SC700-WS Quanten-Computing - Store now, decrypt later

Kurzbeschreibung:

Teilnehmende lernen grundlegende kryptographische Verfahren und deren Bedeutung für Integrität, Authentizität und Vertraulichkeit von Daten kennen. Behandelt werden Risiken durch Quantencomputer sowie das Konzept „Store now, decrypt later“. Zusätzlich erhalten die Teilnehmenden einen Einblick in die Funktionsweise von Quantencomputern und erste Maßnahmen zur Post-Quantum-Kryptographie.

Zielgruppe:

Das Web-Seminar **SC700-WS Quanten-Computing - Store now, decrypt later** richtet sich an:

- Softwareentwickler
- Softwarearchitekten
- Administratoren
- Produktmanager

Voraussetzungen:

Ein technisches Grundverständnis wird vorausgesetzt.

Sonstiges:

Dauer: 1 Tage

Preis: 0 Euro plus Mwst.

Ziele:

Die Teilnehmer des Web-Seminars **SC700-WS Quanten-Computing - Store now, decrypt later**

- erhalten einen kurzen Einblick in die Funktionsweise von Quantencomputer
- aktuelle und mögliche künftige Gefahren für bestehende Algorithmen abschätzen und bewerten zu können

Inhalte/Agenda:

- ♦ **Motivation**
  - ♦ ◊ Sicherheit, Benutzbarkeit, Funktionalität
    ◊ Vertraulichkeit, Integrität, Verfügbarkeit
    ◊ Nicht Abstreitbarkeit, Authentizität
- ♦ **Aktuelle Krypto, Hashing**
  - ♦ ◊ Asymmetrisch
    - ◊ · DH/RSA Fakturierungsproblem
      · ECDH Eindeutige Zuordnung von Punkten
    ◊ Hashing
- ♦ **Funktionsweise Quantencomputer**
- ♦ **Gefahren von Quantencomputer für Krypto**
  - ♦ ◊ Brechen von gängigen Algorithmen
    ◊ Resistenz von Hashe
- ♦ **Ausblick Post Quantum Crypto**
  - ♦