Leibniz Universität Hannover

R|R|Z|N

Sicherheitstage

im Sommersemester 2009

19. Mai 2009 & 10./11. August 2009

Die Sicherheitstage werden am 19. Mai 2009 (Dienstag) und davon abgesetzt am 10. und 11. August 2009 (Montag und Dienstag) vormittags im Seminarraum des RRZN, Schloßwender Straße 5 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. Der Tag im Mai wird sich anlässlich von Conficker mit Malware-Abwehr und dem Umgang mit infizierten Rechnern beschäftigen.

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 für die beiden Blöcke getrennt, sie können auch nur zu einzelnen Vorträgen kommen. 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

Dienstag, 19.05.09	Montag, 10.08.09	Dienstag, 11.08.09
09:15–09:45 **Zur Sicherheitslage** H. Harnisch 09:45–10:45 **Client-Absicherung** H. Harnisch	09:15–10:45 **Personal-Firewall** H. Harnisch	09:15–10:45 **Samba** H. Harnisch
10:45–11:15 Pause	10:45–11:15 Pause	10:45–11:15 Pause
11:15–12:45 **Umgang mit Infektionen** H. Harnisch	11:15-12:45 **Mac-OSX: Firewalling etc.** M. Heisterkamp	11:15–12:15 **Bitlocker & TrueCrypt** B. Gersbeck-Schierholz, H. Harnisch 12:15–12:45 **Diskussion** H. Harnisch

Vorträge

Begrüßung & Zur Sicherheitslage

Es wird ein Überblick der derzeitigen Bedrohungslage gegeben und einige zu ergreifende Maßnahmen werden dargestellt. Insbesondere wird die Lage bzgl. Conficker im Universitäts-Netz erläutert.

Absicherung von Windows-Clients

Eigentlich geht es bei der Grundabsicherung immer um das Gleiche: Anti-Virensoftware, Firewall und regelmäßige Updates. Das ist aber nicht immer ganz einfach und hinzu kommt eine Vielzahl von kleinen Einzelmaßnahmen. Ein paar dieser Dinge werden, gerade auch im Hinblick auf Conficker, erläutert.

Umgang mit Infektionen

Es gibt keinen hundertprozentigen Schutz, so dass es auch bei noch so sorgfältiger Administration und Nutzung zu Malware-Vorfällen kommen kann. Der richtige Umgang mit dem inifzierten PC ist dann entscheidend. Es wird kurz das übliche Vorgehen in der Universität dargestellt. Umfangreicher werden die Untersuchung eines wahrscheinlich infizierten Windows-Systems nach Malware und dafür vom RRZN vorgesehene Tools dargestellt.

Personal Firewalls

Nach einer kurzen Einführung in die TCP- und UDP-Kommunikation und die Grundlagen von Statefull-Firwalls werden die Windows-Firewall und IPTables under Linux vorgestellt. Verschiedene gängige Auffassungen zum Einsatz von Personal-Firewalls werden erläutert und eine Empfehlung für Server und Clients gegeben.

Mac-OSX: Firewall etc.

Unter Mac-OSX arbeiten inzwischen zwei verschiedene Firewalls: eine applikations-bezogene und die schon früher in Mac-OSX enthaltene und auf ipfw von FreeBSD basierende. Die Vor- und Nachteile und die Bedienunsgweisen werden vorgestellt. Darüber hinaus werden weitere Tipps zur Absicherung und Analyse von Mac-OSX-Clients gegeben.

Samba

Samba ist ein Opensource-Programm, dass ähnlich einem NT-Server für Windows-Clients eine zentrale Authentifizierungsstelle und File-Services zur Verfügung stellen kann. Dabei läuft Samba als Anwendung auf einem Unix-Server. Der Vortrag soll in die verschiedenen Nutzungsmöglichkeiten vom unauthentifizierten Share bis hin zur Domänenverwaltung einführen, dabei aber auch mögliche Setups in einer Active-Directory-Domäne oder mit LDAP darstellen. (Dieser Vortrag sollte bereits im letzten Semester auf den Sicherheitstagen gehalten werden, musste aber aus Krankheitsgründen ausfallen.)

Bitlocker & TrueCrypt

Mobile IT-Geräte stellen ein Problem für die IT-Sicherheit dar. Insbesondere der unbefugte Zugriff auf Daten ist deutlich erleichtert, wenn die Geräte verloren oder gestohlen werden, ebenso wenn diese längere Zeit unbeobachtet bleiben. Einem Großteil der Probleme kann man mit Verschlüsselung begegnen. Einerseits kann man ganze Partitionen inkl. Betriebssystem verschlüsseln (z.B. bei Notebooks), andererseits auch nur mobile Datenträger (USB-Sticks). Vorgestellt werden das ab Windows-Vista im Betriebssystem enthaltene Bitlocker und die Open-Source-Software TrueCrypt.

Abschlussdiskussion und Fragen

In der Abschlussdiskussion sollen nicht nur Fragen zu den bereits in den Vorträgen angesprochenen Themen sondern auch darüber hinausgehende Dinge besprochen werden.

Die Sicherheitstage im Wintersemester 2009 werden voraussichtlich am 16. und 17.11.2009 vormittags stattfinden. Programm und Einladung werden wenige Wochen vor den Sicherheitstagen per Mail und auf den Webseiten bekannt gegeben.

Anfahrt

Details zur Anfahrt können Sie unserer Webseite `http://www.rrzn.uni-hannover.de/anfahrt.html` entnehmen. Bitte kommen Sie zum Seminarraum 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: