SC580 Vorfall-Experte des Cyber-Sicherheitsnetzwerks des BSI

Kurzbeschreibung:

Der Workshop vermittelt, wie IT-Sicherheitsvorfälle im Rahmen des BSI-Cybersicherheitsnetzwerks schnell erkannt, analysiert und effektiv vor Ort behandelt werden können. Teilnehmer lernen, das Schadensausmaß zu begrenzen, Folgeschäden zu verhindern und die notwendigen Prozesse zur Regulierung einzuleiten, um betroffene Organisationen gezielt zu unterstützen.

Zielgruppe:

Der Kurs SC580 Vorfall-Experte des Cyber-Sicherheitsnetzwerks des BSI richtet sich insbesondere an Teilnehmer, die bereits über Wissen und Praxis im Bereich Cyber Security verfügen und nun die Zertifizierung zum Vorfall-Experten im CSN des BSI anstreben:

- IT-Leiter
- IT-Sicherheitsbeauftragte (CISO)
- Fachinformatiker
- IT-Techniker/Theoretiker
- ISMS-Experten

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

Voraussetzungen:

Sie möchten Vorfall-Experte 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.

Um für die Teilnahme am Zertifizierungsverfahren zugelassen zu werden, müssen folgende Voraussetzungen erfüllt sein:

- Der Antragsteller muss die mindestens dreitägige Aufbauschulung auf der Grundlage des Curriculums [CUR] besucht haben.
- Bildungsabschluss
  Der Antragsteller muss eine Ausbildung abgeschlossen haben, in der er grundlegende Kenntnisse und Fähigkeiten für seine spätere Tätigkeit als Vorfall-Experte erlangt hat. Hierzu zählt beispielsweise eine abgeschlossene Ausbildung oder ein abgeschlossenes Studium im Bereich IT und/oder Informationssicherheit
- Berufserfahrung
  Der Antragsteller muss aus den letzten acht Jahren mindestens fünf Jahre fachspezifische, praktische Berufserfahrung gerechnet auf Vollzeit im Bereich IT/Informationssicherheit und aus den letzten fünf Jahren mindestens drei Jahre Erfahrung bei der Behandlung von IT-Sicherheitsvorfällen nachweisen.
- Praxiserfahrung
  Der Antragsteller muss in den zurückliegenden drei Jahren (Stichtag: Antragsdatum) an Vorfallbehandlungen oder Projekten mit einem Gesamtumfang von mindestens 40 Personentagen leitend teilgenommen haben.

Die genauen Anforderungen sind beim Cyber-Sicherheitsnetzwerk des BSI hinterlegt: Zertifizierung als Vorfall-Experte

Sonstiges:

Dauer: 3 Tage

Preis: 1580 Euro plus Mwst.

Ziele:

In diesem 3-tägigen Training werden Sie auf die Personenzertifizierung zum Vorfall-Experten durch das BSI vorbereitet.

Die Aufbauschulung vermittelt Ihnen den offiziellen Schulungsplan zur Erlangung der Kenntnisse und Fähigkeiten, die Sie im Rahmen einer Tätigkeit als **zertifizierter Vorfall-Experte** 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 Zertifizierungsprogramm.

Als Schulungsabsolvent haben Sie die Möglichkeit, an der **Prüfung zur Personenzertifizierung beim Cyber-Sicherheitsnetzwerk** teilzunehmen und eine **Zertifizierung zum „Vorfall-Experten“ des BSI** zu erhalten! Das gesamte Zertifizierungsverfahren (mit Prüfung) wird nach Aufwand abgerechnet, weswegen kein genauer Preis genannt werden kann. Im Schnitt fallen jedoch um die 600-700€ an.

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

Inhalte/Agenda:

- ♦ **Rahmenbedingungen für den Vorfall-Experten**
  - ♦ ◊ Digitale Rettungskette
  - ◊ Grenzen der Aufgabe
  - ◊ Überblick über relevante Gesetze
  - ◊ Meldepflicht
  - ◊ Einbindung von Fachpersonal in die Vorfallbearbeitung
  - ◊ Zielsetzung des Betroffenen bei der Beauftragung

  - ♦ **Zusammenfassung Zusatzschulung Vorfall-Praktiker**

  - ♦ **Angriffsszenarien und Sofort bzw. Gegenmaßnahmen**
  - ♦ ◊ Überblick notwendiger Basis-Kenntnisse
  - ◊ Zusammenfassung relevanter Angriffsformen
  - ◊ Darstellung forensischen Vorgehens
  - ◊ Datensammlung/-erhebung
  - ◊ Datenanalyse
  - ◊ Grenzen der Analyse

  - ♦ **Vertiefung des Ablaufs des Standardvorgehens**
  - ♦ ◊ Vorbereitung auf potenzielle Vorfälle
  - ◊ Identifikation des IT-Sicherheitsvorfalls
  - ◊ Eindämmung des Schadensausmaßes
  - ◊ Ermitteln der Ursachen bzw. Auslöser des IT-Sicherheitsvorfalls
  - ◊ Wiederherstellung der Systeme
  - ◊ Dokumentation des IT-Sicherheitsvorfalls

  - ♦ **Zusammenfassung der wichtigsten Aspekte bei der Behandlung**
  - ♦ ◊ Behandlung von speziellen IT-Sicherheitsvorfällen
  - ◊ Individuelle vertiefende Übungen und Anwendungsbeispiele

  - ♦ **Vorfallbearbeitung bei OT (Anlagentechnik) für Vorfall-Experten**
  - ♦ ◊ Vertiefung des Themas „Vorfallbearbeitung von IT-Systeme „abseits der üblichen Büroanwendung“ aus der Schulung für Vorfall-Praktiker

  - ♦ **Vor-Ort-Unterstützung: Überblick verschaffen**
  - ♦ ◊ Vorfall-Experte als Krisen-Manager etablieren
  - ◊ Analysefähigkeit des Unternehmens einschätzen
  - ◊ Festlegung von Rahmenbedingungen der Zusammenarbeit

  - ♦ **Vor-Ort-Unterstützung: Analyse**
  - ♦ ◊ Analyse des IT-Sicherheitsvorfalls
  - ◊ Planung der Vorgehensweise
  - ◊ Notbetrieb
  - ◊ Bereinigung der Systeme
  - ◊ Wiederherstellung der Systeme
  - ◊ Nachbereitung

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