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

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.
Aber was, wenn aktuelle Verfahren den Computern der Zukunft nicht mehr standhalten?

Lernen sie in unserem Web-Seminar **SC700-WS Quanten-Computing - Store now, decrypt later** die aktuellen Verfahren der Kryptografie kennen und auch welche Gefahren von Quantencomputern aus gehen. Hierfür erlangen sie einen kurzen Einblick in die Funktionsweise von Quantencomputer und betrachten erste Maßnahmen für die 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**