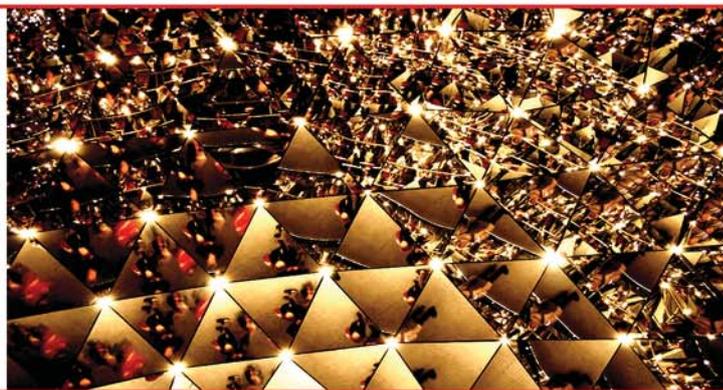




Schulungen und Seminare



PCI DSS Einführung
Grundlagen, Praxis



Schulung Informationssicherheit

Einführung in den Standard der Payment Card Industry, PCI DSS

ZIELGRUPPE

Führungskräfte, Behördenleiter, IT-Leiter, Revisoren, Sicherheitsbeauftragte, Administratoren, Systembetreuer, Datenschutzbeauftragte.

VORAUSSETZUNGEN

Grundlagen IT-Sicherheit, Informationssicherheit

SEMINARZIELE

- Grundlagen PCI DSS Standards
- Zweck des Standards
- Sicherheitsziele und Richtlinien
- Die Sektionen und Controls
- Organisation und Technik
- Auswirkungen der Einführung von PCI DSS auf eine Organisation
- Die Vorteile einer Zertifizierung
- Folgen bei Nichterfüllung von Anforderungen /Gesetzen

AUFBAUKURSE: ISO27001:2005, IT-Recht

METHODE:

Vortrag, Präsentation, Diskussion, Beispiele aus der Praxis, Erfahrungen aus Projekten.

KURSSPRACHE:

deutsch

DAUER & ABLAUF:

2 Tage

Beginn: 9:00 Uhr **Ende:** 17:00 Uhr

Pausen: Mittag, ca. 12:30 - 13:30 Uhr
Kaffeepause jeweils ca. 15 min
vormittags und nachmittags

ORT:

axivia GmbH
Industriering 7,
63868 Großwallstadt

KURSBESCHREIBUNG:

PCI-Compliance (-Konformität) ist für Sie und Ihre Organisation eine kritische und wichtige Aufgabe. axivia und SRC haben ein maßgeschneidertes 2-Tagestraining entwickelt, um die unternehmensrelevanten Anforderungen des Standards der Payment Card Industry - PCI DSS - zu verstehen und die Grundlagen für eine erfolgreiche, dauerhafte Umsetzung und Zertifizierung zu schaffen.

KURSAUFBAU:

Tag1: Einführung in den PCI-DSS

- PCI Motivation
- Präsentation und Interpretation der PCI DSS Anforderungen
- Rollen: Händler, Service Provider, Software Vendor
- PCI DSS Scope
- Häufige Missverständnisse
- Präsentation und Diskussion verschiedener Strategien zur Umsetzung
- Erfahrungen und typische Probleme
- Fragen und Antworten

Tag2: PCI DSS in Ihrem Hause

- Analyse der PCI DSS Umgebung (PCI DSS Scope)
- Detaillierte Diskussion einzelner Anforderungen, Umsetzungsstrategien
- Compliance Validation: SAQ, Security Scan und Security Audit

Fokus z.B. auf:

- Verschlüsselung / Key Management
- ISMS (Policies, Procedures, etc.)
- Netzwerk Konfiguration
- Diskussion eines "Sample Report on Compliance"
- technische Fallbeispiele aus der Praxis (SIEM, Log-Management, Verschlüsselung)
- Fragen & Antworten

REFERENTEN:

Manuel Atug
SRC Security Research & Consulting GmbH

Reinald Kempf, ISO27001 Lead Auditor
axivia GmbH