Sicherheitstage SS 2007

Die nächsten Sicherheitstage finden in der Zeit vom 20. bis 22. Juni 2007 vormittags im Seminarraum des RRZN, Schloßwender Straße 5 statt.

Die Sicherheitstage sollen Serviceangebote des RRZN mit Bezug zur IT-Sicherheit vorstellen und zu einigen Sicherheitsthemen in der Administration einen tieferen Einblick geben. Zudem sollen die Vormittage Gelegenheit zum Gespräch und Erfahrungsaustausch geben.

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 http://www.rrzn.uni-hannover.de/organisatorisches.html. Die Anmeldung erfolgt dabei zwar für alle drei Vormittage, bitte melden Sie Sich aber auch dann an, wenn Sie nur an einigen Vorträgen teilnehmen wollen.

Terminplan

<table>
<tr><th>Mittwoch, 20.06.07</th><th>Donnerstag, 21.06.07</th><th>Freitag, 22.06.07</th></tr>
<tr><td>09:15-09:45
IT an der LUH
Müller-Schloer (CIO)</td><td rowspan="2">09:15-10:45
Netzboot mit PXE
Harnisch, RRZN</td><td>09:15-09:45
Disaster Recovery
Brandt, RRZN</td></tr>
<tr><td>09:45-10:45
Zur Sicherheitslage
Harnisch, RRZN</td><td>09:45-10:30
Hacking-Demonstration
Kötter., RRZN</td></tr>
<tr><td>10:45-11:15 Pause</td><td>10:45-11:15 Pause</td><td>10:30-11:00 Pause</td></tr>
<tr><td rowspan="2">11:15-12:45
Netfilter/IP-Tables
Harnisch, RRZN</td><td rowspan="2">11:15-12:45
Netzboot im Pool
Heisterkamp, RRZN</td><td>11:00-12:00
RRZN-Dienste
div., RRZN</td></tr>
<tr><td>12:00-12:45
Abschlussdiskussion & Fragen
Harnisch, RRZN</td></tr>
</table>

Vorträge

IT an der Leibniz Universität Hannover
Der CIO der Universität, Herr Prof. Müller-Schloer, wird die Vortragsreihe beginnen und dabei seine Arbeit für die Universität vorstellen. Überlegungen und Planungen werden angesprochen, und Fragen können diskutiert werden.

Zur Sicherheitslage
Die aktuelle Entwicklung, wie sie u.a. vom DFN-CERT und dem BSI in Bezug auf Angriffe gesehen wird, wird dargestellt. Dabei werden BOT-Netze und Root-Kits angesprochen, und es wir verstärkt auf die zunehmende Bedrohung durch nutzerinitiierte Schwachstellenausnutzungen eingegangen: Eine zunehmende Bedrohung geht von Trojanern, Phishing und Cross-Site-Scripting aus.

Netfilter / IP-Tables
Mit Netfilter ist die zusätzliche Absicherung eines Einzelsystems mit einer Software-Firewall (Personal Firewall) möglich. In diesem Vortrag soll das Konzept von Netfilter/IP-Tables unter Linux erklärt werden. Fortgeschrittene Themen wie die Begrenzung der Zugriffsanzahl zur Abwehr von DoS- und SSHBruteforce-Angriffen werden angesprochen.
Die direkte Manipulation mit den iptables-Kommandos und die Einbindung in den init-Prozess werden dargestellt. Zudem wird für eine GUI-gestützte Konfiguration das Tool FWBuilder vorgestellt.

Netzboot mit PXE
Viele moderne PCs mit Netzwerkkarte onboard unterstützen PXE-Boot. Damit kann ein Rechner aus dem Netzwerk von einem Server gestartet werden, ohne dass ein Betriebssystem lokal auf einer Festplatte oder CD vorhanden sein muss. Dieses erleichtert auch bei PCs mit Festplatte die Administration, erhöht aber zugleich die Sicherheit durch das Starten nichtinfizierter Systeme (z.B. Virenscanner) aus dem Netz und das erheblich leichtere Neuaufsetzen bei Infektionsverdacht. In diesem Vortrag sollen die Grundzüge von PXE, der Ablauf beim Booten und die nötige Server-Infrastruktur dargestellt werden. Besonderer Fokus liegt dabei auf Linux/Debian als Server und PXELinux als Boot-Loader.

Netzboot im Pool
Das Booten aus dem Netz mit PXE eignet sich insbesondere für Ausbildungs-Pools. Einerseits handelt es sich dabei meist um gleichartige Hard- und Software, andererseits benötigt man häufig wechselnde Installationen (beispielsweise abhängig von angesetzten Kursen). Studentische Pools mit wechselnden Nutzern sind aus Sicherheitssicht schwierig, da ein einzelner Nutzer nicht allein für das System verantwortlich ist und evt. bei der Nutzung ein bereits vorher infiziertes oder manipuliertes System vorfindet. In diesem Kurs sollen Überlegungen, ein Setup und Skripte vorgestellt werden, die das schnelle (evt. sogar regelmäßige) automatische Aufsetzen und Klonen von Betriebssysteminstallationen ermöglichen.

Disaster-Recovery mit Veritas-Netbackup
Das RRZN bietet seit längerem einen zentralen Backup-Dienst an. Dieser Dienst, die Installation, nötige Absprachen, das Recovery und ggf. nötige Zusatzlizensierungen sollen nur kurz angesprochen werden. Vertieft soll auf die Möglichkeit des „Disaster-Recovery“ oder „Baremetal-Backups“ eingegangen werden, mit dem ein Rechner fast automatisch komplett wieder aufgesetzt werden kann. Dieser Service wird vom RRZN für Windows-Server seit März angeboten.

Hacking-Demonstration
In diesem Vortrag soll an Beispielen gezeigt werden, wie einfach Hacking sein kann. Mit im Internet frei erhältlichen Tools mit komfortabler Oberfläche können Angriffe gegen ungepatchte und schlecht gesicherte Systeme fast von jedem ausgeführt werden. Unter Anderem soll gezeigt werden, wie durch Social-Engineering Systeme hinter Firewalls angegriffen werden – Angriffe, die neben einer guten Clientinstallation nur durch mündige Nutzer abgewehrt werden können. Auch soll vorgeführt werden, wie unsicher Wireless-Netze ohne WPA sind.

RRZN-Dienste

In diesem Vortrag sollen Neuerungen in mehreren Service-Angeboten des RRZN vorgestellt werden. Zudem können Fragen zu den Diensten gemeinsam diskutiert werden. Die verschiedenen Ansprechpartner werden jeweils in kurzen Abschnitten die Dienste und Veränderungen darstellen:

- CA/PKI: neue Global-Policy und Root-CA (Gersbeck-Schierholz)
- Sophos: SAV/SAU unter Vista, Linux-Client mit On-Demand-Prüfung (Brandt, Harnisch)
- WSUS: Umstellung auf WSUS 3 (Brandt, Harnisch)
- Netzschutz: Policy als Webseite (Peter)

Abschlussdiskussion und Fragen

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

Workshop (27.06.2007)

Zu den Themen der Sicherheitstage wird ein separater Workshop am 27. Juni 2006 (Mittwoch) von 14:00 bis 17:00 Uhr im RRZN stattfinden. Die genauen Themen werden erst später unter Berücksichtigung der Diskussionen auf den Sicherheitstagen festgelegt. Beabsichtigt ist derzeit als Hauptthema das Booten aus dem Netz mit PXE und der Einsatz in Ausbildungs-Pools.
Da dieser Teil im Ausbildungsraum am Computer stattfinden wird, ist die Teilnehmerzahl auf 20 begrenzt. Eine separate Anmeldung zum Workshop ist erforderlich und kann ab den Sicherheitstagen online erfolgen.

Die Sicherheitstage im Wintersemester 2007/2008 werden wieder einen stärkeren Fokus auf Windows-Betriebssysteme und –Netze haben und werden vom 19. bis 21.11.2007 vormittags stattfinden. Programm und Einladung werden wie gewohnt wenige Wochen vor den Sicherheitstagen per Mail und auf den Webseiten bekannt gegeben.