Organisation, Anmeldung & Ansprechpartner in Regensburg:
R-Tech GmbH
Natalie Schwab
Franz-Mayer-Str. 1
93053 Regensburg
Fon: +49 (0) 041 / 604 889 – 20
Fax: +49 (0) 041 / 604 889 – 11
E-Mail: natalie.schwab@it-sec-cluster.de

Organisation, Anmeldung & Ansprechpartner in Augsburg:
aiti-Park – IT-Gründerzentrum GmbH
Evi Trinker
Werner-von-Siemens-Str. 6
86159 Augsburg
Fon: +49 (0) 821 / 450 433 - 0
Fax: +49 (0) 821 / 450 433 - 109
E-Mail: info@aitiRaum.de

Ideeller Träger
Bayerischer IT-Sicherheitscluster e.V.
Franz-Mayer-Str. 1
93053 Regensburg
Telefon: +49-(0)941-604889-18
Telefax: +49-(0)941-604889-11
sandra.wiesbeck@it-sec-cluster.de

Titelbilder
www.fotolia.de

TERMINE UND ORTE IN 2016:

Regensburg (IT-Speicher):
1. Lehrgang: 17.2.+18.2./16.3.+17.3. (jeweils 9:00-17:00 Uhr)
2. Lehrgang: 21.9.+22.9./26.10.+27.10.(jeweils 9:00-17:00 Uhr)

Augsburg (aiti-Park):
Lehrgang: 11.5.+12.5./8.6.+9.6. (jeweils 9:00-17:00 Uhr)

Nachhaltig fördern:
Informationssicherheit erfordert eine kontinuierliche Auseinandersetzung mit dem Thema. Deswegen verstehen wir unseren Zertifikatslehrgang als den Beginn und nicht das Ende der Reise. Auch nach erfolgreichem Abschluss versorgen wir unsere Informationssicherheits-Beauftragten mit aktuellem Wissen und praktischen Lösungsansätzen im Rahmen des Anwenderkreises »Informationssicherheit in der Praxis« des Bayerischen IT-Sicherheitsclusters e.V.

Dauer und Preis:
Dauer: 4 Tage
Gerne reservieren wir in unseren ausgesuchten Schulungs-Hotels auch ein Zimmer zu speziellen Konditionen für Sie.

Teilnehmerzahl: Mindestens 4, maximal 12 Personen
Bei zu geringer Teilnehmerzahl behält sich die R-Tech GmbH vor, die Veranstaltung 14 Tage vor Beginn abzusagen.

Seminarpreis:
2.100,- € inkl. Prüfungsgebühren zzgl. gesetzl. Mwst.
Im Preis enthalten sind Getränke, Mittagessen sowie Schulungsunterlagen. Mitglieder des Bayerischen IT-Sicherheitsclusters e.V. sowie der weiteren Netzwerke der R-Tech GmbH erhalten 20 % Ermäßigung.

Zielgruppe:
EDV-Leiter, IT-Verantwortliche, IT-(Projekt)Manager bzw. IT-Verantwortliche innerhalb von Projektteams, Sachverständige, Datenschutzbeauftragte, Berater, aktive bzw. angehende Informationssicherheits-Beauftragte

Lernziele:
- Entwicklung eines Verständnisses für die Notwendigkeit einer unternehmensweiten Informationssicherheit
- Vermittlung strategischer Konzepte und Einführung in relevante IT-Grundlagen
- Durchführung einer Risikoanalyse und Implementierung eines Risikomanagements
- Zusammenhänge erkennen: Best practices, ISMS, Risikomanagement, Audit und Zertifizierung

ITSECURITY
Bavarian IT Security & Safety Cluster

ZERTIFIKATSLEHRGANG INFORMATIONSSICHERHEITS-BEAUFTRAGTER

IN KOOPERATION MIT

OTH REGENSBURG

Mit dem Zertifikatslehrgang »Informationssicherheits-Beauftragter« bietet der Bayerische IT-Sicherheitscluster e.V. Unternehmen und Organisationen die Möglichkeit, Mitarbeiter für die Funktion des Informationssicherheits-Beauftragten zu qualifizieren.

→ DAS KONZEPT

Im Gegensatz zu herkömmlichen Schulungen, ist die unmittelbare Verbindung der Wissensvermittlung mit der direkten praktischen Umsetzung in der eigenen Organisation explizit Bestandteil des Lehrgangs. Bewusst sind zwischen den einzelnen Lehrgangsveranstaltungen Praxisphasen von rund 4 Wochen eingeplant, um das neu erworbene Wissen direkt anzuwenden, aber auch den nachfolgenden Block anhand der Situation im eigenen Unternehmen vorzubereiten.
Inhaltlich fokussiert der Zertifikatslehrgang auf praxisrelevante organisatorische, rechtliche und technische Themen und hebt sich auch mit diesem Ansatz von anderen Seminaren in diesem Bereich ab.

Vorteile des Zertifikatslehrgangs sind:
- 4 Schulungstage werden auf 4 Wochen verteilt
- Direkte Umsetzung des vermittelten Wissens im eigenen Unternehmen als Teil des Ausbildungskonzeptes
- Hohe Praxisrelevanz durch erfahrene Experten

→ BLOCK 1 (1 TAG)

- **Der Informationssicherheits-Beauftragte**
  Organisatorische Stellung, Aufgaben und Verantwortlichkeiten.

- **Einführung wesentlicher Fachtermini**
  Erläuterung relevanter Begriffe wie Vertraulichkeit, Integrität und Verfügbarkeit, Schutzbedarf, Sicherheitsvorfall und -kategorisierung und weitere.

- **IT-Risikomanagement**
  Vorgehen zur Analyse, Bewertung, Reduktion und Akzeptanz von IT-Risiken.

- **Rechtliche Aspekte**
  Darstellung relevanter Vorschriften und Gesetze zu Datenschutz und Informationssicherheit.

- **Haftungsrisiken für IT-Verantwortliche und Geschäftsführung**

  Relevante Gesetze und normative Rechtsgrundlagen der IT-Compliance. Zivilrechtliche Haftung für Verstöße und mangelnde Betriebsorganisation. Strafdrohungen, Bußgelder.
  Eigenhaftung der Leitungsebene und der Beschäftigten Haftungsmaßstab, Schadensszenarios.
  Rechtsfragen des Cloud Computing: Anbieterauswahl, Vertragsgestaltung, Datentransfer ins Ausland

- Einweisung in das kursbegleitende »**Handbuch Informationssicherheits-Beauftragter**

Ab 19:00 Uhr gemeinsames Abendessen

→ BLOCK 2 (1 TAG)

- **»Informationssicherheitskonzept« und weitere zentrale Dokumente**
  Darstellung typischer Richtlinien und Anweisungen sowie deren Abstimmung mit übergeordneten Leitlinien.

- **»Awareness« und Kommunikation**
  Methoden und Inhalte sinnvoller Sensibilisierungsmaßnahmen.

- **Standards und Rahmenwerke**
  Einführung in die gängigen Standards ISO27001, BSI IT-Grundschutz, ISIS12, ISA+.

- **Informationssicherheit als kontinuierlicher Prozess**

- **Herausforderung für den Informationssicherheits-Beauftragten:**
  - Durchsetzung in der Organisation
  - Zusammenarbeit mit dem Datenschutzbeauftragten, QM
  - Berichtswesen (Revision, Jahresbericht, interne Reviews)

→ BLOCK 3 (1 TAG)

- **Grundprinzipien der technischen Informationssicherheit**
  Darstellung von Struktur und Komponenten moderner IT-Landschaften, Benutzerberechtigungskonzept, Patch- & Updatemanagement, Datensicherung und Backup, Zutritts- & Zugangskontrolle.

- **Grundlagen Netzwerktechnologie**
  Einführung in das OSI-Modell und Netztopologien; Funktionsweise von Netzwerkkomponenten und -schutzsystemen.

- **Einsatz mobiler Geräte**
  Typische Nutzungsszenarios, Bedrohungslage und Anforderungen im Unternehmenseinsatz.

- **Kontrolle und Überwachung**
  Organisatorische und technische Möglichkeiten (z.B. Logfile-Analyse / SIEM).

→ BLOCK 4 (1 TAG)

- **Cloud Computing**
  Erläuterung von organisatorischen, technischen und rechtlichen Faktoren.

- **Verschlüsselung**
  Schutz von Daten »at rest«, »in motion«, »in use« sowie Absicherung von Kommunikation und Internetnutzung.

- **»Round up«**
  Wiederholung der bisherigen Themen anhand einer praxisbezogenen Fallstudie.

im Anschluss optional:
Ablegen einer schriftlichen Prüfung zur Erlangung des Hochschul-Zertifikats »Informationssicherheits-Beauftragter«.