Zertifizierungsordnung zum Informationssicherheitsbeauftragter

A) Gegenstand

(was legt die Ordnung fest)

Diese Zertifizierungsordnung gilt für die Weiterbildung zum Informationssicherheitsbeauftragter. Sie bestimmt die Soll-Definition des Qualifikationsniveaus, Regelungen der Prüfung des Nachweises durch die Teilnehmer und der Bestätigung durch ein Personenzertifikat.

B) Qualifikationsniveau

(welche Qualifikation soll erreicht werden)

Befähigung für die Tätigkeit als Informationssicherheitsbeauftragter bzw. als Führungskraft zu Informationssicherheit in kleinen, mittleren oder großen Institutionen mit besonderem Fokus auf Informationssicherheits-Management. Verständnis wesentlicher Grundlagen, Prinzipien und Methoden zur Realisierung von Informationssicherheit durch Betrachtung aus einer übergreifenden Perspektive, damit Zurechtfinden in der Komplexität der Informationssicherheit, Erstellen gesamthafter Lösungen, Erreichen eines besseren Verständnisses und Anwenden und Übertragen der Prinzipien auf neue Techniken oder verwandte Gebiete mit Themen und Kompetenzen mit einem Umfang von 25 Unterrichtseinheiten, eine Unterrichtseinheit beträgt 60 Minuten reine Lernzeit. Die Themenbereiche sind:

Grundlagen: Definitionen / Begriffe und Motivation / Nutzen (Schutz, Rechtskonformität, ...); Ziele / Anforderungen (Vertraulichkeit, Integrität, Verfügbarkeit, ...); Schutzbedarfsfeststellung und Informationssicherheitsniveau; Rechtliches mit EU NIS-Richtlinie, IT-Sicherheitsgesetz, BSI-Kritisverordnung, BSI-Gesetz, EU Datenschutz-Grundverordnung, weitere.

Management: Zur Realisierung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus via Informationssicherheits-Management allgemein mit Komponenten und Zusammenwirken mit Bedeutung, Prinzip, Lebenszyklus, Verantwortung, Informationsicherheits-Politik, -Strategie, -Organisation (Strukturen und Prozesse), -Kontrolle, schematisch gemäß IT-Grundschutz BSI-Standard 200-1 "Managementsysteme für Informationssicherheit" in der Übersicht, anwendbar gemäß IT-Grundschutz BSI-Standard 200-2 "IT-Grundschutz-Methodik" mit 200-3 "Risikoanalyse auf der Basis von IT-Grundschutz", Business Continuity Management gemäß IT-Grundschutz BSI-Standard 200-4, international gemäß ISO-Standard 2700x und Herausforderungen der Informationssicherheit mit beispielhaften Lösungen.

Prinzipien, Methoden, Maßnahmen: Zum allgemeinen Verstehen von Sicherheitsprinzipien mit -methoden und -maßnahmen strukturiert als Modell gemäß dem Zusammenwirken in neun wesentliche Prinzipien in Authentifikation (Wissen, Besitz, Eigenschaft, starke und Einmal-Passwörter, ...), Autorisierung (MAC, DAC, RBAC, Ebenen, ...), Administration (Organisation, Umsetzung, ...), Protektion (Bewusstsein+Ermächtigung, Datensicherung, Härtung, Kommunikationskontrolle, Verschlüsselung, ...), Auditierung (Protokollierung, Angriffserkennung, ...), Sichere Entwicklung (Schutzbedarfsfeststellung, Bedrohungsanalyse, ...), Sicherer Betrieb (physischer Schutz, sichere Auslieferung, ...), Sichere Nutzung (sicherheitskonformes Verhalten, Datenlokalität, ...), Sicherheitsmanagement (Sicherheitsprozesse, Sicherheitsvorgaben, ...).

Gefahren und Lösungen: Zum konkreten und anwendbaren Verständnis von Gefahren und Schutzmaßnahmen mit Arten von Angreifern, Angreifer-Motivatoren und Arten von Gefahren, Sicherheitsebenen, Gefahrenstrukturierungen und zahlreichen Gefahren mit typischen, beispielhaften Lösungsmethoden wie Höhere Gewalt; Fehlplanung, Fehlfunktion, Fehlhandlung, Missbrauch; Ausfall, Diebstahl / Verlust / Zerstörung von Geräten, Datenträgern, Dokumenten; Social Engineering mit Social Hacking, Phishing, Vishing, Smishing, Spear-Phishing, CEO-Fraud, Whaling; Soziale Netze; Identitätsmissbrauch, Erpressung, Korruption; Passwort-Angriffe (Abschauen, Cracken, Credential-Stuffing, ...); Unbefugtes Eindringen, Exploits-, Script-, Buffer-

Overflow-Attacken; Lauschangriffe / Datendiebstahl, Hoaxes und Malware mit Virus, Wurm, Scareware, Spyware, Ransomware, Kryptominer, Adware, Malvertising, Trojaner, Blended Malware; Angriffe auf Verschlüsselung (Brute-Force, Man-in-the-Middle); Denial-of-Service-Attacken (DoS, DDoS, Defacement, Botnetze, ...) und Web-basierte Angriffe (Webserver Poisoning, CrossSite-Scripting, ...).

Angriffsmanagement: Zur Erkennung und Reaktion auf Angriffe mit Angriffsprävention/-vorbeugung (CERT), Angriffserkennung/-detektion (Grundsätzliches, Einzelnes, Erkennungssystem host-basiert, netzwerk-basiert, als Modell mit Sensoren, Auswertungslogik mit Wissensbasis, Aktoren, konkrete Möglichkeiten wie Daten-Überwachung via Soll-Ist-Vergleiche, Netzwerk-Überwachung via Sniffer, Netzwerk- und System-Überwachung via Honeypot/Honeynet, ... und Beispiele konkreter Werkzeuge) und Angriffsbehandlung/-reaktion (mit möglichem Vorgehen).

C) Prüfungsregelungen

(wie wird gemessen, ob Teilnehmer das Qualifikationsniveau haben)

Gegenstand

In einer Prüfung wird festgestellt, ob der Teilnehmer das Qualifikationsniveau erfüllt.

Anmeldung

Die Anmeldung erfolgt in einer eigenständigen Prüfungsanmeldung.

Rücktritt

Will ein Teilnehmer an der Prüfung nicht teilnehmen, so hat er dies vor Beginn der Prüfung, spätestens am Anfang der Prüfung, dem Prüfer mitzuteilen. In diesem Fall gilt die Prüfung als nicht durchgeführt.

Tritt ein Teilnehmer ansonsten nach Beginn der Prüfung zurück, so gilt die Prüfung als nicht bestanden.

Identitätsnachweis

Der Prüfling muss sich vor Prüfungsbeginn mit einem gültigen Lichtbildausweis ausweisen.

Termin, Ort, Form, Dauer, Sprache

Die Prüfung erfolgt als eigenständige Prüfung.
Termin und Ort gemäß Ankündigung bzw. Vereinbarung.

Der Prüfling sollte sich rechtzeitig vor dem angesetzten Prüfungszeitpunkt einfinden.
Bei verspäteten Eintreffen kann der Zutritt und die Teilnahme durch den Prüfer verweigert werden.

Die Prüfung dauert 45 Minuten. Die Prüfungszeit läuft während der Abwesenheit des Prüflings (z.B. beim Aufsuchen der Toiletten) weiter. Zusätzliche Zeit wird nicht gewährt.

Dazu werden Fragebögen ausgeteilt und von jedem Teilnehmer eigenständig, ohne Hilfsmittel und schriftlich beantwortet und an den Prüfer zurückgegeben.

Die Prüfung erfolgt in deutscher Sprache.

Online-Prüfung:

Zur geeigneten Beaufsichtigung hat der Teilnehmer das von der DresPleier GmbH eingesetzte Videokonferenz-System zu nutzen und die Übertragung von Bild (Video mit sichtbarem Teilnehmer), Ton (Audio) und Monitor (Desktop-Teilen) zu aktivieren. Die Prüfung hat daher als Einzelprüfung zu erfolgen und das Equipment des Teilnehmers muss dies ermöglichen.

Ablauf: Zur Prüfung des Raums auf unerlaubte Hilfsmittel ist vor der Prüfung ein Mal 360 Grad mit der Kamera durch den Raum zu schwenken. Der Teilnehmer erscheint 15 Minuten vor Prüfungsbeginn, schaltet das Videokonferenz-System zur Ansicht frei und weist sich über gültigen Lichtbildausweis aus. Zum Prüfungsbeginn bekommt er die Prüfungsfragen per Mail zugesendet im Open Document Format (ODT für Textdokumente). Er beantwortet die Fragen direkt im Dokument durch Ankreuzen. Zum Ende speichert er das Dokument als PDF ab und sendet es sofort per Mail als PDF

an den Prüfer zurück. Zusenden, PDF-Speichern und Zurücksenden erfolgen außerhalb der Prüfungszeit. Ein Austreten während der Prüfung ist nur zeitlich begrenzt (wenige Minuten) gestattet. Bei gravierenden technischen Störungen wird die Prüfung abgebrochen und kostenlos wiederholt.

Fragen, Bewertung

Zu den Themenfeldern ist ein Fragenpool erstellt mit 64 Multiple-Choice-Fragen, die alle Themenfelder abdecken gewichtet in der Anzahl: 8 zu Grundlagen, 24 zu Management, 12 zu Prinzipien, Methoden, Maßnahmen, 12 zu Gefahren und Lösungen, 8 zu Angriffsmanagement. Die Fragen können vier Antwortmöglichkeiten haben:

- eine Antwort ist richtig,
- mehrere Antworten sind richtig,
- alle Antworten sind richtig oder
- keine Antwort ist richtig.

Die richtigen Antworten sind anzukreuzen. Für jede richtig beantwortete Frage gibt es einen Punkt. Eine Frage gilt als richtig beantwortet, wenn alle Antworten richtig angekreuzt sind. Ist eine Antwort falsch, gilt die gesamte Frage als falsch beantwortet (Null Punkte). Es gibt keine Punktabzüge. Die Antworten müssen klar erkennbar sein, versehentlich falsch angekreuzte Antworten sind deutlich zu korrigieren. Im Zweifelsfall wird die Frage als falsch gewertet.

Zur Prüfung werden daraus per Zufall 40 Fragen ausgewählt, die alle Themenfelder abdecken gewichtet in der Anzahl: 4 zu Grundlagen, 16 zu Management, 8 zu Prinzipien, Methoden, Maßnahmen, 8 zu Gefahren und Lösungen, 4 zu Angriffsmanagement.

Zum Bestehen der Prüfung müssen 50%, also 20 Fragen richtig beantwortet sein.

Hilfsmittel

Der Prüfling darf zur Beantwortung der Fragen keinerlei Hilfsmittel benutzen,
sondern muss diese eigenständig beantworten.

Betrug, Störung

Im Falle eines Betrugs dokumentiert der Prüfer dies und entscheidet je nach Bedeutung des Vorfalls über eine Verwarnung oder den Ausschluss aus der Prüfung. Bei einem Ausschluss gilt die Prüfung als nicht bestanden. Werden Verstöße nach der Prüfung festgestellt, so kann ein ausgestelltes Personenzertifikat widerrufen werden.

Stört ein Teilnehmer die Prüfung, so kann er von der Prüfung ersatzlos ausgeschlossen werden. Die Prüfung gilt dann als nicht bestanden.

Einsicht, Wiederholung

Ist die Prüfung nicht bestanden, so kann der Teilnehmer auf Antrag eine Prüfungseinsicht nach Abstimmung mit der DresPleier GmbH vornehmen. Anfallende Kosten hat der Teilnehmer zu erstatten.

Eine nicht bestandene Prüfung kann wiederholt werden.
Dazu ist eine Prüfung mit entsprechenden Kosten zu buchen.

D) Zertifikat

(wie wird das Qualifikationsniveau bestätigt)

Ausstellung

Die Prüfung wird zeitnah ausgewertet.

Bei einer erfolgreichen Prüfung wird dem Teilnehmer ein Personenzertifikat als Bestätigung mit der Post zugesendet. Ansonsten wird der Teilnehmer über das Nichtbestehen informiert.

Inhalte

Das Personenzertifikat enthält:

- Familienname, Vorname(n), ggf. Titel, Geburtsdatum

- Bezeichnung
- Qualifikationsniveau (der Umfang an Unterrichtseinheiten ist dabei nur angegeben, wenn diese auch konkret in einem Online-Seminar absolviert werden)
- Prüfungsdatum und Prädikat "mit Erfolg bestanden"
- Gültigkeitsdauer des Zertifikats
- Bei Rezertifzierung eines von der DresPleier GmbH ausgestellten Zertifikats Angaben zum Zertifizierungszeitraum

Verwendung

Das Personenzertifikat darf nur in der ausgestellten Form verwendet werden.
Es darf nicht verändert, in Teilen oder in täuschender Absicht genutzt werden.

Im Falle von Missbrauch kann das Personenzertifikat nachträglich widerrufen werden.

Dauer, Rezertifizierung

Das Personenzertifikat hat eine zeitlich begrenzte Gültigkeit,
da es die Aktualität einer Qualifikation bestätigt.

Das Personenzertifikat hat eine Gültigkeit von fünf Jahren ab dem Zeitpunkt der Prüfung.

Eine Rezertifizierung ist möglich. Dazu ist eine Prüfung mit entsprechenden Kosten zu buchen und erfolgreich zu absolvieren.

Widerruf

Wird ein Personenzertifikat vom Aussteller widerrufen, so ist dies vom Zertifikatsinhaber unverzüglich auf dessen Kosten an den Aussteller im Original per Post zuzusenden und darf dieses vom Zertifikatsinhaber nicht weiter verwendet werden.

E) Sonstiges

(was ist zudem relevant)

Aufbewahrungsfrist

Prüfungsunterlagen werden 1 Jahr lang aufbewahrt,
Informationen zum Zertifikat für die Gültigkeitsdauer des Zertifikats.

Inkrafttreten

Die Zertifizierungsordnung tritt am 07.05.2024 in Kraft
und ersetzt alle früheren Zertifizierungsordnungen.

Die Geschäftsführung

Firma: DresPleier GmbH ; **Geschäftsführer:** Dr. Christoph Pleier ; **Sitz und Registergericht:** Landshut HRB 6587 ; **USt-ID:** DE814347435
Anschrift: Vils 8, 84149 Velden ; **Telefon:** 08742/5870894 ; **Telefax:** 03222/4170655 ; **Mail:** info@DresPleier.de ; **Web:** www.DresPleier.de