Leibniz Universität Hannover

R|R|Z|N

Sicherheitstage

im Wintersemester 2010

18./19. Januar 2009

Die Sicherheitstage werden am 18. und 19. Januar 2010 (Montag und Dienstag) vormittags im RRZN, 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 Serviceleistungen des RRZN.

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 des RRZN 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`.

Terminplan

Montag, 18.01.10	Dienstag, 19.01.10
09:15–10:45 **Booten in x86-Architekturen** H. Harnisch	09:15–10:15 **Passwörter** H. Harnisch 10:15–10:45 **Passwortmanager KeePass** B. Gersbeck-Schierholz
10:45–11:15 Pause	10:45–11:15 Pause
11:15–12:45 **Linux im Active-Directory** R. Euhus	11:15–12:15 **SSH** H. Harnisch 12:15–12:45 **Diskussion** H. Harnisch

Vorträge

Die Vorträge finden wie gewohnt im Seminarraum des RRZN statt.

Booten in x86-Architekturen

Im Zuge von Software-Updates und Hardware-Umbauten kann es leicht zu einem nicht mehr bootenden System kommen. Ebenso gibt es manchmal Probleme mit der Boot-Reihenfolge, wenn viele Geräte an einem Server angeschlossen sind. Für die Behebung der Probleme ohne komplette Neuinstallation des Betriebssystems ist eine genaue Kenntnis der Abläufe beim Booten notwendig.

In diesem Vortrag sollen die Schritte beim Booten und gewisse damit zusammenhängende Einstellungen im Betriebssystem vorgestellt werden. Zudem werden auch die durch Extensible Firmware Interface (EFI) und GUID Partition Table (GPT) eingeführten bzw. anstehenden Neuerungen berücksichtigt.

Linux im Active-Directory

Es wird vorgestellt, wie ein Linux-System in eine Active-Directory-Umgebung eingebunden werden kann. Der Fokus des Vortrags liegt auf der Verwendung von Samba-Tools. Das Linux-System soll dabei keine Server-Dienste übernehmen, sondern als Workstation dienen, d.h. es geht um die Nutzer-Verwaltung und den Zugriff auf Windows-Shares.

Da ein solches Setup insbesondere in einer Umgebung mit überwiegendem Einsatz von Windows als Betriebssytem interessant ist, liegt die Verwendung als Linux-Terminalserver nahe. Dabei können für die gelegentlichen Arbeiten unter Linux oder die gezielte Nutzung von Linux-Applikationen von Windows-Arbeitsplätzen aus grafische Logins auf der Linux-Workstation zum Einsatz kommen. Im Vortrag werden die für diesen Zweck gut geeignete NX-Technik und deren verschiedenen Ausprägungen vorgestellt.

Passwörter & Passwortmanager KeePass

Passwörter sind trotz bekannter Schwächen und Nachteile weiterhin der Standardweg zur Authentifizierung von Nutzern an IT-Systemen. Es gibt viele bekannte Grundregeln für den Umgang mit Passwörtern. Diese sollen im Vortrag vorgestellt und auch kritisch hinterfragt werden, dabei werden z.B. auch neuere Methoden zum Knacken von Passwort-Hashes vorgestellt. Aus den Betrachtungen werden Hinweise und Empfehlungen abgeleitet.

Daneben sollen auch Möglichkeiten zur technischen Umsetzung von Passwort-Policies dargelegt und Tools zum Umgang mit Passwörtern vorgestellt werden, u.A. der Passwortmanager KeePass. An Beispielen wie Passwort-Speicherung im Browser werden die notwendigen Abwägung zwischen Sicherheitsansprüchen und Benutzungskomfort diskutiert.

Secure Shell (SSH)

In diesem Vortrag soll nur kurz auf die Grundfunktionen von ssh eingegangen werden. Der Fokus des Vortrags liegt vielmehr auf der Nutzung von Private-/Public-Keys zur Authentifizierung sowie erweiterten Einstellungsmöglichkeiten, die erst in neueren Versionen hinzugekommen sind. Insbesondere die fallweise Konfiguration mittels match-Direktive wird vorgestellt. Auch wird am Beispiel einer automatisierten Dateiübertragung, wie sie häufiger zwischen Servern zum Einsatz kommt, gezeigt, wie die Nutzungsmöglichkeiten eines ssh-Zugangs auf das nötige Maß beschränkt werden können.

Anfahrt

Details zur Anfahrt können Sie unserer Webseite `http://www.rrzn.uni-hannover.de/anfahrt.html` entnehmen. Bitte kommen Sie zum Seminarraum sowie zum Ausbildungsraum über den Hof, nicht mehr über den alten Zugang innerhalb des Hauses. Der Eingang befindet sich in der mit der Nummer 4 versehenen Ecke und ist nicht der mit 2 bezeichnete Haupteingang des RRZN: