Cyber Security
Zusatzqualifikation für IT-Berufe (IHK)

Aufgrund der immer häufiger werdenden Angriffe auf die IT-Systeme von Unternehmen, Verwaltungen und Behörden ist es unumgänglich, dass Mitarbeiter IT-Spezialkenntnisse haben müssen, damit sie die digitalen Daten und Systeme im Unternehmen schützen können.
Hierfür sind neue Qualifikationen notwendig, um künftig über geeignete Fachkräfte zu verfügen. Mit der Zusatzqualifikation Cyber Security erwerben die Teilnehmer jetzt das dringend benötigte Know-how über IT-Sicherheit und Datenschutz. Die Qualifizierung ist auch für ausgebildete Fachkräfte im Rahmen des Qualifizierungschancengesetzes offen.
Der Lehrgang bereitet die Teilnehmer auf die Prüfung vor der IHK vor.

Herzlich Willkommen bei BISA.

IT education

BISA IT training approved qualification

Ready to be a CISO
Chief Information Security Officer

VORTEILE UND BENEFITS

- Umsetzung bereits in der Lernphase (Training-on-the-Job)
- Individuelle Betreuung auch nach der Schulung
- Best-Practice aus IT-Technik / Beratung / Schulung und Training
- IHK-Abschluss

OUTPUTS

- Analyse von rechtlichen Vorgaben zur Informationssicherheit und IT-Compliance
- Umsetzung der Anforderungen an eine Cyber-Abwehr
- Beurteilung von Gefährdungen und Risiken
- Anwendung von Methoden der Kryptographie
- Analyse der Bedrohungen von Web-Services und Applikationen
- Unterscheidung und kontrollierter Einsatz von Tools zum Angreifen von Webservices zur Schwachstellenanalyse
- Umsetzung der Methoden und Werkzeuge der digitalen Forensik

ORGANISATION:

Der Lehrgang findet berufsbegleitend an zwei Tagen in der Woche statt. Der Umfang beträgt 320 UE.
Bei geschlossenen Gruppen sind weitere Zeitmodelle möglich.

Kosten des Lehrgangs € 5.980

Die Philosophie von BISA:

BILDUNG. WISSEN. BERNARDS.

Wir stehen für effektive, pragmatische und einfache Lösungen sowie eine höfliche, ehrliche und transparente Zusammenarbeit auf Augenhöhe.

BERNARDS INFORMATION SECURITY ACADEMY
Am Hofgarten 20 | 53113 Bonn

UNSER PODCAST

IT-SECURITY **IS A UNICORN**

rb@bernards-akademie.de
+49 178 / 8500101

ANALYSE VON RECHTLICHEN VORGABEN ZUR INFORMATIONSSICHERHEIT UND IT-COMPLIANCE

- EU-DSGVO -> nationale Gesetze (BDSG)
- ISO-Normen -> ISO 27001 (ISMS)
- ISO-Normen -> ISO 9001 (Qualitätsmanagement)
- ISO-Normen -> ISO 31000 (Risikomanagement)
- Telekommunikationsgesetz (TKG)
- Nutzungsdatenerfassung (z.B. Webseiten, Cloud-Services)
- Geheimschutzhandbuch (BMWi)
- BaFin (Wirtschaftsrecht)
- PCIDSS (max 2h)
- Hackerparagraph (Ausspähen und Abfangen von Daten, StGB §202)

UMSETZUNG DER ANFORDERUNGEN AN EINE CYBER-ABWEHR

- Grundlegende Begriffe
- Security Management
- Ziele und Motivation
- Social Engineering
- Riskmanagement
- Definition von Rollen
- Security Architektur
- Information Protection"
- Weitere Inhalte
- Identity Access Management
- Was sind Rollen- und Rechtekonzepte
- Kryptographie
- Grundlagen: symmetrische und asymmetrische Verschlüsselung
- Datei- und Transportverschlüsselung
- Physische Sicherheit
- Kennenlernen der wesentlichen Prinzipien wie Zutrittsschutz
- Business Continuity Management
- Ziele, Motivation und grundlegende Techniken

ANALYSE DER BEDROHUNGEN VON WEB-SERVICES UND APPLIKATIONEN

- Prinzipien der sicheren Anwendungsentwicklung kennenlernen und umsetzen
- OWASP Top 10 für Web Anwendungen
- Grundlagen zu Web Services
- OWASP Top 10 für Web Services
- Angriffsszenarien kennenlernen
- Bsp. SQL-Injection (wie funktioniert diese? Was kann man dagegen tun?)
- Gegenmaßnahmen definieren
- Scan-Berichte lesen und interpretieren können (Bsp. QUALYS)
- Tools zum Angreifen von Web-Services kennenlernen und einsetzen
- Landing-Zones im Cloud-Umfeld (Datenhaltung in der Cloud) (Telekom spez.)

UMSETZUNG DER METHODEN UND WERKZEUGE DER DIGITALEN FORENSIK

- IT-Forensik
- Ziele der IT-Forensik
- Rechtliche Rahmenregelungen
- Sicherstellen von Beweisen, um forensische Untersuchungen durchführen zu können
- Prinzipien der IT-Forensik
- Gängige Tools der IT-Forensik kennenlernen
- Schwerpunkt deren besonderer Einsatzbereich