Verschlüsselungstechniken, Signaturen und Zertifikate

Aus unserer heutigen Kommunikation ist Verschlüsselung nicht mehr wegzudenken. Praktisch alle Webserver liefern ihre Seiten über https (also verschlüsselt) aus. Die Kommunikation zwischen Zweigstellen von Unternehmen erfolgt über VPNs (verschlüsselt) durch das Internet, in Zukunft werden Anmeldungen nicht mehr mit Hilfe von Benutzername und Passwort stattfinden, sondern mit Schlüsselpaaren (FIDO2). Aber wie funktioniert das eigentlich und ist es wirklich sicher?

Welche Eigenschaften hat ein Schlüsselpaar (Private Key, Public Key) und was kann man damit machen. Wie stellt eine Zertifizierungsstelle ein Zertifikat aus und was ist eigentlich ein Zertifikat. Was erhält man von einer Zertifizierungsstelle und was macht man damit? Was darf weitergeben werden und was nicht? Was steckt hinter Begriffen wie Hash, RSA und Diffie-Hellman?

Diese und viele weitere Fragen werden im Seminar leicht verständlich beantwortet.

Zielgruppe

Alle die sich mit Verschlüsselung und Zertifikaten beschäftigen.

Ihr Nutzen

Nach dem Seminar wissen Sie, wie symmetrische und asymmetrische Verschlüsselungsverfahren funktionieren und Sie können diese Verfahren anwenden. Sie wissen wie eine digitale Signatur erstellt wird und wie Authentifizierung mit Schlüsseln funktioniert. Sie können eine Zertifikatsanforderung erstellen, daraus ein Zertifikat generieren und es entsprechend einsetzen. Sie sind vertraut mit dem Standard X.509 und kennen die wichtigsten Felder in X.509-Zertifikaten und ihre Bedeutung.

Methoden

Präsentation, Trainervortrag, Übungen mit virtuellen Maschinen, Simulation, Gruppendiskussion

Schwerpunkte

- Ziele der Verschlüsselung
- Kryptologie, Kryptographie, Kryptanalyse
- Kryptographische Grundlagen
- Modulare Arithmetik
- Symmetrische Verschlüsselung
- Hashes (MD5, SHA-1, SHA-256)
- Asymmetrische Verschlüsselung
- Das RSA-Kryptosystem
- Digitale Signaturen
- Authentifizierung mit Schlüsseln
- Schlüsselaustausch nach Diffie-Hellman
- Open-Source vs. Security by Obscurity
- Aufbau und Bestandteile einer PKI
- Standards (X.500, X.509)
- Architektur von Zertifizierungsstellen (RootCA, IntermediateCA, SubCA)
- Zertifizierungsstellen (CA) erstellen
- Zertifikatsanforderungen (CSR) erstellen
- X.509-Zertifikate erstellen
- Zertifikatsketten

- SSL/TLS
- SSH/SCP
- Anwendungen (HTTPS, FTPS, SFTP, SCP)

Termine

Nürnberg

28.03.2022 - 30.03.2022 1.571,00 EUR (0% USt.)

inkl. Lehrmaterial, Mittagessen und Getränken

Nürnberg

19.10.2022 - 21.10.2022 1.571,00 EUR (0% USt.)

inkl. Lehrmaterial, Mittagessen und Getränken

Dauer

3 Tage

8:30 Uhr bis 16:00 Uhr

Standard-Inhouse-Seminar

Seminar, das ohne Veränderung von Inhalten und Dauer für eine Gruppe von Teilnehmern gebucht wird. Ort und Beginn werden individuell abgestimmt.

4.725,00 EUR

zzgl. Reisekosten für den Trainer in Höhe von 0,30 € je km ab Nürnberg zum Veranstaltungsort und zurück,
zzgl. pauschal 100,- € Hotelkosten für den Trainer pro Tag ab 200 km
zzgl. 40 € für Seminarunterlagen pro TN

Max. 12 Teilnehmer

Zertifikat

Zertifikat der GRUNDIG AKADEMIE

Ansprechpartner

Doris Eckstein

Tel: +49 911 95117-535

doris.eckstein@grundig-akademie.de

Winfried Gmeiner

Tel: +49 911 95117-522

winfried.gmeiner@grundig-akademie.de

Renate Prosser

Tel: +49 911 95117-317

renate.prosser@grundig-akademie.de