Industrie- und Handelskammer
Bonn/Rhein-Sieg

Zusatzqualifikation Cybersecurity

Die folgende Handreichung soll Ihnen helfen die Inhalte der Zusatzqualifizierung in Ihren betrieblichen Ablauf zu integrieren. Unser Dank gilt der Telekom Ausbildung, die in Zusammenarbeit mit dem Berufsbildungsausschuss der IHK Bonn/Rhein-Sieg dieses Papier erarbeitet hat.

§ 2 Abs. 1 Nr. a

Rechtliche Vorgaben zur Informationssicherheit und IT-Compliance anwendungsbezogen analysieren

Inhalte/Lernziele (Fertigkeiten, Kompetenzen, Fähigkeiten - FKF)

Schutzziele des Datenschutzes und der IT-Sicherheit auch aus unternehmerischer Perspektive analysieren

Bestimmungen und Zusammenspiel von Vorgaben zur Informationssicherheit und IT-Compliance unterscheiden

Dauer (Empfehlung Bruttowochenangabe)

1 Woche

Kurzbeschreibung

Welche Anforderungen außerhalb des Unternehmens gibt es und wie beeinflussen sie interne Prozesse und Richtlinien?

Es wird erwartet, dass der Prüfling wesentliche Bestimmungen und die daraus abzuleitenden Regelungen kennt.

Inhalte

- EU-DSGVO -> nationale Gesetz (BDSG)
- ISO-Normen -> ISO 27001 (ISMS), ISO 9001 (Quality Mgmt), ISO 31000 (Risk Mgmt)
- Telekommunikationsgesetz (TKG)
- Nutzungsdatenerfassung (z.B. Webseiten, Cloud-Services)
- Geheimschutzhandbuch (BMWi)
- BaFin (Wirtschaftsrecht), PCIDSS (int. Standard für Verwendung von Kreditkarteninformationen)
- Hackerparagraph (Ausspähen und Abfangen von Daten, StGB §202)

§ 2 Abs. 1 Nr. b

Methoden, Konzepte und Werkzeuge der IT-Sicherheit definieren und einsetzen

Inhalte/Lernziele (Fertigkeiten, Kompetenzen, Fähigkeiten - FKF)

Merkmale und Anforderungen einer „Cyber-Abwehr“ definieren

Gefährdungen und Risiken beurteilen sowie Techniken und Tools der Abwehr einsetzen

Risikomanagementprozesse und -konzepte nach Vorgaben anwenden

Grundbegriffe sowie Methoden der Kryptographie unterscheiden und bestehende Kryptographie-Algorithmen anwenden

Dauer (Empfehlung Bruttowochenangabe)

1 Woche

Kurzbeschreibung

Erarbeitung wesentlicher Merkmale und Anforderungen einer Cyber-Abwehr.

Vertiefung der Grundkenntnisse und Weiterentwicklung in spezifische Anforderungen der IT-Sicherheit wie Zugangssicherheit, Security Architektur, Kryptographie etc..

Kenntnisse zur Gefährdungslage und die Techniken der Abwehr werden erarbeitet.

Dabei werden auch zentrale Fragen des Umgangs mit Risiken und Fähigkeiten zur Risikoanalyse sowie Grundkenntnisse bearbeitet, die der Absicherung des Unternehmens/Betriebs im Schadenfall dienen.

Inhalte

- Security Management
  - Ziele und Motivation
  - Social Engineering
- Riskmanagement
  - Definition von Risiken, Risiken erkennen, Umgang mit Risiken
- Security Architektur
  - Information Protection
  - Plattform Architekturen
- Identity Access Management
  - Was sind Rollen- und Rechtekonzepte?
- Kryptographie
  - Grundlagen: symmetrische und asymmetrische Verschlüsselung, etc.
  - Datei- und Transportverschlüsselung
- Physische Sicherheit
  - Kennenlernen der wesentlichen Prinzipien wie Zutrittsschutz
- Business Continuity Management
  - Ziele, Motivation und grundlegende Techniken

Zusatzqualifikation Cyber Security

§ 2 Abs. 1 Nr. c

Bedrohungen für, Angriffe auf und Schwachstellen von Web-Services sowie Applikationen analysieren

Inhalte/Lernziele (Fertigkeiten, Kompetenzen, Fähigkeiten - FKF)

Sicherheitsanforderungen von Webservices und Applikationen analysieren

Angriffsszenarien auf Webservices und Anwendungen identifizieren und unterscheiden

Tools zum Angreifen von Webservices und Anwendungen unterscheiden und kontrolliert anwenden

Gegenmaßnahmen ableiten, abstimmen und im Team umsetzen

Prinzipien der sicheren Anwendungsentwicklung anwenden

Datenbanksysteme testen und optimieren, dabei Sicherheitsmechanismen, insbesondere Zugriffsmöglichkeiten und -rechte, festlegen und implementieren

Dauer (Empfehlung Bruttowochenangabe)

4 Wochen

Kurzbeschreibung

Erwerb von Kenntnissen zu IT-Sicherheit und Datenschutz bei der Entwicklung und dem Betrieb von Anwendungen, Web Services und auch Datenbanken.

Unterscheiden der Begriffe, Konzepte und Praktiken der Web Application Security (WAS).

Kennenlernen der häufigsten Angriffe auf Webanwendungen und möglicher Gegenmaßnahmen.

Inhalte

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

Zusatzqualifikation Cyber Security

§ 2 Abs.1 Nr. d

Methoden und Werkzeuge digitaler Forensik einsetzen

Inhalte/Lernziele (Fertigkeiten, Kompetenzen, Fähigkeiten - FKF)

Rechtliche Grundlagen für forensische Untersuchungen analysieren und nach Vorgaben

anwenden Prinzipien der IT Forensik unterscheiden

forensische Untersuchungen an IT-Systemen vorbereiten und unterstützen

Dauer (Empfehlung Bruttowochenangabe)

2 Wochen

Kurzbeschreibung

Erwerb von Kenntnissen der generellen Themen sowie von Methoden und Tools der digitalen Forensik.

Aufbauend auf den juristischen Grundlagen ist die Fähigkeit zur beweisfesten Spurensicherung in IT- Security eine unerlässliche Kompetenz in der IT-Sicherheit.

Die erforderlichen Kenntnisse werden erworben. Ein generelles Verständnis wird geschaffen.

Inhalte

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

Zusatzqualifikation Cyber Security
Ideen/Beispiele für praxisbezogene Aufgaben

Bitte beachten Sie, dass solche Aufgaben im Betrieb tatsächlich eigenständig durchgeführt werden müssen.

- Für eine Webanwendung oder ein „Asset“ erfolgt eine Bestimmung des Risikos. Dazu spielen neben den Anschaffungskosten für ein IT-System oder Entwicklungskosten für ein Programm bei der Beurteilung weitere Faktoren eine Rolle, die in der praxisbezogenen Aufgabe analysiert und erläutert werden. (Schadensszenario und Risiko)
- Es soll der Aufbau einer neuen Webpräsenz erfolgen, dazu sind die Anforderungen zu analysieren und zu beschreiben. Nach dem Aufbau auf Basis eines Apache Webservers ist die regelmäßige Auswertung der Protokolldateien access.log und error.log erforderlich. Es wird der Aufbau der Logfiles erläutert und die die Informationen im Hinblick auf datenschutzrechtliche Rahmenbedingungen beurteilt.
- Kampagne „Social Hacking“ für eine Abteilung/ein Unternehmen/einen Geschäftskunden mit planen und durchführen (Mitarbeitende erhalten vorbereitete Phishing E-Mails, Erstellen eines Ergebnisberichts, der das Verhalten transparent macht)
- Analyse eines Angriffs auf ein IT-System durch eine sicherheitskritische Schwachstelle am Beispiel aktueller Sicherheitsvorfälle aus der Presse durchführen
- Einen Datenträger selbst IT-forensisch sichern und die Sicherung geeignet dokumentieren (am Beispiel eines zu untersuchenden Windows-Systems, mit dem Dateisystem NTFS und zugehörigen Windows- und Anwendungs-Artefakten, und unter überwiegender Nutzung von Windows als Auswertungsumgebung)
- Durchführen einer forensischen Analyse von Datenträgern bspw. Mittels des Tools „autopsy“
- Wiederherstellung gelöschter/beschädigter Daten am Beispiel eines Windows Systems
- „Netzwerkforensik“ in einer Infrastruktur vornehmen, Erzeugen und Analysieren von Packet Captures mit tcpdump und Wireshark u.a. Tools
- Sicheres Duplizieren von Datenträgern als forensische Kopie zur Beweissicherung + Erläuterungen
- Sessionmanagement in eine Webanwendung integrieren
- Einfaches „Reverse Engineering“ einer auf einem IT-System vorgefundenen Malware durchführen
- Honeypot System planen und installieren (+auswerten)
- Entwicklung einer Checkliste zur sicheren Apache-Serverkonfiguration
- Analyse der Sicherheitseigenschaften einer Webanwendung (Web Scanner bzw. Web Application Scanner für Penetrationstests einer Kundenanwendung einsetzen und Ergebnisse dokumentieren) (auf bekannte Schwachstellen untersuchen)
- Einsatz von WebShields- Web Application Firewall bei einem Kundensystem – am Beispiel mod_security des Apache Webservers
- Angriff auf eine Webanwendung simulieren
- Entwicklung eines Rootkits (oder ggf. auch einer Malware) zur Demonstration der Anforderungen für IT-Sicherheit im Rahmen einer Anwenderschulung