MICRO CONSULT

Stand 16.06.2026

Security: Kryptographie und sichere Systeme

**Ziele -
Ihr Nutzen**

Sie erhalten einen Einblick in die Methoden der Kryptographie und Kryptoanalyse, das Design sicherer Anwendungen und die Abwehr-Mechanismen für potenzielle Angriffe. Mit Beispielprogrammen vertiefen und veranschaulichen Sie dieses Wissen. Zahlreiche Hinweise zur Entwicklung und Umsetzung sicherer Applikationen unter Linux sind Ihnen eine Hilfe für die spätere Praxis.

Teilnehmer

Softwareentwickler, Entwicklungsleiter, Systemarchitekten

Voraussetzungen

Linux-Grundkenntnisse, Programmierkenntnisse in C

Security: Kryptographie und sichere Systeme

Inhalt

Grundlagen der Kryptographie

- Chiffrierung, Integrität, Authentifizierung
- Algorithmen und Hashfunktionen
- Kryptografische Protokolle
- Public Key Infrastructures (PKI) und Zertifikate

Kryprographie in der Anwendung

- Beispiele für sichere Algorithmen
- Betriebsmodi und deren Bedeutung
- Wie erreicht man Integrität? HMAC und digitale Signaturen
- Secure Boot und Systeme in feindlicher Hand

Key-Handling und Passwörter

- Angriffe auf Public-Key-Verfahren, Chiffrierung und Integrität
- Protokolle: Replay und Denial of Service (DoS)

Applikationssicherheit unter Linux

- Secure Application Design: Speicher- und Ressourcen-Schutz in Applikationen
- User Privileges
- Capabilities
- Namespaces und Container
- Madatory Access Control

Wege zum sicheren System

- Authentifizierung unter Linux nutzen: PAM
- Auswahl von Algorithmen und Protokollen
- Ausgewählte freie Software
- Besonderheiten bei der Implementierung von Kryptographie
- Gängige Fehler und Sicherheitslücken

Präsenz-Training

Preis *	Dauer
-	3 Tage

Anmeldecode: KRYPTO
* 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.