Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-
Sicherheitsnetzwerk

Curriculum zur Qualifikation von Vorfall-Experten

(Stand 10.06.2022)

Das vorliegende Curriculum bildet den Rahmen für Schulungsanbieter, um Schulungen zum Vorfall-Experten des Cyber-Sicherheitsnetzwerks vergleichbar und nach einem einheitlichenQualifikationsstandard anzubieten. Es beschreibt, welches Wissen für die Aufgabenerfüllungdes Vorfall-Experten als Teil der Digitalen Rettungskette erwartet wird.

Es ist die Aufgabe des Schulungsanbieters, auf der Grundlage der Themen des Curriculums eigenständig Schulungen zu entwickeln und durchzuführen. Das Curriculum beschreibt die Themengebiete, die der Vorfall-Experte wissen sollte und die im Rahmen der Prüfung für eine Personenzertifizierung abgefragt werden. Zusätzlich werden Methoden und Hilfsmittel vorgeschlagen, die dem Schulungsanbieter helfen können, das Wissen nachhaltig zu vermitteln.

Hierbei kann die Reihenfolge der Module individuell festgelegt und durchgeführt werden. Die Übungen (Modul 6) können parallel zu den entsprechenden theoretischen Modulen durchgeführt werden. Das Curriculum gibt lediglich den Umfang und Inhalt der Themen vor.

Schulungsanbieter können Akademien, Universitäten, Verbänden usw. sein. Zusätzliche Informationen für Schulungsanbieter zum Ablauf und Umfang der Schulungen finden sich im „Leitfaden für Schulungsanbieter“.


Das Symbol kennzeichnet die vorgeschlagene didaktische Methode bzw. den Einsatz eines möglichen Hilfsmittels.


Das Symbol kennzeichnet Links zu weiterführenden Informationen.

Das Curriculum ist modular aufgebaut und wurde nach Evaluierung der Qualifikation desVorfall-Experten überarbeitet. Dabei wird das Thema „Remote-Unterstützung“ jetzt in der Zusatzschulung für Vorfall-Praktiker vermittelt, so das für individuelle Übungen, Beispiel und neue Themen mehr Zeit geschaffen wurde.

Es werden folgende Module vorgeschrieben, die verpflichtend zu behandeln sind:

1. Einführung in das Cyber-Sicherheitsnetzwerk incl. Rahmenbedingungen für Digitale Ersthelfer, Vorfall-Praktiker und Vorfall-Experten (2 UE)
2. Zusammenfassung der wichtigsten Grundlagen der Zusatzschulung für den Vorfall-Praktiker (1 UE)
3. Angriffsszenarien und Forensik (3 UE)
4. Vertiefung des Ablaufs des Standardvorgehens (1 UE)
5. Zusammenfassung der wichtigsten Aspekte bei der Behandlung von Vorfällen z. B. Phishing-Vorfällen oder Ransomware-Vorfällen (1 UE)
6. **NEU:** Individuelle vertiefende Übungen und Anwendungsbeispiele für Vorfall-Experten (3 UE)
7. **NEU:** Vorfallbearbeitung bei OT (1 UE)
8. Vor-Ort-Unterstützung: Überblick verschaffen (3 UE)
9. Vor-Ort-Unterstützung: Analyse (4 UE)
10. „Nach einem Vorfall ist vor einem Vorfall" (1 UE)

Der „Leitfaden zur Reaktion auf IT-Vorfälle für Vorfall-Praktiker und Vorfall-Experten“ konkretisiert wichtige Themen des Curriculums und sichert zusätzlich ein einheitliches Vorgehen und eine gleichbleibende Qualität der Qualifikation. In dem Leitfaden werden zu jedem Modul die Intention und die Lernziele ausführlich erläutert. Aufgaben, Checklisten und Tests im Leitfaden ergänzen die Themen und können den Schulungsanbietern zur Verfügung gestellt werden.

Rahmenbedingungen für den Vorfall-Experten

1. Digitale Rettungskette
    - Ablaufbeschreibung
    - Rollendefinition

 *Selbsttest: Was zeichnet mich als guten Vorfall-Experten aus?*

2. Grenzen der Aufgabe
    - Behebung des IT-Sicherheitsvorfalls
    - Komplexität des IT-Sicherheitsvorfalls
    - Umfang der Beauftragung
    - Verfügbarkeit von Ressourcen (personell, finanziell, Know-how)

 *Partnerübung: Bewertung konkreter Praxis-Beispiele*

3. Überblick über relevante Gesetze
    - IT-Sicherheitsgesetz
    - EU-Datenschutzgesetz, Bundesdatenschutzgesetz (DSGVO)
    - Telemediengesetz, Telekommunikationsgesetz
    - Arbeitsschutz bzw. Sicherheitsbeauftragter für die Produktion usw.
4. Meldepflicht
    - Welche Meldeprozesse gibt es?
    - Wann muss/soll der Betroffene melden?
    - Wie spreche ich die Anzeigenpflicht an?
    - Mit welchen Problemen bzw. Einwänden könnte ich konfrontiert sein? (Kommunikationsprobleme, „hidden agenda“, usw.)
    - Meldepflichten für UBI aus IT-SiG 2.0 (insbesondere UBI 3 Störfallbetriebe, da dies auch kleinere Unternehmen sein können)

 *Rollenspiel: Meldungen anhand fiktiver Beispiel (Meldender vs. Vorfall-Experte)*

5. Einbindung von Fachpersonal in die Vorfallbearbeitung
    - Juristen
    - Kommunikationsspezialisten
    - Datenschutzbeauftragte
    - Betriebsrat/Personalrat
6. Zielsetzung des Betroffenen bei der Beauftragung
    - Schnelle Behebung versus vollständige Aufklärung

Zusammenfassung Zusatzschulung Vorfall-Praktiker

Die wichtigsten Aspekte der Themen der Zusatzqualifikation zum Vorfall Praktiker sollen in geeigneter Form kurz wiederholt und zusammengefasst werden. Voraussetzung ist, dass sich die Teilnehmenden bereits im Vorfeld durch den Besuch der Zusatzschulung Vorfall-Praktiker oder dem Leitfaden für die Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten beschäftigt haben.

Folgende Themen sind im Curriculum für die Qualifikation zum Vorfall-Praktiker festgelegt:

1. Einführung in das Cyber-Sicherheitsnetzwerk incl. Rahmenbedingungen für Digitale Ersthelfer, Vorfall-Praktiker und Vorfall-Experten und eine Zusammenfassung der Inhalte des Basiskurses
2. Verhalten am Telefon incl. nicht technischer Maßnahmen
3. Gefährdungen und Angriffsformen und Übersicht über die aktuelle Gefährdungslage
4. Ablauf der Standartvorgehen
5. Behandlung von IT-Sicherheitsvorfällen z. B. Phishing-Vorfälle, Ransomware-Vorfällen usw.
6. Remote-Unterstützung
7. Vorfallbearbeitung bei IT-Systemen „abseits der üblichen Büroumgebung“
8. „Nach dem Vorfall ist vor dem Vorfall“ –Präventive Maßnahmen

Angriffsszenarien und Sofort bzw. Gegenmaßnahmen

1. Überblick notwendiger Basis-Kenntnisse
    - Der gängigen Betriebssysteme: Windows, Linux, Mac OS
    - Netzwerk
    - Schadprogramme (Malware)

Links zu weiterführenden Lerndokumenten

2. Zusammenfassung relevanter Angriffsformen
    - typische Angriffe
    - Angriffsformen auf Firmware
    - zu mobilen Plattformen, Embedded Devices, ICS-Komponenten usw.
    - Lagebilder, Quellen und Diskussionsforen über aktuelle Angriffswege usw.

Links zu weiterführenden Lerndokumenten

3. Darstellung forensischen Vorgehens
    - Methode Live-Forensik
    - Methode Dead-Forensik
4. Datensammlung/-erhebung
    - Full-Image

- Memory-Image
- Triage-Forensik

5. Datenanalyse
    - Systemspuren unter Windows, Linux und Mac OS
    - Systemlog- Analyse
    - Auswertung laufender Prozesse
    - Untersuchung von Autostart-Möglichkeiten
    - Auswertungen weiterer Logdateien (Virenscanner- oder Firewall- Protokolle)
6. Grenzen der Analyse

Rollenspiel: Die Analysemethoden können an fiktiven Beispielvorfällen(Übungsszenarien) eingeübt werden.

Vertiefung des Ablaufs des Standardvorgehens

1. Vorbereitung auf potenzielle Vorfälle
    - Welche Prozesse könnten unterstützen?
    - Wo könnten weitere Personen unterstützen?
    - Existiert ein Vorfallreaktionsplan?
2. Identifikation des IT-Sicherheitsvorfalls
    - Was ist passiert?
    - Handelt es sich um kein Sicherheitsereignis, sondern um einen Sicherheitsvorfall?
    - Welcher Angriffstyp liegt vor?
3. Eindämmung des Schadensausmaßes

 *Workshop: Liste von Sofortmaßnahmen gemeinsam erstellen und diskutieren*

4. Ermitteln der Ursachen bzw. Auslöser des IT-Sicherheitsvorfalls
    - Beweissicherung
    - Datensammlung und Datenanalyse
    - Gesamtwertung

 *Einzelübung: Bewertung konkreter Praxis-Beispiele*

5. Wiederherstellung der Systeme

 *Workshop: Erstellen einer Checkliste für den Wiederanlauf. Welche Punkte müssen beachtet werden?*

6. Dokumentation des IT-Sicherheitsvorfalls
    - Berichtswesen und Berichtspflicht (Formular)
    - Welche Informationen sind für einen IT-Dienstleister mit einem Team ausVorfall-Experten notwendig?
    - Welche Sachverhalte sind für die Versicherung oder für ein möglichesGerichtsverfahren festzuhalten?
    - Zusätzliche Dokumentation, z. B. Erstellen einer Liste der wichtigsten organisatorischen, prozessualen und technischen Rahmenbedingungen(Checkliste)

 *Rollenspiel: Das Standardvorgehen kann mit einem fiktiven Beispielunternehmen(Übungsszenarium) eingeübt werden.*

Zusammenfassung der wichtigsten Aspekte bei der Behandlung

1. Behandlung von speziellen IT-Sicherheitsvorfällen
    - Wichtigste Aspekte bei einem Phishing-Angriff
    - Wichtigste Aspekte bei Ransomware
    - ggf. Aspekte eines APT-Angriffs
2. Individuelle vertiefende Übungen und Anwendungsbeispiele für Vorfall-Experten
   Diese Vertiefung ist vom Schulungsanbieter auszuarbeiten, mit dem Ziel, sich praktisch mit der Behebung eines IT-Sicherheitsvorfall auseinanderzusetzen. Die Inhalte sind nicht Umfang der Kompetenzprüfung bei der Zertifizierungsstelle.

Vorfallbearbeitung bei OT (Anlagentechnik) für Vorfall-Experten

Vertiefung des Themas „Vorfallbearbeitung von IT-Systeme „abseits der üblichen Büroanwendung“ aus der Schulung für Vorfall-Praktiker

1. IT-Systeme kommen auch abseits der üblichen Büro-Anwendung zum Einsatz.
    - Gebäudeautomatisierung
    - Steuerung und Parametrisierung von CNC-Maschinen, Laserbearbeitung und Komponenten in größeren Maschinen und Anlagen
    - Produktionsplanung und -steuerung
2. Beispiele für Architekturen. Welche Technik kommt zum Einsatz?
3. Was sind mögliche Gefahren für die Steuerungstechnik?
    - Ausfall durch Defekt oder Löschen/Verschlüsseln von Datenträgern
        - Problem: Fehlende Backups, keine Austauschhardware.
    - Manipulation
        - Problem: Fehlerhafte Parameter führt Fehlproduktion
        - Beeinträchtigung der Sicherheit der Maschine kommen kann (Veränderung von sicherheitsrelevanten Parametern)
4. Grenzen der Aufgabe
5. Ablauf des Standardvorgehen
    - Eindämmung des Schadensausmaßes
    - Trennung der Netzwerksegmente
    - Abschaltung teilweise nicht ohne weiteres möglich
6. Angriffsszenarien und Sofort bzw. Gegenmaßnahmen
    - Manipulation von Parametern, Automationslogik mit dem Ziel den Ablauf zu sabotieren.
7. Grenzen der Analyse
    - Abzug von Speicherdaten aus Sensoren, Aktoren und anderen ICS-Komponenten schwierig. Analyse momentan häufig sehr zeitaufwändig.

Vor-Ort-Unterstützung: Überblick verschaffen

1. Vorfall-Experte als Krisenmanager etablieren
    - Erster Eindruck zählt
    - Kommunikationsstrategie
    - Wie schafft man es, Vertrauen und Ruhe auszustrahlen?
    - Wie verschafft man sich Gehör
    - Wie spreche ich den Kunden richtig an?

Rollenspiel: Wie reagiert der Vorfall-Experte auf unterschiedliche Situationen beim betroffenen Unternehmen.

2. Analysefähigkeit des Unternehmens einschätzen
    - Welche Situation liegt im Unternehmen vor?
    - Sichten der Netzwerkpläne
    - Kommunikationsmatrix erstellen
    - Dokumentation der Systemarchitektur
    - Kompetenz und Personalressourcen
    - Backups usw.

Einzelübung: Einschätzung der Analysefähigkeit unterschiedlicherUnternehmensbeispiele

Gruppendiskussion: Erstellung eines Fragenkataloges für die Ersteinschätzung

3. Organisatorische Voraussetzungen klären
    - Was ist passiert?
    - Gibt es einen Notfallplan?
    - Sind Meldewege definiert?
    - Können Dienstleister eingebunden werden?
4. Festlegung von Rahmenbedingungen der Zusammenarbeit
    - NDA (non disclosure agreement)
    - Datenschutz
    - Meldung
    - Kommunikationswege
    - Dokumentation
    - Was kann nicht geleistet werden? Wo wird Unterstützung benötigt?

Vor-Ort-Unterstützung: Analyse

1. Analyse des IT-Sicherheitsvorfalls
    - Tiefgründige Analyse (flüchtigen/nichtflüchtigen Daten, Writeblocker)
    - Identifikation betroffener Systeme
    - Analyse des Auslösers
    - Schadensfeststellung
2. Planung der Vorgehensweise
3. Notbetrieb
    - Prüfung
    - Herstellung des Notbetriebs (Isolierung oder Verlagerung der Systeme)
4. Bereinigung der Systeme
    - Beseitigung der Schadsoftware bzw. schadhafte Dateien
    - Neuinstallation des Betriebssystems
5. Wiederherstellung der Systeme
6. Nachbereitung

 *Rollenspiel: Die Analysemethoden können an fiktiven Beispielvorfällen (Übungsszenarien) eingeübt werden*

„Nach einem Vorfall ist vor einem Vorfall"

1. Sensibilisierung des Unternehmens für präventive Sicherheitsmaßnahmen
    - Mitarbeiter
    - IT-Sicherheitslandschaft
        - Patchmanagement
        - Härtungsmaßnahmen
        - Penetrationstest
    - Notfallmanagement und Notfalldokumentation usw.

     *Links zu weiterführenden präventiven Maßnahmen*

2. Aufbau eines Sicherheitsbewusstseins
3. Analyse von Geschäftsprozessen
4. Aufbau eines Sicherheits- und Notfallkonzeptes
5. Konzeption von Übungen
6. Info-Paket durch CSN bereitstellen

 *Inhalt des Informations-Pakets*

 *Links zum Informationspaket für Vorfall-Experten*

7. Aufrechterhaltung der Kompetenz des Vorfall-Experten
    - Weiterbildung
    - Beiträge für eine Wissensdatenbank
    - Leiten von regionalen Foren

- Teilnahme an Expertenkreisen und Übungen des Vorfall-Experten zwischen den einzelnen Vorfällen