SC460 Secure Architecture and Design

Kurzbeschreibung:

Die Welt verändert sich rasend schnell und mit ihr der Bedarf an neuen Technologien. Dadurch steigt auch das Risiko für digitale Bedrohungen und die Bedeutung von Cybersicherheit steigt. Organisationen und Unternehmen benötigen eine Vielzahl komplexer Systeme und Maßnahmen, um den Schutz und die Sicherheit von großen Datenmengen und wichtigen Vermögenswerten zu gewährleisten. Durch eine veraltete und lückenhafte Sicherheitsarchitektur werden Unternehmen zur Zielscheibe für interne und externe Hackerangriffe. Aus diesem Grund müssen Architekturkonzepte so entwickelt sein, dass sie eine möglichst geringe Angriffsfläche bieten. Der Workshop **SC460 Secure Architecture and Design** befähigt Sie, derartigen Bedrohungen entgegenzuwirken.

Secure Architecture and Design ist Grundvoraussetzung, um eine sichere Anwendung zu bauen. Dabei kann man eine sichere Architektur durch unterschiedliche Herangehensweisen erreichen, entweder mithilfe einer klassischen, etwas „mechanischen“ Methode, in der der BSI-Grundschutz zur Anwendung kommt oder alternativ über etwas freiere risikobasiertere Methoden.

In diesem Seminar werden Sie unterschiedliche Verfahrensweisen kennenlernen. Der Fokus liegt auf zwei wesentlichen Perspektiven. In der Best Practice Perspektive wird die Anwendung allgemein anerkannter Design-Prinzipien näher beleuchtet. Die Bedrohungsperspektive macht deutlich, was alles schief gehen kann. In diesem Zusammenhang lernen Sie Threat Modeling kennen. Mit dieser sehr bewerten konzeptionellen Analysetechnik lassen sich potenzielle Schwachstellen und Risiken bereits frühzeitig bei der Entwicklung von Anwendungen idenzifizieren und erforderliche Maßnahmen ableiten.

Der Kurs legt besonderen Wert auf praxisnahe Anwendungen, indem zahlreiche Übungen angeboten werden, die es den Teilnehmern ermöglichen, ihr erlerntes Wissen direkt in die Tat umzusetzen und zu festigen.

Der Kurs ist Teil des "qSkills Secure Software Quadrant", bestehend aus:

- SC460 Secure Architecture and Design
- SC470 Secure Development Principles
- SC475 OWASP Security Champion
- SC480 Secure Operations

Zielgruppe:

Das Training **SC460 Secure Architecture and Design** ist ideal geeignet für:

- Software Entwickler
- Software Architekten
- Cloud Architekten

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **SC460 Secure Architecture and Design** gut folgen zu können, sollten Sie folgende Voraussetzungen mitbringen:

- grundlegende IT-Kenntnisse
- gundlegende IT-Security-Begriffe

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus Mwst.

Ziele:

Das Training **SC460 Secure Architecture and Design** hat folgende Kursziele:

- Kenntnis und Anwendung gängiger Security Design Prinzipien
- Fähigkeiten einen Threat Model Workshop durchzuführen
- Wissen über gängige Design-Schwachstellen und deren Behebung

Inhalte/Agenda:

- ♦ **Security-Design-Prinzipien – Einführung, Anwendung und Messbarkeit**
- ♦ **Vertrauen / Trust-Principals**
  - ♦ ◊ „Never trust the Client“
  - ◊ „Zero Trust“
  - ◊ „Trusted 3rd Party“

♦ **Secure◊Design - Authentication**

- ♦ ◊ Sichere Identifier / Identities
  - ◊ Password-Based Authentication
  - ◊ Sichere Einsatz von Krypto-Verfahren
  - ◊ Kerkhof’s Principal

♦ **Secure◊Design Prinzipien: Autorisierung**

- ♦ ◊ „Segregation of Duties“
  - ◊ „Least Privilege“
  - ◊ „Avoid Broadly generic functions“
  - ◊ “Authorize close to the source”
  - ◊ „Extension of Kerkhoffs-Principle“

♦ **Weitere◊ Prinzipien im Überflug**

- ♦ ◊ „Do not be Chatty“
  - ◊ „Encrypt High“
  - ◊ „Decrease visibility“

♦ **Secure◊Design – Input / Output / Communication**

- ♦ ◊ „Input-Validierung“
  - ◊ „Output- Validierung“
  - ◊ „Black-Listing / White-Listing“
  - ◊ „Do not interpret – discard“
  - ◊ “Intercept – do not process”
  - ◊ “Don’t call me – I call you!”
  - ◊ “Resilient Design”

♦ **Secure◊Design – “Reste-Rampe”**

- ♦ ◊ “Visibility”
  - ◊ “Default is tight”
  - ◊ “Fail save”
  - ◊ “Double book-keeping”
  - ◊ “No Filesystem”

♦ **Threat-◊Modelling**

- ♦ ◊ Einführung, Anwendung, Historie, Grundlagen

♦ **Threat-◊Modelling-Methoden**

- ♦ ◊ Misuse-Cases
  - ◊ Attack-Trees
  - ◊ STRIDE
  - ◊ EoP-Card-Game
  - ◊ Tools
  - ◊ Application-Level-Threat-Modelling

♦ **Schwach◊stellen und Praxis-Übung**

- ♦ ◊ Identity Management
  - ◊ Authentication
  - ◊ Authorization

♦ **Schwach◊stellen**

- ♦ ◊ Kommunikation
  - ◊ Speicher
  - ◊ Input-Attacks
  - ◊ Angriffe durch privilegierte Benutzer
  - ◊ Angriffs-Erkennung
  - ◊

- Nachvollziehbarkeit
- Angriffe über die Infrastruktur
- Datenschutz
- Open-Source-Security
- Angriffe auf Software-Lebenszyklus
- Angriffe auf Krypto
- Angriffe auf Fehler-Situation

- **Bewertung von Schwachstellen**
  - Angriffs-Vektor
  - CVSS
  - Risiko-Bewertung

- **Workshops durchführen und dokumentieren**

- **Moderation eines Workshops**

- **Abschluss-Übung**
  - Threat Modelling
  - Risiko-Bewertung der Findings
  - Secure Design-Maßnahmen analysieren

- **Viele praktische Übungen zu den einzelnen Modulen**