Stand 16.06.2026

Security: Sicheres Update und Boot - Praktische Umsetzung für moderne Embedded-Systeme - Präsenz-Training

**Ziele -
Ihr Nutzen**

Sie wissen um potientielle Sicherheitslücken in eingebetteten Systemen (embedded systems) wie z.B. IoT und können Risiken anhand ausgewählter Methoden bewerten.

Geeignete Gegenmaßnahmen werden anhand von Secure Boot und Update erläutert und deren Umsetzung demonstriert.

Abschließend findet eine Überprüfung auf Wirksamkeit statt.

IHRE VORTEILE:

Effektiver und praxisnaher Aufbau, praktische Tipps zu Security und Safety, Live-Demonstrationen.

Teilnehmer

Hardware- und Software-Architekten, Hardware- und Software-Entwickler, Testingenieure, Projektmanager, Systemingenieure

Voraussetzungen

Grundverständnis für eingebettete Systeme sowie Grundkenntnisse im Bereich Security

Security: Sicheres Update und Boot - Praktische Umsetzung für moderne Embedded-Systeme - Präsenz-Training

Inhalt

Bedrohungsanalyse

Angreifermodell

- Vorstellung Use Cases
- Brainstorming: Angriffspfade
- Zusammenfassung Angriffe

Bedrohungen (anhand verschiedener Verfahren)

- Stride
- TRIKE
- Tools

Normen

- ISO27000-Familie
- BSI-Grundschutzkatalog
- NIST SP 800-30: Guide for Conducting Risk Assessments

Risikoanalyse

Assets

- Vorstellung SIBASE Demonstrator Assets
- Brainstorm: IoT Assets

Risikobewertung (anhand verschiedener Verfahren)

- DREAD
- EVITA

- Tools

Normen

- BSI-Standard 200-3(CD) Risikoanalyse auf der Basis von IT-Grundschutz
- NIST SP 800-30: Guide for Conducting Risk Assessments

Gegenmaßnahmen

Secure Boot

- Chain of Trust
- Anwendung von Crypto
- Anwendung von HW-Security (TPM 1.2)
- Alternativen

Secure Update am Beispiel SIBASE

- Secure Communication
- Grundsätze sicherer Kommunikation am Beispiel IoT
- Identifikations-/Authentifikationsmechanismen
- Ablauf des Updates
- Anwendung von Crypto (AES,RSA,(EC)DH)
- Behandlung der Credentials

Umsetzung (Implementierung erläutern)

- Sicherer Entwicklungsprozess
- Microsoft Security Development Lifecycle

Protokolle für Secure Communication

- TLS am IoT Sensor
- IPSEC bei ATV-Ethernet

Turnkey Solutions

- Übersicht mit Fähigkeiten
- Insight TPM2.0

Evaluierung / Überprüfung Wirksamkeit

- SIBASE Demo
- IOT TLS Demo
- TPM Demo (TPM2.0 Policies, Secure Boot)

Präsenz-Training

Preis *	Dauer
-	1 Tag

Anmeldecode: SECUP
* Preis je Teilnehmer, in Euro zzgl. USt.

Coaching

Unsere Coaching-Angebote bieten den großen Vorteil, dass unsere Experten ihr Wissen und ihre Erfahrungen direkt in Ihren Lösungsprozess einbringen und damit unmittelbar zu Ihrem Projekterfolg beitragen.

Für Ihre Anfrage oder weiterführende Informationen stehen wir Ihnen gern zur Verfügung.