**LMS-Fragen für Cyber Risk Assessment und Management DLMCSECRAM01\_E**

(Fünf Multiple-Choice-Fragen pro Lektion mit je einer richtigen Antwort und drei falschen Antworten. Geben Sie in der zweiten Spalte den entsprechenden Abschnitt der Lektion an).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lektion/**  **Frage-Nr.** | **Abschnitt** | **Frage** | **Richtige Antwort** | **Falsche Antwort** | **Falsche Antwort** | **Falsche Antwort** |
| 1/1 | 1.1 | Ein Unternehmen sollte in die Minderung eines Risikos investieren … | … wenn die Kosten für die Risikominderung geringer sind als der mögliche Verlust. | … wenn die Kosten für die Risikominderung höher sind als der mögliche Verlust. | … wenn die Kosten für die Risikominderung niedriger sind als 10.000 €. | … wenn der Verlust durch dieses Risiko höher ist als ein Prozent des Jahresumsatzes. |
| 1/2 | 1.2 | Was ist ein Merkmal einer Cyber-Katastrophe? | Eine große Gruppe von Benutzern und Benutzerinnen ist von dem Ereignis betroffen. | Die Eintrittswahrscheinlichkeit einer solchen Katastrophe ist immer höher als die einer realen Katastrophe. | Cyber-Katastrophen haben immer Auswirkungen auf die reale Welt. | Die Organisation ist weiterhin in der Lage, das Ereignis, das sie beeinträchtigt, zu kontrollieren. |
| 1/3 | 1.3 | Welcher Beschränkung unterliegt ein Cyber-Risiko? | Die Ursache für ein Cyber-Risiko ist auf eine Cyber-Bedrohung beschränkt. | Die Folgen eines Cyber-Risikos sind auf den Cyber-Raum beschränkt. | Die Ursachen eines Cyber-Risikos sind nicht beschränkt. | Ein Cyber-Risiko hat die gleichen Beschränkungen wie ein normales Risiko. |
| 1/4 | 1.3 | Eine böswillige Bedrohung liegt vor, wenn … | … ein verärgerter Mitarbeiter aus Rache Daten löscht. | … ein Blitz in das Rechenzentrum einschlägt und dies zu Datenverlust führt. | … ein/e Systemadministrator:in versehentlich einen Produktionsserver herunterfährt. | … ein/e Benutzer:in seine eigenen gehosteten Daten löscht. |
| 1/5 | 1.2 | Welches dieser Ereignisse gilt als eine globale Cyber-Katastrophe? | die WannaCry Ransomware-Angriffe im Jahr 2017 | die AWS-Cloud-Unterbrechung im Jahr 2019 | der Ausfall von Azure AAD im Jahr 2021 | die Waldbrände in Griechenland im Jahr 2021 |
| **Lektion/**  **Frage-Nr.** | **Abschnitt** | **Frage** | **Richtige Antwort** | **Falsche Antwort** | **Falsche Antwort** | **Falsche Antwort** |
| 2/1 | 2.1 | Welche der folgenden Strategien ist keine gültige Risikomanagementstrategie? | das Risiko ignorieren | das Risiko akzeptieren | das Risiko übertragen | das Risiko verringern |
| 2/2 | 2.2 | Was ist Teil der Eintrittswahrscheinlichkeitsmetrik? | der Bedrohungsakteur | der Verlust der Vertraulichkeit | der Verlust der Integrität | der finanzielle Schaden |
| 2/3 | 2.3 | Was ist keine Risikostufe? | selten | hoch | niedrig | mittel |
| 2/4 | 2.2 | Welches Kompetenzniveau hat ein professioneller Penetrationstester im OWASP-Risikobewertungs-Framework? | 9 | 6 | 12 | 1 |
| 2/5 | 2.5 | Wie hoch ist die Eintrittswahrscheinlichkeit eines Black-Swan-Ereignisses im Cyber-Raum? | nahezu null | sehr hoch | null | genauso hoch wie bei anderen Cyber-Risiken |
| **Lektion/**  **Frage-Nr.** | **Abschnitt** | **Frage** | **Richtige Antwort** | **Falsche Antwort** | **Falsche Antwort** | **Falsche Antwort** |
| 3/1 | 3.1 | Welche Bedeutung haben die Kanten in Attack-Trees? | Die Kanten stellen Verbindungen zwischen Bedrohungen dar. | Die Kanten stellen eine Bedrohung dar. | Die Kanten stellen die Auswirkungen einer Bedrohung dar. | Die Kanten stellen die Eintrittswahrscheinlichkeit einer Bedrohung dar. |
| 3/2 | 3.2 | Was ist die gewünschte Eigenschaft für eine Spoofing-Bedrohung? | Authentifizierung | Integrität | Reputationsverlust | Vertraulichkeit |
| 3/3 | 3.2 | Welche Bedrohung ist in STRIDE bei einem Datenfluss nicht möglich? | Erweiterung der Berechtigungen | Manipulation | Offenlegung von Informationen | Denial-of-Service |
| 3/4 | 3.3 | Welche Bedrohung ist in LINDDUN dieselbe wie in STRIDE? | Offenlegung von Informationen | Verknüpfbarkeit | Erkennbarkeit | Ahnungslosigkeit |
| 3/5 | 3.3 | Was ist in LINDDUN eine Minderungsmaßnahme? | unnötige Daten entfernen | Besitz der Daten verbergen | Daten an eine/n Benutzer:in binden | möglichst viele Daten speichern |
| **Lektion/**  **Frage-Nr.** | **Abschnitt** | **Frage** | **Richtige Antwort** | **Falsche Antwort** | **Falsche Antwort** | **Falsche Antwort** |
| 4/1 | 4.1 | Was ist NIST? | eine Behörde des Handelsministeriums der Vereinigten Staaten | eine Behörde der Europäischen Kommission | eine Behörde des Innenministeriums der Bundesrepublik Deutschland | eine Behörde des Verteidigungsministeriums des Vereinigten Königreichs |
| 4/2 | 4.1 | Auf welcher Ebene befinden sich die Geschäftsprozesse in der NIST-Risikomanagement-Pyramide? | Ebene 2 | Ebene 1 | Ebene 3 | Ebene 4 |
| 4/3 | 4.1 | Was ist kein Schritt im NIST-Risikomanagementprozess? | entwickeln | vorbereiten | kategorisieren | implementieren |
| 4/4 | 4.2 | Was ist ein Teil der Risikoidentifizierung gemäß ISO/IEC 27005? | Identifizierung der bestehenden Maßnahmen | Identifizierung der Prozesse | Identifizierung der Bedrohungsakteure | Identifizierung früherer Risiken |
| 4/5 | 4.3 | Was beschreibt BSI 100-3 am besten? | Risikoanalyse durchführen | Incident-Response umsetzen | Sichere Entwicklung erreichen | Risikomanagement einsetzen |
| **Lektion/**  **Frage-Nr.** | **Abschnitt** | **Frage** | **Richtige Antwort** | **Falsche Antwort** | **Falsche Antwort** | **Falsche Antwort** |
| 5/1 | 5.1 | Was ist ein primäres Asset? | Kundenkontakte | Geheimnisse | Personal | Prozesse |
| 5/2 | 5.1 | Was gehört nicht zu einem Risikobewertungsprozess? | Umsetzung der Minderungsmaßnahmen | Bewertungsvorbereitung | Threat Modeling | Risikobewertung |
| 5/3 | 5.1 | Was ist eine Threat-Modeling-Methode? | PASTA | NOODLE | PIZZA | SALAD |
| 5/4 | 5.3 | Was sollte bei jedem Schritt des SEI-Risikomanagement-Paradigmas getan werden? | kommunizieren | kontrollieren | verfolgen | planen |
| 5/5 | 5.2 | Was ist keine gültige Minderungsmaßnahme für Black-Swan-Ereignisse? | Eintrittswahrscheinlichkeit verringern | Auswirkungen verringern | das Risiko übertragen | das Risiko akzeptieren |
| **Lektion/**  **Frage-Nr.** | **Abschnitt** | **Frage** | **Richtige Antwort** | **Falsche Antwort** | **Falsche Antwort** | **Falsche Antwort** |
| 6/1 | 6.1 | Was ist „Risikobereitschaft“? | die Schwelle, wie hoch ein Risiko sein darf, damit es noch akzeptiert wird | die Schwelle, wie viele Risiken akzeptiert werden können | das allgemeine Risikoniveau einer Organisation | die maximale Risikostufe, die eine Bedrohung erreichen kann |
| 6/2 | 6.2 | Was gehört nicht zum Krisenmanagement? | Verringerung | Bereitschaft | Reaktion | Erholung |
| 6/3 | 6.2 | In welcher Phase des Incident-Response-Prozesses findet die Rekonstruktion statt? | Behandlung | Nachbearbeitung | technische Vorbereitung | organisatorische Vorbereitung |
| 6/4 | 6.3 | Was ist eine Sicherheitslösung? | SIEM | SDLC | PDCA | ESD |
| 6/5 | 6.4 | Welches Ereignis ist normalerweise nicht durch eine Cyber-Versicherung abgedeckt? | ein vom Systemadministrator verursachter Unfall | Datenmissbrauch | Datenverlust | Zweckentfremdung des Systems |