Leitfaden zum Personenzertifizierungsprogramm

Security Incident Manager (TÜV®)

Inhalt

Herausgeber und Eigentümer:
TÜV NORD CERT GmbH
Zertifizierungsstelle für Personen
Am TÜV 1
45307 Essen
E-Mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 01
Status: freigegeben BM 17.03.2025
Gültig ab: 17.03.2025

Leitfaden zum Personenzertifizierungsprogramm Security Incident Manager (TÜV®)

1. Allgemein

Die Anzahl der Cyberangriffe auf die Unternehmen wächst in den letzten Jahren stetig an. Diese treten in den vielfältigsten Varianten in der Praxis auf. Neben den oft erwähnten Ransomware-Attacken, Übernahme von Verzeichnisdiensten wie das Active Directory oder Datendiebstahl von ganzen (Kronjuwelen-) Datenbanken gibt es vielfältige leichte und schwere Angriffe die beispielsweise Abzielen auf Betrug, Einblick in Betriebsgeheimnisse, Veränderung von Daten, Störung der Verfügbarkeit oder Fremdnutzen der unternehmerischen Plattformen für andere Zwecke.

In jedem Fall müssen die betroffenen Unternehmen fähig sein, sich von diesen Angriffen wieder zu befreien. Dabei ist neben einem eingespielten Team, klaren Abläufen oder der koordinierten Hilfe von externen Dienstleistern auch die schnelle Rückkehr zum Normalbetrieb sowie die forensische Sicherung während der Abarbeitung wichtig.

Der Security Incident Manager muss die Prinzipien, Methoden und Verfahren der Bearbeitung von Informationssicherheitsvorfällen entsprechend den Belangen der Wirtschaft beherrschen. Er muss die Kompetenz besitzen, um beim Aufbau, der Abarbeitung und der Verbesserung des Prozesses zur Reaktion auf Sicherheitsvorfälle zu unterstützen.

2. Anwendungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Zertifikats Security Incident Manager (TÜV) im Rahmen von anerkannten Lehrgängen. Die Lehrgänge können sowohl als Präsenzschulung, Blended Learning als auch Online anerkannt sein.

3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung	Schulung im Zertifizierungsgebiet
Security Incident Manager (TÜV®)	Abgeschlossene Berufsausbildung / gleichwertig ersatzweise 2 Jahre Berufserfahrung	fachbezogener Lehrgang mit mind. 24 UE*. und erfolgreichem Abschluss

Hinweise zur Tabelle:

- 1 UE entspricht einer Unterrichtseinheit von 45 Minuten.
- „Erfolgreicher Abschluss“ bedeutet das Bestehen der zum Lehrgang bzw. zur Zertifizierung gehörenden Abschlussprüfung gemäß diesem Personenzertifizierungsprogramm.

4. Prüfungsgegenstand und Prüfungshilfsmittel

Die Präsenzprüfungen nach Präsenzlehrgängen finden in der Regel am letzten Lehrgangstag oder am Tag nach dem letzten Lehrgangstag am Ort des Lehrgangs statt.

Für Online-Prüfungen werden entsprechende separate Termine angeboten.

Aktuelle technische Voraussetzungen finden sich unter folgendem Link:
https://www.tuev-nord.de/de/unternehmen/bildung/personenzertifizierung/pruefungsinformationen-1/

Einige Tage vor der Prüfung bekommen die Kandidatinnen und Kandidaten eine E-Mail mit den Zugangsvoraussetzungen, Links, Installationsanleitungen, der geltenden Prüfungsordnung für Online-Prüfungen und speziellen Informationen zur jeweiligen Prüfung. Darüber hinaus werden mit der Mail die notwendigen Passwörter zur Prüfung mitgeteilt.

Es sind keine Unterlagen als Hilfsmittel zugelassen.
Bei Bedarf sind Taschenrechner erlaubt, andere elektronische Hilfsmittel sind nicht zulässig.

5. Prüfungsübersicht

Prüfung Security Incident Manager (TÜV)	schriftlich:
Dauer:	60 min.
Anzahl der Prüfungsaufgaben gesamt:	30
MC-Aufgaben:	30
Höchstpunktzahl:	30
Mindestpunktzahl:	18 (60 %)

Details s. Anlagen

6. Schriftliche Präsenzprüfung

Die Prüfungsaufgaben werden in einem separaten Aufgabenheft vorgelegt. Die Lösungen zu jeder Prüfungsaufgabe werden auf den Seiten des Einzelberichts eingetragen. Nur die Antworten auf dem Einzelbericht werden gewertet.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Auswahlmöglichkeiten durch Ankreuzen jede richtige Lösung ausgewählt werden. Es können eine, mehrere oder alle Auswahlmöglichkeiten richtig sein. Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Kreuze an den richtigen Stellen der Tabelle gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten.

7. Schriftliche Online-Prüfung

Die Prüfungsaufgaben erscheinen einzeln auf dem Bildschirm. Die Lösungen zu jeder Prüfungsaufgabe werden direkt zur Aufgabe eingetragen.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Antwortmöglichkeiten durch Anklicken jede richtige markiert werden. Es können eine, mehrere oder alle Auswahlmöglichkeiten richtig sein.
Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Markierungen an den richtigen Stellen gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten. Die Aufgaben werden automatisch gewertet.

8. Gesamtbewertung

Die Prüfung Security Incident Manager (TÜV) ist bestanden, wenn die schriftliche Prüfung bestanden ist.

Es erfolgt keine Mitteilung über Einzelergebnisse oder Punktzahlen.

Maßgeblich für die Bewertung sind bei nachträglichen Korrekturen, die erreichten 60 %, nicht die auf- oder abgerundete Punktzahl.

9. Zertifizierungsentscheidung und Zertifikatserteilung

Bei bestandener Prüfung wird durch die TÜV NORD CERT ein Zertifikat ausgestellt.

Das Zertifikat enthält folgende Angaben:

a) Personalien der zertifizierten Person (Titel, Vorname, Name, Geburtsdatum)
b) Bezeichnung der Qualifikation
c) Prüfungsinhalte
d) Unterschrift der Fachleitung Personenzertifizierung
e) Ausstellungsdatum

Jedes Zertifikat erhält eine eindeutige Nummer:

44-02-10201295-tt.mm.jjjj- DE02-32157 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
02	Zertifikat
10201295	Kurzkennzeichnung des Zertifizierungsgebietes
tt.mm.jjjj	Tag der Prüfung
DE02	Kennzahl des Prüfungszentrums
32157	Prüfungszentrumsspezifische Kandidatenidentifikationsnummer

Das Zertifikat darf nur in der zur Verfügung gestellten Form verwendet werden. Es darf nicht nur teil- oder auszugsweise benutzt werden. Änderungen des Zertifikats dürfen nicht vorgenommen werden. Das Zertifikat darf nicht irreführend verwendet werden.

10. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

11. Gültigkeit der Zertifikate

Diese Bescheinigung der bestandenen Prüfung ist unbegrenzt gültig.

12. Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Security Incident Manager (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Motivation und Grundlagen (MG)	**4 UE**	**5 MC**
2. Anforderungen, Checklisten, Standards und rechtliche bzw. regulatorische Grundlagen (CH)	**4 UE**	**5 MC**
3. Management von Sicherheitsvorfällen aus Sicht des ISOs / CISOs / IT-Managers (MS) • Sinnvolle Pläne, Taktiken und Richtlinien • Schnellstart am Beginn einer ISO- bzw. CISO-Tätigkeit • Ausarbeitung eines Security-Incident-Response-Prozesses • Vorbereitung und Unterstützung durch die Geschäftsführung • Führungsaufgaben und Teambildung • Koordinationsaufgaben rund um den Kompetenzaufbau • Finanzierung und Bereitstellung der Ressourcen • Rechtliche Betrachtung von Sicherheitsvorfällen • Umgang mit Anzeigen und Ermittlungsbehörden • Ergänzung des Berichtswesens um geeignete Kennzahlen • Prüfungsaspekte, Kontrollmöglichkeiten und Auditierung	**4 UE**	**5 MC**
4. Bearbeitung von Sicherheitsvorfällen aus Sicht des IT-Betriebs und der Technik (SV) • Kompetenzen und Fähigkeiten • Planung und proaktive Maßnahmen • Durchführung der Incident Response und reaktives Arbeiten • Soziales Verhalten und Zusammenarbeit • Übungen und Tests • Nachschau und Verbesserungen nach einem Sicherheitsvorfall • Operative Berichterstellung zum Sicherheitsvorfall	**4 UE**	**5 MC**
5. Mitwirken bei einem Sicherheitsvorfall von Externen und weiteren Fachbereichen (MW) • Übersicht über übliche Dienstleistungen von Externen • Vorbereitungsarbeiten für den Ernstfall • Einbindung der eigenen Fachbereiche • Zusammenarbeit und typische Konflikte • Übungen und Tests • Vertragsgestaltungen mit Externen	**4 UE**	**5 MC**

4 Exkurs (SP) • Ausgelagerte Lösungen • Cloud-Überwachung und Security Incident Response in der Cloud • Forensisches Basiswissen und Erste Hilfe	**4 UE**	**5 MC**
5 Abschlussprüfung		
schriftlich	**60 min.**	**30 MC**

*

UE: Unterrichtseinheit à 45 Minuten
MC: Multiple-Choice-Aufgaben
o: offene Aufgaben

In der Tabelle „Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung“ handelt es sich bei den Angaben der Unterrichtseinheiten um Richtwerte, die in Einzelfällen bedingt durch Zusammensetzung der Teilnehmenden, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.