Erwerben Sie die Kenntnisse und Fähigkeiten zur Anwendung kryptographischer Verfahren und Verschlüsselungstechniken im Kontext der IT-Sicherheit

Sicherheitsmaßnahmen können nur dann wirksam sein, wenn deren Bestimmung und Umsetzung eine ganzheitliche Betrachtung, einschließlich der Betrachtung der Perspektive potenzieller Angreifer, zugrunde liegt.

Eine Vielzahl von Sicherheitsmaßnahmen berücksichtigt die Anwendung kryptographischer Verfahren, wie die Nutzung digitaler Zertifikate und Signaturen, den Aufbau von Public-Key-Infrastrukturen (PKI), den verschlüsselten Datenaustausch in Netzwerken via Ethernet- oder IP-Verschlüsselung oder auf der Anwendungsschicht via S/MIME. Die sinnhafte Einführung und Nutzung solcher Verfahren und Komponenten setzt ein strukturiertes Vorgehen in der Bedrohungsanalyse, unter Berücksichtigung aktueller Angriffsmethoden und Vorgehensweisen potenzieller Angreifer, voraus. Des Weiteren müssen die ordnungsgemäße Anwendung kryptografischer Verfahren umgesetzt und fehlerhafte Implementierungen sowie Konfigurationen von Sicherheitskomponenten verhindert werden. Ein angemessenes Sicherheitsniveau der Nutzung kryptographischer Verfahren wird erreicht, wenn das Zusammenwirken aller Faktoren bei der Einführung und Verwendung bewusst gesteuert wird.

Die Auseinandersetzung mit der Nutzung und Anwendung kryptographischer Verfahren unterstützt zusätzlich den Wissensaufbau im Bereich der Informationssicherheit, insbesondere des Datenschutzes sowie der IT-Sicherheit.

ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung ist die Vermittlung der für die praktische Anwendung kryptographischer Verfahren erforderlichen **Fachkenntnisse**, der aktuellen **Verschlüsselungstechniken**, der Anwendung von **Sicherheitszertifikaten** und **digitalen Signaturen** sowie des Aufbaus von **Public-Key-Infrastrukturen** (PKI).
Die Teilnehmer erwerben Kenntnisse über aktuelle **Bedrohungs- und Risikolagen** bei der Nutzung kryptographischer Verfahren, wie S/MIME, SSL oder X.509-Zertifikaten und die **Umsetzung von Maßnahmen zur Sicherstellung der Schutzziele** einer Organisation.

INHALT

- Einführung
  - Definition und Abgrenzung der IT-Sicherheit
  - Diskussion konkreter Beispiele
- Theoretische Grundlagen
  - Grundlegende Operationen in der Kryptographie (einführende mathematische Grundlagen)
  - Historische Verfahren der Kryptographie
  - Kryptographische Hashverfahren
  - Symmetrische Verschlüsselungsalgorithmen
  - Asymmetrische Verfahren (Verschlüsselung und digitale Signatur mit RSA und elliptischen Kurven)
  - Schlüsselaustauschverfahren (Diffie-Hellmann und Elliptic Curve Diffie-Hellmann)
  - Zufallszahlen
  - PKI-Infrastrukturen (Digitale Zertifikate, Wurzel- und CA-Instanzen, Sperrlisten, OCSP)
- Ermittlung und Definition von IT-Sicherheitsanforderungen
  - Technische Richtlinien und Vorgaben des Bundesamts für Sicherheit in der Informationstechnik
  - Bedrohungsanalyse
  - Risikobewertung
  - Nutzung des CORAS-Verfahrens
- Ausgewählte Themenschwerpunkte (werden nach Bedarf der angemeldeten Teilnehmer vertiefend behandelt)
  - Frameworks und Bibliotheken für die Entwicklung sicherer Komponenten
  - Vorgehensmodelle in der Entwicklung und Validierung
  - Evaluierung und Zertifizierung gemäß ISO 15408 (Common Criteria)
  - Netzwerksicherheit - Diskussion aktueller Verfahren auf OSI Layer-2 und Layer-3
- Praktische Übungen (finden verteilt über den gesamten Verlauf des Seminars statt)
  - Schlüsselgenerierung / Erzeugung von Zertifikaten
  - Verschlüsselung von Daten und Dateien
  - S/MIME-Sicherheit
  - Netzwerkanalyse und Netzwerksicherheit
  - Passwortsicherheit

Abschluss: Teilnahmebestätigung | **Optional:** Prüfung mit Personenzertifikat (DGI®)

ZIELGRUPPE

- Personen, die kryptographische Verfahren bewerten oder anwenden müssen (z.B. Lösungsarchitekten)
- IT-Sicherheitsbeauftragte
- Chief Information Security Officer
- Datenschutzbeauftragte

IHR DOZENT

Herr Dr.-Ing. Armin Lunkeit
Herr Dr.-Ing. Lunkeit ist Senior Director Network Encryption bei der Rohde & Schwarz Cybersecurity GmbH.

Seminar ROB 2727 | Stand Januar 2020