

# Sicherheitstage

im Wintersemester 2012/2013

19./20. November 2012

Die Sicherheitstage werden am 19. und 20. November 2012 (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 sofort 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/sicherheitsteam.html>.

## Terminplan

Montag, 19.11.2012	Dienstag, 20.11.2012
09:15–10:00 <b>Aktuelle Sicherheitslage</b> H. Harnisch	09:15–10:30 <b>Physische IT-Sicherheit</b> H. G. Krojanski
10:00–11:00 <b>Sicherheit von Webanwendungen</b> W. Börger	10:30–11:00 <b>Sicherheitslage von mobilen Apps</b> S. Fahl
11:00–11:30 Pause	11:00–11:30 Pause
11:30–12:15 <b>FileVault 2</b> M. Heisterkamp	11:30–12:15 <b>Neue SPAM- und Virenabwehr</b> M. Heisterkamp, H. Harnisch
12:15–13:00 <b>Sophos Antivirus</b> H. Harnisch	12:15–13:00 <b>Diskussion</b>

## Vorträge

Die Vorträge finden wie gewohnt im Seminarraum des Rechenzentrums (Geb. 1210) statt.

### Aktuelle Sicherheitslage

Es wird ein kurzer Überblick der derzeitigen Bedrohungslage und ihrer Veränderung gegeben. Insbesondere auch die sich durch Cloud und Smartphones neu ergebenden Fragestellungen werden angerissen.

### Sicherheit von Webanwendungen

Webanwendungen sind aus dem Alltag nicht mehr wegzudenken und immer mehr Anwendungen und Informationen werden über das Internet zugänglich gemacht. An Sicherheit wird dabei häufig nicht gedacht, und gerade selbst geschriebene Anwendungen weisen oft gravierende Sicherheitslücken auf. Dieser Vortrag gibt einen Überblick über mögliche Schwachstellen in Webanwendungen und zeigt, wie diese vermieden werden können.

### FileVault 2

Mac OS X bietet mit FileVault schon seit mehreren Jahren eine Möglichkeit zum Verschlüsseln von persönlichen Daten. Mit der Version 10.7 (*Lion*) wurde eine neue Version von FileVault eingeführt. Während die erste Version von FileVault nur die einzelnen Benutzerverzeichnisse verschlüsseln konnte, kann mit FileVault 2 die gesamte Festplatte verschlüsselt

werden. Der Vortrag beschäftigt sich mit der Einrichtung und Konfiguration von FileVault 2 und stellt technische Details dieser Festplattenverschlüsselung vor.

## Sophos Antivirus

Mit dem Release-Wechsel Anfang 2011 der an der Universität eingesetzten Windows-Version der Antiviren-Software Sophos wurde auch die durch das Rechenzentrum betriebene Serverstruktur und die Updatekonfiguration geändert. Dabei haben sich nicht nur die Update-Pfade verändert, 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.

## Physische IT-Sicherheit

Unter dem Begriff physische IT-Sicherheit werden Gefährdungen diskutiert, die durch unmittelbare Einwirkung auf Computersysteme entstehen. In diesem Vortrag werden Beispiele gezeigt, die für den Betrieb von IT-Systemen (Notebooks bis Server) an der Universität relevant sind und geeignete Maßnahmen vorgestellt.

## Sicherheitslage von mobilen Apps

In den letzten Jahren erfreuen sich mobile Geräte wie Smartphones und Tablets immer größerer Beliebtheit. Benutzer nehmen sie überall mit hin, um online zu sein oder zu spielen. Mit dem Aufkommen von mobilen Geräten begann das Phänomen der Appification. Während auf herkömmlichen Desktopsystemen der Browser das Universalwerkzeug für den Internetzugriff darstellt, existieren auf mobilen Plattformen wie Android und iOS für so gut wie jeden Online Service eigene Applikationen – so genannte Apps. Forschungsarbeiten der jungen Vergangenheit haben gezeigt, dass Apps mit Malware zu kämpfen haben, problematische Sicherheitskonfigurationen vornehmen oder anderweitig Daten von Nutzern gefährden können. Dieser Vortrag gibt einen Überblick über die aktuelle Sicherheitslage von mobilen Apps auf Android- und iOS-Geräten und wird basierend darauf Handlungsvorschläge für Nutzer mobiler Geräte geben.

## Neue SPAM- und Virenabwehr

Im September und Oktober dieses Jahres wurde die Spam- und Virenabwehr im Mailempfang für die Universität umgestellt. Das neue Setup und damit einhergehende Änderungen werden dargestellt und erläutert. Über die konkrete Ausgestaltung der neuen Mailfilterung hinaus werden weitere Vorgehensweisen, Probleme und Empfehlungen im Umgang mit Mail angesprochen.

## 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.

