SC700 Kryptographie von den Grundlagen bis zur Quantenresilienz

Kurzbeschreibung:

Kryptographische Verfahren sind eine wesentliche Voraussetzung für eine sichere IT, sei es im Internet, im eigenen Rechenzentrum oder privat zu Hause. Die Sicherstellung der Integrität, Authentizität und Vertraulichkeit von Daten ist ohne Einsatz von kryptographischen Verfahren kaum möglich.

Der Workshop **SC700 Kryptographie – von den Grundlagen bis zur Quantenresilienz** gibt einen umfassenden Überblick über die theoretischen Grundlagen, praktischen Einsatzmöglichkeiten und Implementierungswege kryptographischer Maßnahmen und Funktionen.

Der Kurs behandelt aktuelle Algorithmen für symmetrische und asymmetrische Verfahren, Hash- und Signatur-Verfahren sowie darauf aufsetzende Protokolle für z.B. den Schlüsselaustausch oder die sichere Kommunikation.

Neben den Algorithmen werden die Themen Software-Implementierung, bzw. der Einsatz von Krypto-Bibliotheken adressiert, da in diesen beiden Ebenen die Gefahr von Software-Schwachstellen besteht, die auch sichere Algorithmen angreifbar machen.

Aktuelle Algorithmen wie z.B. RSA (ein asymmetrisches Verfahren) gelten bedingt durch den Fortschritt in der Quanten-Computing-Domäne als potenziell unsicher. Daher werden die Gefährdungen durch Quantum-Computing erarbeitet, das aktuelle Bedrohungspotential aufgezeigt und Möglichkeiten zur Vorbereitung (Krypto-Agilität) vertieft, z.B. durch Einführung von sogenannter Post-Quantum-Kryptographie.

Zielgruppe:

Das Training **SC700 Kryptographie – von den Grundlagen bis zur Quantenresilienz** richtet sich an:

- Softwareentwickler
- Softwarearchitekten
- Administratoren
- Produktmanager

Voraussetzungen:

Um allen Lerninhalten des Kurses **SC700 Kryptographie – von den Grundlagen bis zur 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 – von den Grundlagen bis zur Quantenresilienz**

- erlernen aktuelle Krypto-Verfahren und deren sicherer Implementierung bzw. Konfiguration;

- 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
  - Geschichte der Verschlüsselungstechniken / Anfänge der Verschlüsselung
  - Übersicht bekannter geknackter Verschlüsselungen und Auswirkungen
- **Grundbegriffe der Kryptographie**
  - Vertraulichkeit, Integrität, Authentizität
  - Nichtabstreitbarkeit
  - Schlüssel
  - Schlüsselaustausch
  - Signaturen
  - One-Way-Funktionen
  - Zufallszahlen
  - Zero-Knowledge
- **Symmetrische Verschlüsselung**
  - Funktionsweise Symmetrische Verschlüsselungsalgorithmen
  - Bekannte Algorithmen
    - DES
    - AES
    - BlowFish…
  - Modi verschiedener Verfahren
    - CTR
    - CBC
    - ...
  - Stärken und Schwächen verschiedener Algorithmen
  - Bekannte Angriffe auf symmetrische Algorithmen, Deprecated Versionen
  - Anwendungsfälle und Beispiele
    - Schlüssellängen und empfohlene Modi
    - Implementierung & Konfiguration
    - Vorschriften und Regulation
- **Asymmetrische Verschlüsselung**
  - Funktionsweise von asymmetrischen Algorithmen
  - Unterschied zur symmetrischen Verschlüsselung
  - Bekannte Algorithmen
    - RSA
    - Diffie-Hellman
    - Elliptische Kurven
  - Bekannte Angriffe auf asymmetrische Algorithmen, Deprecated Versionen
  - Anwendungsfälle und Beispiele
    - Schlüssellängen, Kurven etc.
    - Implementierung & Konfiguration
    - Vorschriften und Regulation
- **Schlüsselaustauschverfahren**
  - Funktionsweise
  - Beispiel – Schlüsselaustausch-Implementierung in TLS
  - Anwendungsfälle und Beispiele
    - Implementierung & Konfiguration
    - Vorschriften und Regulation
- **Sichere Signaturen und Hashes**
  - Funktionsweise Hash-Funktion
  - Bekannte Hash-Funktionen
    - MDX-Familie
    - SHA-Familie
  - Message Authentication
    - CMAC
    - HMAC
    - ...
  - Funktionsweise Digitale Signatur
- **Zufallszahlen**
  - Bedeutung von Zufallszahl allgemein und im Kontext der Kryptographie
  - Sichere Pseudo-Zufallszahlengenerierung
  -

- Das Messen von Entropie und die Konsequenzen
- Implementierung und Best-Practices

- **Weitere Anwendungsfälle der Kryptographie**
  - Zertifikate, PKI
  - TLS und aktuelle Cipher-Suites
  - Password-based Key-Derivation
  - Teilen von Geheimnissen
- **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 vielversprechende Post-Quantum-Algorithmen
  - Implementierung und Konfiguration
- **Zusammenfassung, Ausblick und Abschluss**