Sicherheitstage

im Wintersemester 2018/2019

28./29. Januar 2019

Die Sicherheitstage werden am Montag 28. Januar nachmittags und Dienstag 29. Januar 2019 vormittags stattfinden. Die Sicherheitstage sollen zu einigen Sicherheitsthemen von IT-Systemen für Administratorinnen und Administratoren einen tieferen Einblick geben. Zudem sollen die Tage Gelegenheit zum Gespräch und Erfahrungsaustausch bieten, auch zu Serviceleistungen der Leibniz Universität IT Services.

Die Sicherheitstage richten sich in erster Linie an Administratorinnen und Administratoren und die IT-Beauftragten der Einrichtungen sowie die IT-Sicherheitsbeauftragten der Fakultäten und zentralen Einrichtungen der Leibniz Universität Hannover. Dabei sollen auch Beschäftigte, 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 per Mail an harnisch+sita@luis.uni-hannover.de Die Anmeldung erfolgt dabei zwar für beide halben Tage, bitte melden Sie sich aber auch dann an, wenn Sie nur an einigen Vorträgen teilnehmen wollen.

Bei Anmeldeproblemen wenden Sie sich bitte (bevorzugt per E-Mail) an uns: `http://www.luis.uni-hannover.de/sicherheitsteam.html`.

Veranstaltungsort

Die Sicherheitstage werden im 3d-Raum im Erdgeschoss des LUIS in der Schlosswender Str. 5 stattfinden. Details zum Veranstaltungsort können Sie der Webseite `https://info.cafm.uni-hannover.de/room/1210.000.B024` entnehmen.

Terminplan

Montag, 28.01.19 nachmittags		Dienstag, 29.01.19 vormittags	
13:15–14:45	**Sicherheitslage** H. Harnisch	09:15–10:45	**Awareness** T. Casselt
14:45–15:15	Pause	10:45–11:15	Pause
15:15–16:45	**Linux-Firewalling** M. Kötter	11:15–12:45	**TLS & PKI** H. Harnisch

Vorträge

Sicherheitslage

Es wird ein Überblick der derzeitigen Bedrohungslage gegeben, wie sie auch vom DFN-CERT und dem BSI skizziert wird und sich an der LUH darstellt. Es werden ein paar aufgetretene Sicherheitsprobleme und -vorfälle exemplarisch vorgestellt und zu ergreifende Maßnahmen empfohlen.

Ebenfalls werden einige Empfehlungen und beabsichtigte Umstellungen angesprochen, die sich technisch aber auch organisatorisch in der Universität ergeben.

TLS-Verschlüsselung & Public-Key-Infrastructure

TLS-Verschlüsselung bei Webseiten aber auch anderen Diensten wie Mail ist heute eigentlich Standard. In den letzten Jahren hat es bei TLS größere Änderungen gegeben, auch in Bezug auf das Management von Zertifikaten und dem Betrieb einer PKI. Zudem steht in der innerhalb der LUH verwendeten DFN-PKI ein Wechsel des auslaufenden Root-CA-Zertifikats an.

Der Vortrag geht vorallem auf den bevorstehenden Wechsel der CA-Zertifikate ein, der mit dem Auslaufen vieler Zertifikate im Juli einhergeht. Dabei sollen einerseits Änderungen in der PKI-Verwendung der LUH sowie in der Policy der DFN-PKI dargestellt werden. Es sollen aber auch die nötigen Schritte für den Zertifikatswechsel inkl. Tests für Server-Administratoren besprochen werden.

Awareness / Sicherheit für Anwender

Eine Vielzahl von Angriffen benötigt keine technischen Sicherheitslücken sondern nutzt die Schwachstelle Mensch: Social Engineering bleibt nach technischer Absicherung von Systemen die größte Sicherheitslücke. Zunehmend zielen Angriffe in diese Richtung; die Perfektionierung von Phishing ist ein aktuelles Beispiel.

Daher ist Awareness ein wichtiges Element der Informationssicherheit – aber auch eins der schwersten. In diesem Vortrag sollen wichtige Punkte für die Sicherheitsschulung von Nutzerinnen und Nutzern gegeben werden. Dafür werden exemplarisch Schulungselemente vorgestellt. Die Administratorinnen und Administratoren sollen in die Lage versetzt werden, als Multiplikatoren oder in Einzelfällen Endanwenderinnen und Endanwender zu schulen.

Linux-Firewalling / IPTables

Nach einer kurzen Einführung in die TCP- und UDP-Kommunikation und die Grundlagen von Statefull-Firewalls wird IPTables unter Linux vorgestellt. IPTables ist nochimmer die verbreitete und in den meisten Distributionen angebotene Firewall. Zuhörende sollen in die Lage versetzt werden, ihre Server- und Client-Systeme mittels IPTables abzusichern.

In einem zweiten Teil des Vortrags wird ein Ausblick auf NFTables und weitere Entwicklungen im Bereich des Firewallings unter Linux gegeben.