SC570 Vorfall-Praktiker des Cyber-Sicherheitsnetzwerks des BSI

Kurzbeschreibung:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist für die Fragen der IT-Sicherheit zuständig. Um das reaktive Angebot im Bereich Cyber Security bzw. IT-Sicherheit zu stärken, wurde das Cyber-Sicherheitsnetzwerk (CSN) als Anlaufstelle zur Vorfallbearbeitung gegründet. Dieser freiwillige Zusammenschluss von qualifizierten IT-Security-Experten hat das Ziel, IT-Sicherheitsvorfälle schneller zu erkennen, zu analysieren, das Schadensausmaß zu begrenzen und weitere Schäden zu verhindern.

Der Workshop **SC570 Vorfall-Praktiker des Cyber-Sicherheitsnetzwerks des BSI** versetzt Sie in die Lage, im Falle von IT-Sicherheitsvorfällen schnell und effektiv vor-Ort-Hilfe leisten und die entsprechenden Prozesse zur Schadensregulierung einleiten zu können.

Zielgruppe:

Der Kurs SC570 Vorfall-Praktiker des Cyber-Sicherheitsnetzwerks des BSI richtet sich insbesondere an Teilnehmer, die bereits über Wissen und Praxis im Bereich Cyber Security verfügen und nun die Registrierung als Vorfall-Praktiker im CSN des BSI anstreben:

- Fachinformatiker
- IT-Techniker/Theoretiker
- ISMS-Experten

Kursteilnehmer sind häufig Entscheider, Berater und Mitarbeiter, die schon über Kenntnisse im Bereich **IT-Sicherheit** und **IT-Technik** verfügen.

Voraussetzungen:

Sie möchten Vorfall-Praktiker werden? Gute Entscheidung!
Ein konkretes Risiko, durch einen IT-Vorfall betroffen zu sein, besteht für ca. 83 Millionen Bürger*innen und ca. 3 Millionen Klein- und Kleinstunternehmen.

Voraussetzung für eine Registrierung beim Cyber-Sicherheitsnetzwerks ist die Qualifizierung zum Digitalen Ersthelfer gemäß dem ACS-Standard zur Digitalen Rettungskette und nachweisbare Kenntnisse im IT-Bereich. Die genauen Anforderungen sind beim Cyber-Sicherheitsnetzwerk des BSI hinterlegt: **Vorfall-Praktiker im CSN**

Sonstiges:

Dauer: 3 Tage

Preis: 1190 Euro plus Mwst.

Ziele:

In diesem 2,5-tägigen Training werden Sie auf die Prüfung zum Vorfall-Praktiker vorbereitet und am letzten (halben) Schulungstag schriftlich sowie mündlich geprüft.

Die Aufbauschulung vermittelt Ihnen den offiziellen Schulungsplan zur Erlangung der Kenntnisse und

Fähigkeiten, die Sie im Rahmen einer Tätigkeit als **Vorfall-Praktiker** benötigen.

In der Gruppe erarbeiten Sie sich Ihre Fähigkeiten zur Behandlung von Informationssicherheitsvorfällen und festigen Ihre Kenntnisse der Cyber Security.

Im Anschluss an den Workshop erhalten alle Kursteilnehmer die Arbeitsergebnisse als Handout, die offiziellen Trainingsunterlagen und den Nachweis über die Teilnahme am Schulungsprogramm.

Als registriertes Schulungsunternehmen im Cyber-sicherheits-Netzwerk bietet qSkills den Kursteilnehmern die Möglichkeit, die Aufbauschulung mit dem Prüfungsworkshop am selben Schulungsort zu verbinden. Nach bestandener Prüfung können sich die Teilnehmer beim Cyber-Sicherheitsnetzwerk als **Vorfall-Praktiker** registrieren.

Hinweis: Im Unterschied zur Prüfung zum Vorfall-Experten (SC580) findet die Prüfung zum Vorfall-Praktiker direkt am dritten Schulungstag bei qSkills im Haus statt. Während die Teilnahme an den ersten beiden Schulungstage sowohl in Präsenz als auch online erfolgen kann, ist die Teilnahme am letzten halben Tag (Prüfungsworkshop) nur in Präsenz möglich.

Nach der Registrierung wird ein Vorfall-Praktiker auf den Webseiten des CSN gelistet und veröffentlicht.

Inhalte/Agenda:

- **Einführung in das CSN und Zusammenfassung der Basiskurse**
  - ◊ Digitale Rettungskette
  - ◊ Rollen und Grenzen der Aufgabe
  - ◊ Rechtliche und gesetzliche Rahmenbedingungen
  - ◊ Zusammenfassung des Basiskurses für Digitale Ersthelfer

- **Verhalten am Telefon incl. nicht technischer Maßnahmen**
  - ◊ Serviceorientiertes Telefongespräch
  - ◊ Nicht technische Maßnahmen

- **Gefährdungen und Angriffsformen und Übersicht über die aktuelle Gefährdungslage**
  - ◊ Begriffserklärung (Gefährdung, Schwachstelle, Bedrohung, Angreifer usw.)
  - ◊ Arten von Angriffen bzw. Angriffsformen
  - ◊ Ursachen von Argriffen
  - ◊ Unterschiedliche Angriffsmethoden
  - ◊ Phasen eines Cyber-Angriffs
  - ◊ Top aktuelle Angriffsformen bzw. aktuelle Gefährdungslage
  - ◊ Feststellen von Angriffen bzw. Infektionen
  - ◊ Handlungsempfehlungen für den Vorfall-Praktiker
  - ◊ Grenzen der Hilfeleistung durch den Vorfall-Praktiker

- **Ablauf des Standardvorgehens**
  - ◊ Vorbereitung auf potenzielle Vorfälle
  - ◊ Identifikation des IT-Sicherheitsvorfalls
  - ◊ Eindämmung des Schadensausmaßes
  - ◊ Ermitteln der Ursachen bzw. Auslöser des IT-Sicherheitsvorfalls
  - ◊ Wiederherstellen der Systeme
  - ◊ Dokumentation des IT-Sicherheitsvorfalls

- **Behandlung von IT-Sicherheitsvorfällen z. B. Phishing-Vorfälle, Ransomware-Vorfällen**
  - ◊ Einführung in Phishing, Phishing-Kanäle, Mögliche Folgen von Phishing
  - ◊ Weitere Informationen zu den häufigsten Folgen und Statistik zum entstandenen wirtschaftlichen Schaden
  - ◊ Erkennung von Phishing-Angriffen, Reaktion auf erfolgreiche Phishing-Attacken
  - ◊ Einführung in Ransomware, Aktuelle Lage zu Ransomware
  - ◊ Typisches Vorgehen von Ransomware-Angreifern
  - ◊ Ransomware-Vorfall bewältigen
  - ◊ Rechtliche Fragen

- **Remote-Unterstützung**
  - ◊ Remote- oder Vor-Ort-Unterstützung
  - ◊ Kommunikation mit dem Kunden
  - ◊ Verbindungs- und Zugriffsmöglichkeiten
  - ◊ Datensammlungs- und Analysemöglichkeiten

- **Vorfallbearbeitung von IT-Systeme „abseits der üblichen Büroanwendung“**
  - ◊ IT-Systeme kommen auch abseits der üblichen Büro-Anwendung zum Einsatz
  - ◊ Beispiele für Architekturen. Welche Technik kommt zum Einsatz?
  - ◊ Was sind mögliche Gefahren für die Steuerungstechnik?
  - ◊ Grenzen der Aufgabe
  - ◊ Ablauf des Standardvorgehen
  - ◊ Angriffsszenarien und Sofort bzw. Gegenmaßnahmen
  - ◊ Grenzen der Analyse

- **Nach einem Vorfall ist vor einem Vorfall**
  - ◊ Sensibilisierung des Unternehmens für präventive Sicherheitsmaßnahmen
  - ◊ Aufbau eines Sicherheitsbewusstseins
  - ◊ Analyse von Geschäftsprozessen
  - ◊ Aufbau eines Sicherheits- und Notfallkonzeptes
  - ◊ Konzeption von Übungen
  - ◊ Info-Paket durch CSN bereitstellen
  - ◊ Aufrechterhaltung der Kompetenz des Vorfall-Praktikers
  - ◊