Sicherheitstage WS 2007/2008

Die nächsten Sicherheitstage finden in der Zeit vom 19. bis 21. November 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.
Die Plätze werden zwar bevorzugt an Teilnehmer aus der Leibniz Universität Hannover vergeben, externe Teilnehmer anderer Hochschulen sind aber willkommen. Bei Anmeldeproblemen wenden Sie Sich bitte (bevorzugt per Mail) an uns: http://www.rrzn.uni-hannover.de/kontakt.html.

Terminplan

<table>
<tr><th>Montag, 19.11.07</th><th>Dienstag, 20.11.07</th><th>Mittwoch, 21.11.07</th></tr>
<tr><td rowspan="2">09:15-10:30
Zur Sicherheitslage
Harnisch, RRZN</td><td>09:15-09:45
Konfiguration des IIS
Harnisch, RRZN</td><td rowspan="2">09:15-10:30
SSH und STunnel
Harnisch, RRZN</td></tr>
<tr><td>09:45-10:45
Webserver-Betrieb
Niederlag, RRZN</td></tr>
<tr><td>10:30-11:00 Pause</td><td>10:45-11:15 Pause</td><td>10:30-11:00 Pause</td></tr>
<tr><td>11:00-12:00
Web-DAV
Niederlag, RRZN</td><td rowspan="2">11:15-12:45
PHP-Sicherheit
Kunz, RRZN</td><td>11:00-12:00
RRZN-Dienste
div., RRZN</td></tr>
<tr><td>12:00-12:45
Schadcodeerkennung
Kötter, RRZN</td><td>12:00-12:30
Abschlussdiskussion & Fragen
Harnisch, RRZN</td></tr>
</table>

Vorträge

Begrüßung & Zur Sicherheitslage
Die aktuelle Entwicklung, wie sie u.a. vom DFN-CERT und dem BSI in Bezug auf Angriffe gesehen wird, wird dargestellt. Erklärt wird das Prinzip von Bot-Netzen und die vielfältigen Arten, wie diese aufgebaut werden. Herausgestellt werden soll, dass es schwerer wird, infizierte Rechner zu finden, und dass traditionelle Schutzmaßnahmen (Firewall, Virenscanner) zwar weiterhin sehr wichtig aber für neuere Angriffe wirkungslos sind.
Quasi als Einstimmung auf den „Webserver-Tag“ am Dienstag sollen typische Angriffe, Tools und Vorkommnisse kurz dargestellt werden. Zudem sollen grundlegende Überlegungen und Vorgehensweisen bei der Programmierung einer Webseite angesprochen und die Studie „Sicherheit von Webanwendungen“ des BSI von 2006 vorgestellt werden.

Web-DAV als sichere und einfache Alternative zu Samba
Auch kleine Arbeitsgruppen benötigen oftmals Netzwerkfreigaben für ein effektives Arbeiten. Als Antwort darauf wird oft ein Samba-Server installiert. In diesem Vortrag wollen wir uns Web-DAV als einfache und sichere Alternative für eine Netzwerkfreigabe anschauen. Dabei werden sowohl die server- als auch die client-seitigen Grundlagen geschildert.

Erkennung von Schadcode in Netzwerkverkehr mit Hilfe von Emulation
Das rechtzeitige Erkennen von Angriffen auf Infrastrukturen ist eine der Herausforderungen der heutigen Zeit. Signaturbasierende Verfahren werden seit langem in Antiviren-Scannern und IDS genutzt und durch die Anzahl der Signaturen allerdings auch immer langsamer und ressourcenintensiver.
Der Vortrag beschäftigt sich mit der Erkennung von Angriffen durch Emulation, Ausführen von suspekten Streams auf einer x86-CPU-Emulation.

Konfiguration des Internet-Information-Servers
Der IIS ist auf Windows-Systemen sehr schnell eingerichtet. Allerdings täuscht die GUI über die Tücken der sicheren IIS-Konfiguration hinweg: die Einstellungsmöglichkeiten verstecken sich zum Teil in vielen Fenstern und hinter vielen Knöpfen. Der Vortrag soll nicht umfassend die Konfiguration des IIS vorstellen, sondern einführend einige Aspekte erklären, z.B. den Zusammenhang zu Dateirechten.

Sicherheitsaspekte beim Betrieb eines Webservers am Beispiel Apache
Gerade beim Komfort heutiger Linux-Distributionen ist ein Webserver (scheinbar) sehr schnell eingerichtet. Für die Distributoren ist dabei vor allem der Aspekt einer möglichst breiten und auf viele verschiedene Szenarien ausgerichteten Konfiguration wichtig. Hinsichtlich der Sicherheit ist jedoch eine möglichst entschlackte und angepasste Konfiguration sinnvoll. In diesem Vortrag wollen wir uns mit einigen hinsichtlich des sicheren Betriebs wichtigen Aspekten der Konfiguration und Funktion des Apache-Webservers beschäftigen.

SSH und STunnel
Es soll anhand von verschiedenen SSH-Implementationen die Nutzung und der Vorteil von Public-Private-Keys vorgeführt werden. Zudem soll SSH als einfaches VPN genutzt werden, um z.B. auf eine Netzfreigabe oder eine auf IP-Bereiche zugriffsbeschränkte Webseite zugreifen zu können. Es soll aber auch die Serverkonfiguration angesprochen werden, mit deren Hilfe einige dieser Funktionen unterbunden werden können.
STunnel ist ein Tool, mit dessen Hilfe eine TCP-Verbindung SSL-verschlüsselt werden kann. Traditionell wurde das Tool für Pop-Zugriffe genutzt, was heutzutage dank der SSL-/TLS-Implementierung in Mail-Clients nicht mehr nötig ist. Dennoch ist STunnel ein interessantes Produkt: Es gibt andere unverschlüsselte Protokolle, und es kann auch zur Clientauthentisierung genutzt werden.

RRZN-Dienste
In diesem Vortrag sollen Service-Angebote 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:

- Mail: Spamabwehr mit PureMessage (Pracht)
- Backup: neue Veritas-Version (Giesker)
- WLAN & VPN: neuer WPA-Zugang, zertifikatsbasierte Profile (Oltmann)
- WSUS: Umstellung auf WSUS 3 (Brandt, Harnisch)

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.

Die Sicherheitstage im Sommersemester 2008 werden voraussichtlich vom 16. bis 18.06.2008 vormittags stattfinden. Programm und Einladung werden wie gewohnt wenige Wochen vor den Sicherheitstagen per Mail und auf den Webseiten bekannt gegeben.