SC700 Kryptographie 101 inkl. Quantenresilienz

Kurzbeschreibung:

IT-Fachkräfte erhalten eine praxisnahe Einführung in Grundlagen und Anwendung kryptographischer Verfahren. Vermittelt werden symmetrische und asymmetrische Algorithmen, Hash- und Signatur-Verfahren sowie Protokolle für sichere Kommunikation. Behandelt werden Implementierungsaspekte mit Krypto-Bibliotheken, Risiken durch Software-Schwachstellen sowie aktuelle Herausforderungen durch notwendige Migrationen zur Post-Quantum-Resilienz.

Zielgruppe:

Das Training **SC700 Kryptographie 101 inkl. Quantenresilienz** richtet sich an:

- Softwareentwickler
- Softwarearchitekten
- Administratoren
- Produktmanager

Voraussetzungen:

Um allen Lerninhalten des Kurses **SC700 Kryptographie 101 inkl. Quantenresilienz** gut folgen zu können, ist ein praktisches technisches Grundverständnis Voraussetzung.

Sonstiges:

Dauer: 2 Tage

Preis: 1490 Euro plus Mwst.

Ziele:

Die Teilnehmer des Kurses **SC700 Kryptographie 101 inkl. Quantenresilienz**

- erlernen aktuelle Krypto-Verfahren und deren sichere Implementierung anhand typischer Einsatzszenarien;
- können aktuelle und mögliche künftige Gefahren für bestehende Algorithmen abschätzen und bewerten;
- erhalten einen Überblick über quantenresiliente Verfahren;
- werden befähigt, eine Post-Quantum-Strategie einschließlich konkreter Maßnahmen zu entwickeln.

Inhalte/Agenda:

- ♦ **Einführung in die Kryptographie**
  - ♦ ◊ Warum Kryptografie?
  - ◊ Definition und Bedeutung der Kryptographie
  - ◊ Einsatzszenarien im Alltag
- ♦ ◊
- ♦ **Grundbegriffe der Kryptographie**
  - ♦ ◊ Vertraulichkeit, Integrität, Authentizität
  - ◊ Nichtabstreitbarkeit
  - ◊ Schlüssel
  - ◊ Schlüsselaustausch
  - ◊ Signaturen
  - ◊ Hash-Funktionen
  - ◊ Zufallszahlen
  - ◊ Zero-Knowledge
- ♦ ◊
- ♦ **Symmetrische Verschlüsselung**
  - ♦ ◊ Funktionsweise Symmetrische Verschlüsselungsalgorithmen
  - ◊ Aktuelle Algorithmen
  - ◊ · DES
    · AES
    · BlowFish
  - ◊ Modi verschiedener Verfahren
  - ◊ · CTR
    · CBC
  - ◊ Stärken und Schwächen verschiedener Algorithmen
  - ◊ Anwendungsfälle und Beispiele
  - ◊ · Schlüssellängen und empfohlene Modi
    · Implementierung und Konfiguration
    · Vorschriften und Regulation
  - ◊ Bekannte Angriffe auf symmetrische Algorithmen
- ♦ ◊
- ♦ **Asymmetrische Verschlüsselung**
  - ♦ ◊ Funktionsweise von asymmetrischen Algorithmen
  - ◊ Unterschied zur symmetrischen Verschlüsselung
  - ◊ Bekannte Algorithmen
  - ◊ · RSA
    · Elliptische Kurven
  - ◊ Anwendungsfälle und Beispiele
  - ◊ · Schlüssellängen, Kurven etc.
    · Implementierung und Konfiguration
    · Vorschriften und Regulation
  - ◊ Bekannte Angriffe auf asymmetrische Algorithmen, Deprecated Versionen
- ♦ ◊
- ♦ **Schlüsselaustauschverfahren**
  - ♦ ◊ Funktionsweise
  - ◊ Diffie-Hellman
  - ◊ Anwendungsfälle und Beispiele
  - ◊ · Implementierung und Konfiguration
    · Vorschriften und Regulation
- ♦ ◊ ·
- ♦ **Sichere Signaturen und Hashes**
  - ♦ ◊ Funktionsweise Hash-Funktion
  - ◊ Bekannte Hash-Funktionen
  - ◊ · MDX-Familie
    · SHA-Familie
  - ◊ Message Authentication
  - ◊ · CMAC
    · HMAC
  - ◊ Anwendungsfälle und Beispiele
  - ◊ · Funktionsweise Digitale Signatur
- ♦ ◊ ·
- ♦ **Quanten-Computing-Grundlagen**
  - ♦ ◊

- ◊ Einführung in Quantenbits (Qubits) und Quantengatter
- ◊ Quantenalgorithmen und ihre Auswirkungen auf kryptografische Verfahren
- ◊ Der Shor-Algorithmus
- ◊ Aktueller Stand Quanten-Computing
- ◊ Ausblick und Prognosen
- ◊

- ♦ **Post-Quantum-Kryptographie**
  - ◊ Grundlagen und Ideen
  - ◊ Kategorien von post-quantum sicheren Algorithmen
    - ◊ · Gitterbasierte
      · Codebasierte
      · Multivariate Polynome
  - ◊ Übersicht über Post-Quantum-Algorithmen
  - ◊ Aktuelle Implementierung und Konfiguration
  - ◊ Normen und Standards
  - ◊ Migration aktueller Verfahren
  - ◊

- ♦ **Zusammenfassung, Ausblick und Abschluss**
- ♦
-