15–12:15 **Datenspuren im Netz** H. G. Krojanski |
| 12:00–12:45 **Mac OS X Firewall** M. Heisterkamp | 12:15–12:45 **Diskussion** |

## Vorträge

Die Vorträge finden wie gewohnt im Seminarraum des Gebäudes 1210 statt.

### IT-Reorg-Umsetzungsprojekt

Ein Überblick über die Umsetzung des IT-Reorganisationsprojekts an der Leibniz Universität Hannover: Hintergrund, Planung, Absichten und geschätzte Auswirkungen auf die tägliche Arbeit.

### Sophos Antivirus

Am Anfang des Jahres gab es einen Release-Wechsel in der an der Universität eingesetzten Windows-Version der Antiviren-Software Sophos. Dabei haben sich nicht nur die Update-Pfade geändert, sondern wir haben auch die Verwaltbarkeit von Client-Installationen und die SNMP-Signalisierung von Fehlern und Malware-Funden eingeführt. Dieser Vortrag soll einen Überblick über die Technik dahinter und die sich dadurch eröffnenden Möglichkeiten geben.

## Neue (Applikation-)Firewall unter Mac OS X Lion

Mit Erscheinen von Mac OS X Lion hat Apple ein dort neues Firewall-Werkzeug namens *pfctl* für den ebenfalls in Mac OS 10.7 neuen Paketfilter *pf*, der von OpenBSD portiert wurde, eingeführt. Die alte Firewall *ipfw* wird von Apple als deprecated eingestuft.

Die bekannte GUI-gesteuerte Applikation-Firewall ist ebenfalls überarbeitet worden.

Zu beiden Themen wird ein kurzer Überblick bezüglich Bedienung und Möglichkeiten gegeben.

## Archiv & Backup als Services

In diesem Vortrag soll die Datensicherheit im Vordergrund stehen. Wie schütze ich mich vor Datenverlust? Wie kann der zentrale Dienstleister der Leibniz Universität Hannover dabei helfen? Welche Datenmengen sind für ein Backup sinnvoll und noch pragmatisch? Welche Daten sollten statt dessen ins Archiv aufgenommen werden?

Anhand des Backup-Tools *Time Navigator* der Firma Atempo, welches die alte Backupsoftware Symantec *NetBackup* ersetzen wird, werden die Möglichkeiten der Datensicherung aufgezeigt. Was ändert sich zum früheren Vorgehen an der LUH? Und wie lässt sich der Backup-Prozess mit Zertifikaten noch sicherer gestalten?

## Web-Single-Sign-On mit Shibboleth und OpenID an der LUH

Das IdM betreibt seit einiger Zeit einen Shibboleth- und OpenID-Identitätsprovider. Registrierte Benutzer können sich darüber authentifizieren, um Zugriff auf angebundene Webanwendungen zu erhalten. Der Vortrag richtet sich an Webseiten-Betreiber, die für ihre Anwendungen eines dieser WebSSO-Verfahren einsetzen wollen. Es werden die technischen Voraussetzungen sowie Vor- und Nachteile der jeweiligen Systeme erläutert.

## Datenspuren im Netz

Ziel dieses Vortrags ist es, ein Bewusstsein zu schaffen, wie viele Informationen beim alltäglichen Umgang mit dem Computer preisgegeben werden. Dies kann absichtlich durch die Anmeldung bei Suchmaschinen oder sozialen Netzwerken geschehen, aber auch unabsichtlich durch Cookies und ähnliche Techniken. Selbst wenn beides vermieden wird, können dennoch Benutzer heimlich über ihre *Fingerabdrücke* wiedererkannt werden. Es werden einige Beispiele diskutiert, auf welche Weise Datenspuren im Netz hinterlassen werden, mögliche Folgen angesprochen und Gegenmaßnahmen vorgestellt. Dabei wird auch angesprochen, was man als Administrator einer Vielzahl von PCs oder einer Webseite unternehmen kann.

# Anfahrt

Details zur Anfahrt können Sie unserer Webseite `http://www.rrzn.uni-hannover.de/anfahrt.html` entnehmen. Sie kommen zum Seminarraum über den Hof (Eingang mit der Nummer 4), oder über den neuen Haupteingang (mit 2 bezeichnet) innerhalb des Hauses.