

Unternehmen sind nicht nur von vorsätzlichen Handlungen Externer betroffen, sondern auch von Handlungen, die von internen gesetzt werden und damit das Unternehmen finanziell oder in seinem Ruf schädigen können. Solchen Bedrohungen gewachsen zu sein ist für Unternehmen eine Herausforderung, die besonderer Mittel und Wege Bedarf.

Die Teilnehmer lernen Verbrechenmuster kennen, die sich innerhalb von IT-Abteilungen abspielen, deren Erkennung und Behandlung (sowie Auswirkungen) und erwerben die Grundlagen, das Erlernte in interne Kontrollsysteme (IKS) zu integrieren.

Voraussetzungen

Keine

Preis pro Teilnehmer

EUR 1400,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

Version: N/A

Seminarinhalte

- * Differenzierung
 - Verbrechen
 - Vergehen
 - Cybercrime
- * Behandlung
 - Reale Fallbeispiele der Behandlung
 - die daraus folgenden Lessons Learned
- * Vorbeugungsmaßnahmen
 - auf juristischer Ebene
 - auf technischer Ebene
- * Erkennungsmaßnahmen zur frühzeitigen Erkennung

