**FRAGE 1 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 01**

**Definieren und erklären Sie die Eigenschaften einer Cyber-Katastrophe.**

Reichweite (1 Pkt): Eine große Gruppe von Benutzerinnen ist von dem Ereignis betroffen. (1 Pkt)

Ausfall (1 Pkt): Ein Dienst, der dem/der Endverbraucher:in zur Verfügung gestellt wird, ist unbrauchbar. Endbenutzer:innen können diesen Dienst nicht nutzen, was sich auf ihre Arbeit oder ihr Leben auswirkt. (1 Pkt)

Unkontrollierbarkeit (1 Pkt): Die Organisation ist nicht mehr in der Lage, ein Ereignis, das sie betrifft, zu kontrollieren. (1 Pkt)

**FRAGE 2 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 01**

**Beschreiben Sie die verschiedenen Arten von Cyber-Katastrophen. Nennen Sie je ein Beispiel.**

Globale Cyber-Katastrophe (1 Pkt): Die Reichweite dieser Katastrophe ist global. Das Ereignis hat globale Auswirkungen. (1 Pkt)

Lokale Cyber-Katastrophe (1 Pkt): Die Reichweite ist auf eine Gruppe von Benutzern beschränkt. Die Auswirkungen des Ereignisses sind auf eine Gruppe von Personen oder eine Organisation beschränkt (1 Pkt)

Beispiele:

Globale Cyber-Katastrophe: (1 Pkt)

* **Code Red**
* **Conficker**
* **Dyn DDoS-Angriff**
* **WannaCry / Not Petya Ransomware**

**Lokale Cyber-Katastrophe: (1 Pkt)**

* **AWS-Cloud-Unterbrechung**
* **Garmin Ransomware-Angriff**
* **Ausfall von Azure AAD**

**FRAGE 3 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 01**

**Ein Unternehmen hat einen Designfehler in seiner Webanwendung festgestellt, dessen Behebung 10.000 € kosten würde. Die Anwendung verarbeitet geistiges Eigentum von Kunden und Kundinnen und der Designfehler könnte diese Daten offenlegen. Erklären Sie, wann und warum das Unternehmen das Risiko mindern muss.**

Das Unternehmen muss das Risiko mindern, wenn der potenzielle Verlust höher ist als die Kosten für die Behebung des Designfehlers (3 Pkte). Dies ist darauf zurückzuführen, dass das Risikomanagement verhindern soll, dass das Unternehmen Geld verliert, da es billiger ist, den Fehler zu beheben, als ihn im System zu belassen (3 Pkte).

**FRAGE 4 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 01**

**Erklären Sie, warum Risikoabstraktion in einem Unternehmen notwendig ist. Nennen Sie zwei Beispiele dafür, wie Risiken abstrahiert werden können.**

Risikoabstraktion wird benötigt, um Risiken für verschiedene Managementebenen zusammenzufassen (2 Pkte).

Beispiele:

Ein Krypto-Malware-Angriff kann als finanzielles Risiko (2 Pkte) abstrahiert werden. Eine Datenschutzverletzung kann zu einem Reputationsrisiko (2 Pkte) abstrahiert werden.

**Erklären Sie den Unterschied zwischen einem Risiko und einer Bedrohung und wie diese zusammenhängen.**

**Nennen Sie ein Beispiel für eine Bedrohung mit einem daraus resultierenden Risiko für die Organisation und ein Beispiel für eine Bedrohung ohne Risiko für eine Organisation.**

Ein Risiko ist das Ausmaß der Auswirkungen (1 Pkt), die eine Bedrohung auf eine Organisation haben kann, in Kombination mit der Wahrscheinlichkeit (1 Pkt), dass diese Bedrohung tatsächlich eintritt.

Eine Bedrohung ist die Quelle eines Risikos. Im Allgemeinen ist eine Bedrohung ein Ereignis (1 Pkt), das der Organisation schaden könnte (1 Pkt). Der daraus resultierende Schaden kann die Organisation selbst oder ein Asset der Organisation betreffen (1 Pkt).

Nicht alle Bedrohungen für eine Organisation stellen gleichzeitig Risiken für diese Organisation dar (1 Pkt), aber alle Risiken beinhalten eine Bedrohung (1 Pkt). Eine Bedrohung, die unabhängig (1 Pkt) von einer Organisation ist, würde kein Problem verursachen (1 Pkt).

Zum Beispiel ist ein Exploit für ein bestimmtes System eine schwere Bedrohung (1,5 Pkte). Wenn die Organisation dieses bestimmte System jedoch nicht verwendet, stellt es kein Risiko dar (1 Pkt), da es unmöglich ist, dass diese Bedrohung ein Problem verursacht (1,5 Pkte).

Auf der anderen Seite birgt eine Sicherheitslücke in einer Webanwendung die Gefahr, dass diese Sicherheitslücke ausgenutzt wird (1,5 Pkte). Wenn Assets der Organisation in dieser Anwendung gespeichert sind, besteht für die Organisation das Risiko, dass diese Assets gestohlen oder beschädigt werden (1,5 Pkte).

Zusammenfassend lässt sich sagen, dass eine Bedrohung zu einem Risiko für die Organisation wird, wenn eine gewisse Wahrscheinlichkeit (1,5 Pkte) besteht, dass diese Bedrohung Auswirkungen haben wird. (1,5 Pkte)

**Definieren und erläutern Sie die verschiedenen Bedrohungsquellen und nennen Sie jeweils zwei Beispiele.**

Böswillig (1 Pkt): Eine absichtlich von einer Person durchgeführte Aktion, die darauf abzielt, dem Asset zu schaden (2 Pkte).

* **Ein nicht autorisierter Benutzer erhält aufgrund eines Exploits Zugriff auf interne Daten (1,5 Pkte)**
* **Jemand stiehlt ein Autorisierungs-Token, um Zugang zur administrativen Schnittstelle zu erhalten (1,5 Pkte)**
* **Menschlich nicht böswillig (1 Pkt): Eine nicht vorsätzliche Aktion eines Menschen, die dem Asset schadet. Diese Aktion ist nicht dazu gedacht, dem System zu schaden und war in den meisten Fällen ein Fehler eines Beteiligten. (2 Pkte)**
* **Ein Fehler in der Software macht interne Daten für externe Benutzer:innen zugänglich (1,5 Pkte).**
* **Die Installation eines neuen Patches geht schief, weil einige Systeme übersehen wurden (1,5 Pkte)**

Nicht-menschlich (nicht böswillig) (1 Pkt): Eine Aktion oder ein Ereignis, das nicht von einem menschlichen Akteur eingeleitet wird. Diese Aktion beruht auf höherer Gewalt und entzieht sich der Kontrolle (2 Pkte).

* **Hochwasser zerstört ein Rechenzentrum (1,5 Pkte)**
* **Ein Sturm verhindert den Start eines Flugzeugs, in dem sich kritische Ersatzteile befinden (1,5 Pkte).**

**FRAGE 7 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 02**

**Nennen Sie die verschiedenen Komponenten von Eintrittswahrscheinlichkeit und Auswirkungen in der OWASP-Risikobewertungsmethode.**

Eintrittswahrscheinlichkeit:

* **Bedrohungsakteur (1 Pkt)**
* **Angriffsvektor (1 Pkt)**
* **Schwachstelle (1 Pkt)**
* **Sicherheitsmaßnahmen (1 Pkt) Auswirkungen:**
* **Technische Auswirkungen (1 Pkt)**
* **Geschäftliche Auswirkungen (1 Pkt)**

**FRAGE 8 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 02**

**Erläutern Sie die Definition von Eintrittswahrscheinlichkeit und Auswirkungen in der OWASP-Risikobewertungsmethode. Nennen Sie auch die Unterkategorien.**

Die Auswirkungen beschreiben, wie hoch der potenzielle Schaden ist, den eine Bedrohung für eine Organisation verursachen kann (1 Pkt). OWASP definiert die Auswirkungen in zwei Kategorien. Die technischen Auswirkungen und die geschäftlichen Auswirkungen (2 Pkte). Die Eintrittswahrscheinlichkeit beschreibt, wie wahrscheinlich es ist, dass eine Bedrohung in einer Organisation auftritt (1 Pkt). Die Eintrittswahrscheinlichkeit wird nach OWASP in folgende Kategorien unterteilt:

* **Bedrohungsakteur (0,5 Pkte)**
* **Angriffsvektor (0,5 Pkte)**
* **Schwachstelle (0,5 Pkte)**
* **Sicherheitsmaßnahmen (0,5 Pkte)**

**FRAGE 9 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 02**

**Nennen Sie drei Risikomanagementstrategien und jeweils ein Beispiel.**

Risiko vermeiden (1 Pkt): Das Rechenzentrum liegt in einem Unwettergebiet. Das Rechenzentrum wird in ein anderes Gebiet verlegt, in dem es keine Unwetter gibt (1 Pkt).

Risiko verringern oder mindern (1 Pkt): Das Rechenzentrum liegt in einem Unwettergebiet. Das Rechenzentrum wird unwettersicher gebaut (1 Pkt).

Risiko übertragen (1 Pkt): Das Rechenzentrum liegt in einem Unwettergebiet. Es wird eine Elementarschadenversicherung abgeschlossen (1 Pkt).

Risiko akzeptieren (1 Pkt): Das Rechenzentrum liegt in einem Unwettergebiet. Das Risiko, dass ein Unwetter das Rechenzentrum beschädigen könnte, wird akzeptiert (1 Pkt).

**FRAGE 10 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 02**

**Definieren Sie die Risikomanagementkategorie für die folgenden Beispiele.**

1. **Das Rechenzentrum liegt in einem Unwettergebiet. Das Rechenzentrum wird in ein anderes Gebiet verlagert, in dem es keine Unwetter gibt**
2. **Das Rechenzentrum liegt in einem Unwettergebiet. Das Rechenzentrum wird unwettersicher gebaut**
3. **Das Rechenzentrum liegt in einem Unwettergebiet. Es wird eine Elementarschadenversicherung abgeschlossen.**
	1. **Das Rechenzentrum liegt in einem Unwettergebiet. Das Rechenzentrum wird in ein anderes Gebiet verlegt, in dem es keine Unwetter gibt -> Risiko vermeiden (2 Pkte).**
	2. **Das Rechenzentrum liegt in einem Unwettergebiet. Das Rechenzentrum wird unwettersicher gebaut -> Risiko verringern oder mindern (2 Pkte).**
	3. **Das Rechenzentrum liegt in einem Unwettergebiet. Es wird eine Elementarschadenversicherung abgeschlossen -> Risiko übertragen (2 Pkte).**

**Ein identifiziertes Risiko verfügt über folgende Werte. Berechnen Sie das Gesamtrisikoniveau (fügen Sie die Berechnung für jeden Schritt bei).**

* **Der Bedrohungsakteur verfügt über Netzwerk- und Programmierkenntnisse (6).**
* **Die Motivation ist eine hohe Belohnung (9).**
* **Ein besonderer Zugang oder besondere Ressourcen sind erforderlich (4).**
* **Nur Partner haben Zugriff auf das System (5).**
* **Die Schwachstelle war schwer zu entdecken (3).**
* **Die Ausnutzung ist schwierig (5).**
* **Die Schwachstelle ist ziemlich offensichtlich (6).**
* **Es findet eine aktive Protokollierung und Überprüfung statt (3).**
* **Möglicherweise werden nur wenige kritische Daten offengelegt (6).**
* **Die Integrität ist leicht beschädigt (1).**
* **Bei den sekundären Diensten ist nur eine minimale Unterbrechung möglich (1).**
* **Die Bedrohung ist vollständig nachvollziehbar (1).**
* **Es gibt eine signifikante Auswirkung auf den Jahresgewinn (7).**
* **Ein Verlust des Firmenwerts ist möglich (5).**
* **Es könnte zu minimalen Verstößen gegen die Vorschriften kommen (2).**
* **Der Datenschutz von höchstens einer einzelnen Person ist betroffen (1)**



Berechnen Sie das Gesamtrisikoniveau (2 Pkte): Sowohl die Eintrittswahrscheinlichkeit als auch die Auswirkungen ergeben einen mittleren Wert, daher ist das Risiko ebenfalls mittel.

**Bewerten und erläutern Sie die Wahrscheinlichkeit des Bedrohungsakteurs und der Schwachstelle für das folgende Szenario:**

**Es gab eine Datenschutzverletzung. Der Angreifer war ein angestellter Netzwerk-/Systemadministrator der Organisation und er verdiente durch den Verkauf der Daten eine Menge Geld. Ein spezieller Zugang zur Produktionsdatenbank wurde genutzt, um die Daten über ein falsch konfiguriertes Berechtigungsmanagementsystem zu extrahieren. Die Schwachstelle war für den Angreifer leicht zu finden und auszunutzen, da ihm alle notwendigen Informationen zur Verfügung standen. Der Angreifer erfuhr von dieser Sicherheitslücke durch ein Ticket, das seinem Team zugewiesen wurde. Es war also offensichtlich für ihn. Glücklicherweise hatte das System eine aktive Protokollierung und die Protokolldateien wurden überprüft, um den Angreifer schnell zu finden.**

Bedrohungsakteur:

* **Kompetenzniveau: Netzwerk-/Systemadministrator (1 Pkt) -> (6) Netzwerk- und Programmierkenntnisse (1 Pkt)**
* **Motiv: viel Geld mit dem Verkauf der Daten verdient (1 Pkt) -> (9) hohe Belohnung (1 Pkt)**
* **Gelegenheit: Es wurde ein spezieller Zugriff auf die Produktionsdatenbank verwendet (1 Pkt) -> (4) besonderer Zugang oder Ressourcen erforderlich (1 Pkt)**
* **Größe: Angreifer war ein angestellter Netzwerk-/Systemadministrator (1 Pkt) -> (2) Systemadministratoren (1 Pkt)**

(1 Pkt)



Schwachstelle:

* **Schwierigkeit der Entdeckung: für den Angreifer leicht zu finden und auszunutzen, da ihm alle notwendigen Informationen zur Verfügung standen (1 Pkt) -> (7) leicht (1 Pkt)**
* **Schwierigkeit der Ausnutzung: für den Angreifer leicht zu finden und auszunutzen, da er alle notwendigen Informationen zur Verfügung hatte (1 Pkt) -> (7) leicht (1 Pkt)**
* **Kenntnis: erfuhr von dieser Sicherheitslücke durch ein Ticket, das seinem Team zugewiesen wurde (1 Pkt) -> (6) offensichtlich (1 Pkt)**
* **Intrusion Detection: Das System wurde aktiv protokolliert und die Protokolldateien wurden überprüft (1 Pkt) -> (3) protokolliert und überprüft (1 Pkt)**

(1 Pkt)



**Nennen Sie die STRIDE-Bedrohungen und die gewünschten Eigenschaften für jede Bedrohung.**

* **Spoofing (0,5 Pkte) <-> Authentifizierung (0,5 Pkte)**
* **Manipulation (0,5 Pkte) <-> Integrität (0,5 Pkte)**
* **Repudiation (0,5 Pkte) <-> Nicht-Abstreitbarkeit (0,5 Pkte)**
* **Offenlegung von Informationen (0,5 Pkte) <-> Vertraulichkeit (0,5 Pkte)**
* **Denial-of-Service (0,5 Pkte) <-> Verfügbarkeit (0,5 Pkte)**
* **Erhöhung der Berechtigungen (0,5 Pkte) <-> Autorisierung (0,5 Pkte)**

**FRAGE 14 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 03**

**Nennen und erläutern Sie sechs LINDDUN-Bedrohungen.**

* **Verknüpfbarkeit (0,5 Pkte): Ein Angreifer ist in der Lage, zwei Objekte von Interesse zu verknüpfen, ohne die Identität der betroffenen Datensubjekte zu kennen. (0,5 Pkte)**
* **Identifizierbarkeit (0,5 Pkte): Ein Angreifer ist in der Lage, ein Datensubjekt aus einer Reihe von Datensubjekten durch ein Objekt von Interesse zu identifizieren. (0,5 Pkte)**
* **Nicht-Abstreitbarkeit (0,5 Pkte): Das Datensubjekt ist nicht in der Lage, eine Forderung zu bestreiten (z. B. weil sie eine Aktion durchgeführt oder eine Anfrage gestellt hat). (0,5 Pkte)**
* **Erkennbarkeit (0,5 Pkte): Ein Angreifer ist in der Lage zu erkennen, ob ein interessantes Objekt zu einem Datensubjekt vorhanden ist oder nicht, unabhängig davon, ob er den Inhalt selbst lesen kann. (0,5 Pkte)**
* **Offenlegung von Informationen (0,5 Pkte): Ein Angreifer ist in der Lage, den Inhalt eines Objekts von Interesse über ein Datensubjekt zu erfahren. (0,5 Pkte)**
* **Unkenntnis (0,5 Pkte): Die betroffene Person hat keine Kenntnis von der Erhebung, Verarbeitung, Speicherung oder Weitergabe (und den entsprechenden Zwecken) der personenbezogenen Daten des Datensubjekts. (0,5 Pkte)**
* **Nichteinhaltung von Vorschriften (0,5 Pkte): Die Verarbeitung, Speicherung oder Handhabung personenbezogener Daten ist nicht mit den Gesetzen, Vorschriften und/oder Richtlinien konform. (0,5 Pkte)**

**Beschreiben Sie drei Gemeinsamkeiten und drei Unterschiede zwischen STRIDE und LINDDUN.**

Gemeinsamkeiten:

* **Sowohl LINDDUN als auch STRIDE sind Bedrohungsmodellmethoden. (1 Pkt)**
* **Beides sind Merkhilfen für die Bedrohungskategorien. (1 Pkt)**
* **Beide basieren auf der Modellierung von Systemen und dem Zeichnen von DFDs. (1 Pkt)**

Unterschiede:

* **STRIDE konzentriert sich auf die Assets der Systeme und LINDDUN auf die Objekte von Interesse der Datensubjekte. (1 Pkt)**
* **STRIDE konzentriert sich auf Systembedrohungen und LINDDUN auf Datenschutzbedrohungen. (1 Pkt)**
* **STRIDE konzentriert sich hauptsächlich auf Angriffe von außen und LINDDUN berücksichtigt auch, wie die Daten der Benutzer:innen vor dem System selbst geschützt werden können. (1 Pkt)**

**FRAGE 16 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 03**

**Nennen und erläutern Sie drei Datenflussdiagrammsymbole.**

Prozess (1 Pkt): Jeder ausgeführte Code, der vom System kontrolliert wird. (1 Pkt)

Datenfluss (1 Pkt): Jeder Datenfluss zwischen Prozessen, Datenspeichern oder externen Einheiten (1 Pkt).

 Datenspeicher (1 Pkt): Jedes Teilsystem, das vom System kontrollierte Daten speichert. (1 Pkt)

Externe Entität (1 Pkt): Jede externe Einheit (Benutzer oder System), die mit dem System interagiert, aber nicht vom System selbst gesteuert wird. (1 Pkt)

Vertrauensgrenze (1 Pkt): Eine Grenze zwischen zwei Entitäten, die einen Vertrauenswechsel markiert (z. B. zwischen einem Unternehmensnetzwerk und dem Internet) (1 Pkt)

**FRAGE 17 VON 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F1/Lektion 03**

**Zeichnen Sie einen Attack-Tree in Listenform für das folgende Szenario.**

**Das Hauptziel besteht in der Exfiltration von Daten. Dies kann auf zwei Arten geschehen. Die erste besteht darin, die Daten über einen Mitarbeiter zu erlangen. Der Mitarbeiter kann entweder bestochen oder bedroht werden. Die andere Möglichkeit ist, in das System einzubrechen. Dazu ist es erforderlich, eine Schwachstelle zu finden und diese Schwachstelle auszunutzen.**

1. **Daten exfiltrieren (2 Pkte)**
	1. **Daten durch Mitarbeiter erlangen (3 Pkte)**
		1. **Mitarbeiter bestechen (2 Pkte)**
		2. **Mitarbeiter bedrohen (2 Pkte)**
	2. **In das System einbrechen (&) (3 Pkte das & ist wichtig)**
		1. **Schwachstelle finden (2 Pkte)**
		2. **Schwachstelle ausnutzen (2 Pkte) (2 Pkte) für die richtige Darstellung**

**FRAGE 18 VON 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F1/Lektion 03**

**Nennen Sie die STRIDE-Bedrohungen und ein Beispiel für jede Bedrohung.**

* **Spoofing (1 Pkt): Ein Benutzer kann seine Benutzer-ID im Frontend ändern, um sich als ein anderer Benutzer auszugeben (2 Pkte)**
* **Manipulation (1 Pkt): Ein Benutzer kann eine DB-Abfrage manipulieren, um Daten von anderen Benutzern zu überschreiben (2 Pkte)**
* **Repudiation (1 Pkt): Wenn keine Systemprotokollierung vorhanden ist, können Benutzeraktionen nicht rekonstruiert werden. (2 Pkte)**
* **Offenlegung von Informationen (1 Pkt): Ein offener API-Endpunkt legt interne Dokumente offen (2 Pkte)**
* **Denial-of-Service (1 Pkt): Eine böswillige Benutzereingabe lässt die Anwendung abstürzen (2 Pkte)**
* **Erweiterung der Berechtigungen (1 Pkt): Mit einer böswilligen Eingabe kann ein Benutzer erweiterte Berechtigungen erlangen (2 Pkte)**

**Nennen und erläutern Sie die drei Ebenen des Risikomanagements nach NIST.**

* + - 1. **Organisation (1 Pkt): Die Organisationsebene stellt die höchste Ebene dar. Auf dieser Ebene werden die Risiken, denen die gesamte Organisation ausgesetzt ist, und die organisationsweiten Risikomanagementprozesse verwaltet. (1 Pkt)**
			2. **Mission/Geschäftsprozess (1 Pkt): Die Ebene der Mission/Geschäftsprozesse ist die zweite Ebene. Die auf dieser Ebene durchgeführten Aktivitäten befassen sich nicht mit technischen Risiken, sondern konzentrieren sich auf das Management von Produkt- oder Projektrisiken. (1 Pkt)**
			3. **Informationssystem (1 Pkt): Die dritte Ebene befasst sich mit dem Risiko aus der Perspektive des Informationssystems, wobei der Schwerpunkt auf den technischen und organisatorischen Risiken liegt, denen ein Informationssystem ausgesetzt ist. (1 Pkt)**

**FRAGE 20 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 04**

**Nennen und erläutern Sie die drei Ziele für Minderungsmaßnahmen laut BSI.**

* **Vollständigkeit (1 Pkt): Bieten die Standard-Sicherheitsmaßnahmen Schutz vor allen Aspekten der jeweiligen Bedrohung? (1 Pkt)**
* **Stärke des Mechanismus (1 Pkt): Wirken die in den Standard-Sicherheitsmaßnahmen empfohlenen Schutzmechanismen jeder Bedrohung angemessen entgegen? (1 Pkt)**
* **Zuverlässigkeit (1 Pkt): Wie schwierig ist es, die geplanten Sicherheitsmechanismen zu umgehen? (1 Pkt)**

**Ordnen Sie die sechs Aussagen den sechs Aufgaben im Risikomanagement gemäß ISO/IEC 27005 zu:**

* **Geltungsbereich festlegen**
* **Risiko identifizieren**
* **Risiko vermeiden**
* **Verbleibende Risiken akzeptieren**
* **Risiken dem Management vorstellen**
* **Risiken in einem Ticketsystem zur Nachverfolgung eintragen**
* **Geltungsbereich festlegen -> Kontext ermitteln (1 Pkt)**
* **Risiko identifizieren -> Risikobewertung (1 Pkt)**
* **Risiko vermeiden -> Risikobehandlung (1 Pkt)**
* **Verbleibende Risiken akzeptieren -> Risikoakzeptanz (1 Pkt)**
* **Risiken dem Management vorstellen -> Risikokommunikation (1 Pkt)**
* **Risiken in einem Ticketsystem zur Nachverfolgung eintragen -> Risikoüberwachung und -überprüfung (1 Pkt)**

**FRAGE 22 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 04**

**Nennen Sie die Schritte im Risikomanagementprozess nach ISO/IEC 27005 und geben Sie Beispiele dafür.**

Risikoidentifizierung (1 Pkt): Bedrohungsmodell erstellen, um die Bedrohungen zu identifizieren (1 Pkt).

Risikoeinschätzung (1 Pkt): Bedrohungen aus dem Bedrohungsmodell nutzen und das Risiko dieser Bedrohungen einschätzen (1 Pkt).

Risikobewertung (1 Pkt): Identifizierte Risiken vergleichen und feststellen, welches davon sofortige Aufmerksamkeit erfordert (1 Pkt).

**Beschreiben Sie den im BSI-Standard 100-3 definierten Prozess der Risikobewertung.**

Der BSI-Standard 100-3 beschreibt, wie eine Risikoanalyse auf der Grundlage des IT-Grundschutzes durchzuführen ist und ist in sieben Teile unterteilt: (1 Pkt)

Vorarbeiten (1 Pkt):

* **Der erste Teil beschreibt die Arbeiten, die vor einer Risikobewertung abgeschlossen werden müssen. (1 Pkt)**

Vorbereiten der Bedrohungsübersicht (1 Pkt):

* **Die Bedrohungsübersicht ist das erste, was ein Entscheidungsträger sieht (1 Pkt). Dementsprechend ist es wichtig, dass sie informativ ist und einen Überblick über den Sicherheitsstatus des analysierten Systems bietet. (1 Pkt) Bestimmung von zusätzlichen Bedrohungen (1 Pkt):**
* **Das Modell des IT-Grundschutzes enthält eine Reihe von Bedrohungen für Systeme (1 Pkt). Unter bestimmten Umständen können jedoch zusätzliche isolierte Bedrohungen, denen ein System ausgesetzt ist, über den Umfang der im IT-Grundschutz-Modell genannten Bedrohungen hinausgehen. (1 Pkt)**

Bedrohungsbewertung (1 Pkt):

Der BSI-Standard 100-3 beschreibt die Überprüfung, ob die im Sicherheitskonzept bereits implementierten oder geplanten Maßnahmen, in der Regel Standard-Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen, für jede Bedrohung einen ausreichenden Schutz bieten oder ob Lücken bestehen. (2 Pkte)

Umgang mit Risiken (1 Pkt):

In der Regel identifiziert die Bedrohungsanalyse eine Reihe von Risiken, die durch die Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen nicht ausreichend gemindert werden. (1 Pkt) Konsolidierung des Sicherheitskonzepts (1 Pkt):

Das Sicherheitskonzept wird konsolidiert werden müssen, wenn zusätzliche Sicherheitsmaßnahmen hinzugefügt werden, um die verbleibenden Risiken zu bewältigen (1 Pkt). Darüber hinaus müssen alle Risiken im Sicherheitskonzept zusammen mit der Strategie zur Risikobehandlung dokumentiert werden (1 Pkt).

Feedback zum Sicherheitsprozess (1 Pkt):

Nach einer erfolgreichen Risikoanalyse können die Ergebnisse der Analyse und das Sicherheitskonzept genutzt werden, um den Sicherheitsprozess zu modifizieren. (1 Pkt)

**Benennen Sie die sechs Schritte des Risikomanagementprozesses gemäß NIST SP 800-37 und nennen und erläutern Sie für jeden Schritt eine Beispielaufgabe.**

Vorbereiten (1 Pkt):

* **Definieren einer Risikomanagementstrategie (1 Pkt): Risikomanagementstrategie für die Organisation erarbeiten, die eine Bestimmung der Risikotoleranz beinhaltet. (1 Pkt)**

Kategorisieren (1 Pkt):

* **Kategorisieren und dokumentieren der Systeme (1 Pkt): Die Systeme werden charakterisiert und dokumentiert. Dazu gehören der Zweck des Systems, die verantwortlichen Personen und allgemeine Systembeschreibungen. (1 Pkt)**

Auswählen (1 Pkt):

* **Auswählen eines Basisschutzes zur Verringerung des Risikos dieser Systeme (1 Pkt): Bei den Basismaßnahmen handelt es sich um vordefinierte Sätze von Maßnahmen, die speziell für den Schutzbedarf eines Systems zusammengestellt wurden. Basismaßnahmen dienen als Ausgangspunkt für den Schutz eines Systems. (1 Pkt)**

Implementieren (1 Pkt):

* **Implementieren der entwickelten Maßnahmen (1 Pkt): Die Organisation implementiert die zuvor definierten Sicherheitsmaßnahmen. (1 Pkt)**

Bewerten(1 Pkt):

\*Bewerten der Sicherheitsmaßnahmen (1 Pkt): Die Sicherheitsmaßnahmen werden bewertet, um zu prüfen, ob die definierten Maßnahmen das Risiko verringern (1 Pkt)

Autorisieren (1 Pkt):

* **Risikoautorisierung (1 Pkt): Bestimmen, ob das Risiko durch den Betrieb oder die Nutzung des Informationssystems oder die Bereitstellung oder Nutzung typischer Maßnahmen akzeptabel ist. (1 Pkt)**

Überwachen (1 Pkt):

* **Überwachen von Systemänderungen (1 Pkt): Überwachen des Informationssystems und seiner Betriebsumgebung in Hinblick auf Änderungen, die sich auf die Sicherheit und den Datenschutz des Systems auswirken. (1 Pkt)**

**Beschreiben Sie zwei Möglichkeiten, ein Black-Swan-Ereignis zu bewerten.**

Die erste Bewertungsstrategie für Black-Swan-Ereignisse besteht darin, die Ereignisse zu bewerten und zu analysieren, was mit dem Geltungsbereich passieren würde (2 Pkte). Diese Ereignisse können frühere Black-Swan-Ereignisse und Katastrophen sein. Diese Ereignisse werden dann durchgespielt und die daraus resultierenden Risiken für die Assets analysiert. (1 Pkt)

Die zweite Bewertungsstrategie ist im Grunde die erste in umgekehrter Reihenfolge. Bei dieser Strategie werden die Bedrohungen für die Assets bewertet und daraufhin die Ereignisse ermittelt, die zu Risiken führen können (2 Pkte). Diese Risiken können aus bekannten Bedrohungen aus Threat-Modeling-Strategien resultieren. Mit dieser Bedrohung im Hinterkopf können nun Szenarien dafür gefunden werden. Naturereignisse könnten eine Möglichkeit sein. (1 Pkt)

**FRAGE 26 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 05**

**Erklären Sie die Begriffe „identifizieren“, „analysieren“ und „planen“ aus dem SEI-Risikomanagementparadigma.**

Identifizieren:

In einem ersten Schritt werden die Risiken gesucht und identifiziert. Dies geschieht in der Regel im Rahmen der Risikobewertung. (2 Pkte)

Analysieren:

Nachdem die Risiken identifiziert wurden, müssen sie analysiert werden. Dies geschieht ebenfalls im Rahmen der Risikobewertung. Die Analyse der Risiken beinhaltet deren Bewertung; d. h. die Bestimmung der Eintrittswahrscheinlichkeit und der Auswirkungen der Risiken für die Organisation. Dies ist wichtig, damit sich die Entscheidungsträger auf die richtigen Risiken konzentrieren können. (2 Pkte)

Planen: Nach der Risikoanalyse kann das identifizierte und bewertete Risiko behandelt werden. Dazu muss für jedes Risiko ein Plan zur Risikominderung erstellt werden. Dieser Plan enthält die Maßnahme und einen Zeitrahmen für die Umsetzung dieser Maßnahme. (2 Pkte)

**Führen Sie sechs Punkte auf, die laut SEI für eine korrekte Erfassung von Risiken erforderlich sind.**

* **Datum (1 Pkt)**
* **Risiko-ID (1 Pkt)**
* **Risikoname (1 Pkt)**
* **Risikominderungsplan (1 Pkt)**
* **Frist (1 Pkt)**
* **Implementierungskontrolle (1 Pkt)**

**FRAGE 28 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 05**

**Nennen Sie sechs Annahmen, die zum Threat Modeling verwendet werden können.**

* **Die Mitarbeitenden der Organisation sind vertrauenswürdig. (1 Pkt)**
* **Der Cloud-Anbieter handelt nicht böswillig. (1 Pkt)**
* **Die verwendete Hardware hat keine bekannten Schwachstellen. (1 Pkt)**
* **Die physische Sicherheit ist gewährleistet. (1 Pkt)**
* **Die Cloud-Infrastruktur funktioniert wie beschrieben. (1 Pkt)**
* **Die Netzwerkinfrastruktur des Rechenzentrums ist gut konzipiert und sicher. (1 Pkt)**

**In einer Web-Anwendung wurde eine Sicherheitslücke gefunden. Diese Sicherheitslücke kann dazu genutzt werden, auf interne Daten des Servers zuzugreifen. Die Sicherheitslücke kann nur ausgenutzt werden, wenn ein Benutzer angemeldet ist. Nennen Sie neun mögliche Minderungsmaßnahmen und klassifizieren Sie die Minderungsstrategie dieser Maßnahmen. Nennen Sie eine Minderungsmaßnahme für jede Minderungsstrategie.**

* **Entwickeln einer Lösung für die Sicherheitslücke (1 Pkt) (Risikoverringerung/-minderung) (1 Pkt)**
* **Nur vertrauenswürdigen Benutzern die Anmeldung erlauben (1 Pkt) (Risikovermeidung) (1 Pkt)**
* **Webanwendungs-Firewall einsetzen, um böswillige Anfragen zu blockieren (1 Pkt) (Risikominderung) (1 Pkt)**
* **Sensible Daten von der anfälligen Webanwendung an anderen Ort verschieben (1 Pkt) (Risikovermeidung) (1 Pkt)**
* **Webanwendung so anpassen, dass sie nur vom internen Netzwerk aus zugänglich ist (1 Pkt) (Risikovermeidung) (1 Pkt)**
* **Versicherung abschließen, die den Datenverlust der internen Dokumente abdeckt (1 Pkt) (Risikotransfer) (1 Pkt)**
* **Anbieter für das Hosting und die Verwaltung des Servers und der Webanwendung beauftragen (1 Pkt) (Risikotransfer) (1 Pkt)**
* **Risiko akzeptieren, da es mehr kosten würde, die Sicherheitslücke zu beheben (1 Pkt) (Risikoakzeptanz (1 Pkt)**
* **Maßnahmen implementieren, damit auf die Daten nicht direkt von der Webanwendung aus zugegriffen werden kann (1 Pkt) (Risikoverringerung/-minderung) (1 Pkt)**

**Ein Unternehmen verarbeitet persönliche Daten von Kundinnen und Kunden. Sie werden zusammen mit deren Projektdaten gespeichert. Alle Daten werden in Datenbanken und Netzwerkspeichern gespeichert. Verarbeitet werden die Daten von einem Worker-Cluster und dann auf dem Frontend-Server angezeigt. Geheimnisse werden mit entsprechenden Verfahren für den Zugriff gespeichert.**

**Ordnen Sie die Assets der richtigen Kategorie zu und erläutern Sie jede Kategorie. Nennen Sie ein Beispiel für jede Technologie, die in den unterstützenden Assets verwendet wird.**

Primäre Assets: Primäre Assets sind die Assets, die im Fokus des Unternehmens und des Angreifers stehen. Diese Assets „verdienen das Geld“. Geschäftsaktivitäten und Informationen sind die wichtigsten Assets. (2 Pkte)

* **Persönliche Kundendaten (1 Pkt)**
* **Kundenprojektdaten (1 Pkt)**

Unterstützende Assets: Die sekundären oder unterstützenden Assets sind Dinge, die die primären Assets unterstützen und nur relevant sind, wenn ein primäres Asset durch ein unterstützendes Asset beeinträchtigt wird. (2 Pkte)

* **Datenbank (1 Pkt): MySQL-Datenbank (1 Pkt)**
* **Netzwerkspeicher (1 Pkt): SMB-Netzwerkfreigabe (1 Pkt)**
* **Worker-Cluster (1 Pkt): Virtuelle Maschinen (1 Pkt)**
* **Frontend-Server (1 Pkt): Apache-Webserver (1 Pkt)**
* **Geheimnisse (1 Pkt): Zugriffstoken für die Datenbank (1 Pkt)**
* **Prozesse (1 Pkt): Schlüsselrotationsprozess (1 Pkt)**

**FRAGE 31 VON 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Lektion 06**

**Nennen Sie vier Aufgaben, die ein Security Champion übernehmen kann.**

* **Threat Modeling (1,5 Pkte)**
* **Risikobewertung (1,5 Pkte)**
* **Risikoverfolgung (1,5 Pkte)**
* **Das Team dazu motivieren, die Sicherheitsmaßnahmen zu befolgen (1,5 Pkte)**
* **Best Practices für die Sicherheit prüfen oder verfassen (1,5 Pkte)**
* **Richtlinien zum sicheren Programmieren für das Projektteam festlegen (1,5 Pkte)**
* **Sicherheitsüberprüfungen durchführen (1,5 Pkte)**
* **Automatische Sicherheitsscanner implementieren (1,5 Pkte)**

**Nennen und beschreiben Sie drei Schritte zur Incident-Response-Vorbereitung in der Organisation.**

* **Asset-Management (1 Pkt): Das Asset-Management speichert jegliche Informationen über alle möglichen Assets der Organisation. Dabei kann es sich um primäre oder unterstützende Assets handeln. (1 Pkt)**
* **Rollen und Verantwortlichkeiten (1 Pkt): Die Rollen und Verantwortlichkeiten legen fest, wer welche Aufgaben im Rahmen der Incident-Response übernimmt. Einige Rollen sind z. B. das Bereitschaftsteam, der Incident Investigator, der Incident Manager oder die IT-Abteilung. (1 Pkt)**
* **Zugriffskonzept (1 Pkt): Das Zugriffskonzept beschreibt, wie das Incident-Response-Team auf Systeme oder Assets zugreifen kann. Dazu gehört ein normaler Lesezugriff, z. B. zur Überwachung und Protokollierung, oder ein vollständiger administrativer Zugriff im Falle eines Vorfalls. (1 Pkt)**
* **Kommunikation (1 Pkt): Eine Definition der Kommunikation ist erforderlich, da bei einem Vorfall die Kommunikation unverzüglich hergestellt werden muss. Dazu gehört die interne Kommunikation, die Kommunikation mit Kundinnen und Kunden und die Kommunikation mit den Strafverfolgungsbehörden. (1 Pkt)**
* **Prozessdokumentation (1 Pkt): Alle Aufgaben des Incident-Response-Managements müssen in Prozessen definiert werden. Dadurch erhalten die Teams einen Leitfaden, wie sie sich auf einen Vorfall vorbereiten und wie sie damit umgehen können. (1 Pkt)**
* **Governance und Richtlinien (1 Pkt): Das Incident-Response-Management muss für die Organisation einheitlich sein. Daher sollten Governance und Richtlinien verwendet werden, um diesen Prozess zu deﬁnieren. Diese Richtlinien können z. B. die Definition von Cybervorfällen, die allgemeine Berichterstattung über solche Ereignisse, den Eskalationsprozess oder die Bewertung und Priorisierung von Vorfällen umfassen. (1 Pkt)**
* **Schulung (1 Pkt): Die Reaktion auf Vorfälle muss vermittelt werden. Dies sollte geschehen, damit die Incident-Response-Teams stets auf dem Laufenden sind, was neue Technologien, die Umgebung und die Prozesse der Organisation betrifft. (1 Pkt)**

**FRAGE 33 VON 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Lektion 06**

**Nennen Sie die drei Schritte des Krisenmanagements und geben Sie für jeden ein Beispiel.**

* **Bereitschaft (1 Pkt): Einrichten von Kommunikationskanälen. (1 Pkt)**
* **Reaktion (1 Pkt): Analysieren und Lösen der Krise. (1 Pkt)**
* **Erholung (1 Pkt): Durchführen einer Ursachenanalyse. (1 Pkt)**

**Nennen Sie die drei Schritte der Nachbearbeitungsphase im Incident-Response-Prozess und geben Sie jeweils ein Beispiel.**

Gewonnene Erkenntnisse (1 Pkt): Versammeln der Incident-Response-Verantwortlichen und Besprechung des Incident-Response-Prozesses; feststellen, was besser hätte laufen können (1 Pkt).

Dokumentation (1 Pkt): Verwenden eines dokumentierten Managementsystems, um die durchgeführten Schritte zur Vorfallminderung aufzuschreiben (1 Pkt).

Verbesserung der Organisation (1 Pkt): E-Mail an die Organisation schicken mit der Ursache des Vorfalls und einem Vorschlag für die Absicherung (1 Pkt).

**FRAGE 35 VON 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F2/Lektion 06**

**Erläutern Sie die vier Resilience-Engineering-Maßnahmensätze und nennen Sie zu jedem Maßnahmensatz zwei Beispiele.**

* **Widerstandsmaßnahmen (1 Pkt): Diese Maßnahmen sollen als erste Hürde dazu dienen, den Angreifer zu verlangsamen und zu frustrieren. (1,5 Pkte)**

\*\* Begrenzung für fehlgeschlagene Anmeldungsversuche (1 Pkt)

\*\* Implementierung eines Captcha für das Web-Formular (1 Pkt)

* **Schutzmaßnahmen (1 Pkt): Schutzmaßnahmen sind für die Verhinderung von Angriffen gedacht. (1,5 Pkte)**

\*\* Einrichtung einer sinnvollen Eingabeüberprüfung in der Software (1 Pkt)

\*\* Trennen des Backends vom Internet (1 Pkt)

* **Erkennungsmaßnahmen (1 Pkt): Dieser Maßnahmensatz sollte Maßnahmen zur Erkennung eines Angriffs oder eines böswilligen Ereignisses enthalten. (1,5 Pkte)**

\*\* Implementierung einer sinnvollen Protokollierung und Überwachung (1 Pkt)

\*\* SIEM-Einrichtung für die Protokollkorrelation (1 Pkt)

* **Kompensationsmaßnahmen (1 Pkt): Kompensationsmaßnahmen stellen eine zweite Verteidigungslinie dar, wenn eine Verteidigung in erster Linie nicht möglich ist (1,5 Pkte)**

\*\* Einsatz einer Webanwendungs-Firewall, um böswillige Eingaben zu blockieren (1 Pkt)

\*\* Einrichtung der Mehrfaktor-Authentifizierung für alle Anwendungen im Internet (1 Pkt)

**FRAGE 36 VON 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F2/Lektion 06**

**Über das Protokollierungssystem wurde ein Vorfall in einer Webanwendung entdeckt. Die Angreifer konnten auf den Produktionsdatenbankserver zugreifen. Führen Sie die Bearbeitungsschritte von Vorfällen im Incident-Response-Prozess in der richtigen Reihenfolge auf und erläutern Sie sie. Geben Sie außerdem für jeden Schritt des Szenarios ein Beispiel an.**

Klassifizierung (1 Pkt): Bei der Klassifizierung wird das Eingangsereignis, das zu dem Vorfall geführt hat, analysiert und entschieden, ob es sich um einen echten Vorfall oder einen Fehlalarm handelt. (1,5 Pkte)

* **Protokoll analysieren und ermitteln, ob es sich um einen echten Vorfall handelt (1 Pkt)**

Triage (1 Pkt): Bei der Triage werden die Auswirkungen des Vorfalls analysiert. Hier müssen die betroffenen Assets ermittelt werden. Mit neuen Informationen kann die Triage im Bearbeitungsprozess erneut durchgeführt werden. (1,5 Pkte)

* **Analysieren des Servers und Bestimmen der Reichweite (1 Pkt)**

Eindämmung (1 Pkt): Nachdem die betroffenen Assets gefunden wurden, müssen die Auswirkungen des Vorfalls eingedämmt werden. (1,5 Pkte)

* **Versuchen, die Auswirkungen des Vorfalls zu bewältigen, indem der Server vom Internet getrennt wird (1 Pkt) Beseitigung / Wiederherstellung (1 Pkt): Nachdem der Vorfall eingedämmt wurde, muss die Umgebung gesäubert und alle Spuren des Vorfalls beseitigt oder korrigiert werden. Auch kurzfristige Minderungsmaßnahmen können in diesem Schritt angewendet werden. (1,5 Pkte)**
* **Bereinigen des Datenbankservers und Entfernen der Spuren des Angreifers (1 Pkt)**

Rekonstruktion / Ursachenanalyse (1 Pkt): Wenn der Vorfall eingedämmt und unter Kontrolle ist, kann die Ursachenanalyse beginnen. In dieser Analyse wird untersucht, wie der Vorfall passieren konnte. (1,5 Pkte)

* **Analysieren aller gesammelten Daten und Ermitteln der Ursache des Vorfalls (1 Pkt) (0,5 Pkte für die richtige Reihenfolge)**

**Was ist das Ziel des Risikomanagements?**

**Wählen Sie eine Antwort:**

**Alle möglichen Risiken für ein Unternehmen beseitigen**

**Maßnahmen zur Minderung der identifizierten Risiken planen**

**Entscheidungsträgern dabei helfen, das Risiko für das Unternehmen zu verstehen und es auf ein akzeptables Niveau zu bringen**

**Geeignete Geschäftspläne entsprechend dem Durchschnittsrisiko vorschlagen**

**Die richtige Antwort ist: Entscheidungsträgern dabei helfen, das Risiko für das Unternehmen zu verstehen und es auf ein akzeptables Niveau zu bringen**

**FRAGE 38 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 01**

**Was war die Ursache für die Datenpanne bei Capital One im Jahr 2019?**

**Wählen Sie eine Antwort:**

**Ein falsch konfigurierter Dienst**

**Ein lang andauernder Angriff mit mehreren Phasen**

**Eine missbräuchlich verwendete öffentliche Funktion**

**Ein Angriff eines Staates**

**Die richtige Antwort ist: Ein falsch konfigurierter Dienst**

**Welche Aussage über eine Cyber-Katastrophe ist richtig?**

**Wählen Sie eine Antwort:**

**Cyber-Katastrophen haben keine Auswirkungen auf die reale Welt.**

**Cyber-Katastrophen betreffen eine große Gruppe von Nutzerinnen und Nutzern.**

**Cyber-Katastrophen haben immer schwerwiegende Auswirkungen auf die reale Welt.**

**Cyber-Katastrophen haben normalerweise keine Auswirkungen auf die Benutzer:innen.**

**Die richtige Antwort ist: Cyber-Katastrophen betreffen eine große Gruppe von Nutzerinnen und Nutzern.**

**FRAGE 40 VON 78**

**DLMCSECRAM01\_E\_MC\_mittel/Lektion 01**

**Welches der folgenden Risiken kann als Denial-of-Service-Risiko für**

**eine Organisation abstrahiert werden?**

**Wählen Sie eine Antwort:**

**Ein Angreifer verschafft sich Zugang zu den internen Systemen und legt interne Dokumente offen.**

**Ein interner Mitarbeiter hat das Protokoll einer internen Sitzung über Einstellungsprozesse offengelegt.**

**Der Dienstleister für die Zahlungsabwicklung verweigert die Auszahlung von Geldern als Garantie.**

**Eine Krypto-Malware verschlüsselt die Kundendaten und der Dienst kann dem Benutzer nicht mehr zur Verfügung gestellt werden.**

**Die richtige Antwort ist: Eine Krypto-Malware verschlüsselt die Kundendaten und der Dienst kann dem Benutzer nicht mehr zur Verfügung gestellt werden.**

**Was ist die Bedrohungsquelle eines falsch konfigurierten Servers, der Kundendaten**

**preisgibt?**

**Wählen Sie eine Antwort:**

**Nicht-menschlich, nicht-böswillig**

**Menschlich böswillig Menschlich nicht-böswillig Nicht-menschlich böswillig**

**Die richtige Antwort ist: Menschlich nicht-böswillig**

**FRAGE 42 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 01**

**Welches dieser Ereignisse kann als globale Cyber-Katastrophe eingestuft werden?**

**Wählen Sie eine Antwort:**

**Eine Krypto-Malware verschlüsselt alle Daten einer Organisation.**

**Ein Fehler in einem Dienst unterbricht diesen und die Benutzer:innen können nicht mehr darauf zugreifen.**

**Ein Unwetter legt den Strom in einem Büro lahm und hindert die Mitarbeitenden am Arbeiten.**

**Ein globaler DNS-Ausfall macht das Internet unbrauchbar.**

**Die richtige Antwort ist: Ein globaler DNS-Ausfall macht das Internet unbrauchbar.**

**FRAGE 43 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 01**

**Der Entscheidungsträger einer Organisation mit einem Jahresgewinn von 50 Mio. € hat ermittelt, dass ein Risiko jährliche Kosten von 450.000 € nach sich ziehen könnte. Was wäre die logische Schlussfolgerung?**

**Wählen Sie eine Antwort:**

**Das Risiko muss gemindert werden, wenn die Kosten für die Minderung < 1 % des Gewinns betragen.**

**Das Risiko kann akzeptiert werden, da die Kosten des Risikos < 1 % des Gewinns betragen.**

**Das Risiko kann akzeptiert werden, wenn die Kosten für die Risikominderung jährlich < 450.000 € betragen. Das Risiko muss gemindert werden, da die Kosten des Risikos > 0,1 % des Gewinns betragen.**

**Die richtige Antwort ist: Das Risiko kann akzeptiert werden, wenn die Kosten für die Risikominderung jährlich <**

**450.000 € betragen.**

**Wie lautet die richtige Formel für die Berechnung eines Risikos?**

**Wählen Sie eine Antwort:**

**Die richtige Antwort ist:**

**FRAGE 45 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 02**

**Welche der folgenden Aussagen beschreibt den Bedrohungsakteur nach**

**OWASP?**

**Wählen Sie eine Antwort:**

**Kompetenzniveau**

**Bewusstsein**

**Schwierigkeit der Entdeckung Reifegrad**

**Die richtige Antwort ist: Kompetenzniveau**

**Was ist der schwerwiegendste von OWASP definierte Reputationsschaden?**

**Wählen Sie eine Antwort:**

**Konkurs**

**Markenschaden**

**Großkundenverlust Geschäftswertverlust**

**Die richtige Antwort ist: Markenschaden**

**FRAGE 47 VON 78**

**DLMCSECRAM01\_E\_MC\_mittel/Lektion 02**

**Ein Risiko hat eine Gesamtauswirkung von 2,6 und eine Eintrittswahrscheinlichkeit von 7,3. Wie lautet die Risikostufe**

**in der OWASP-Risikomatrix?**

**Wählen Sie eine Antwort:**

**Kritisch**

**Niedrig Hoch Mittel**

**Die richtige Antwort ist: Mittel**

**Welches der folgenden Ereignisse kann als Black-Swan-Ereignis eingestuft werden?**

**Wählen Sie eine Antwort:**

**Ein Angreifer findet eine Schwachstelle in einem System und löscht alle Daten. Die Organisation ist nun**

**bankrott.**

**Ein Angreifer findet eine Schwachstelle im Server der Organisation. Er verunstaltet die Website und die Organisation verliert an Ansehen.**

**Zwei Unwetter legen beide Rechenzentren auf verschiedenen Kontinenten lahm. Die Organisation kann ihren Dienst nicht anbieten, solange das Unwetter andauert.**

**Kosmische Strahlen ändern ein Bit in der Kommunikation. Ein einzelner Datensatz muss erneut übertragen werden.**

**Die richtige Antwort ist: Zwei Unwetter legen beide Rechenzentren auf verschiedenen Kontinenten lahm. Die Organisation kann ihren Dienst nicht anbieten, solange das Unwetter andauert.**

**FRAGE 49 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 02**

**Ein Frontend-System hat eine Schwachstelle, durch die in einem ganz bestimmten Grenzfall**

**privilegierter Zugriff erlangt werden kann. Es handelt sich um Closed-Source-Software. Bewerten Sie die Schwierigkeit der Ausnutzung.**

**Wählen Sie eine Antwort:**

**Automatisiert**

**Schwierig Leicht Theoretisch**

**Die richtige Antwort ist: Theoretisch**

**FRAGE 50 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 02**

**Eine Organisation bietet Nutzerinnen und Nutzern einen Dienst an. Ein Bug ermöglicht es authentifizierten Benutzern,**

**Teile des Dienstes zum Absturz zu bringen. Der Dienst wird für die Benutzer:innen transparent wiederhergestellt. Markieren Sie die richtige Strategie für das Risikomanagement.**

**Wählen Sie eine Antwort:**

**Risiko reduzieren, indem um jeden Preis eine Fehlerbehebung bereitgestellt wird**

**Risiko vermeiden, indem die Benutzerauthentifizierung deaktiviert wird**

**Risiko übertragen, indem eine Versicherung für Cyberangriffe abgeschlossen wird, die 1 % des aktuellen Jahresgewinns kostet**

**Risiko akzeptieren, da es keine wirklichen Auswirkungen auf die Organisation hat**

**Die richtige Antwort ist: Risiko akzeptieren, da es keine wirklichen Auswirkungen auf die Organisation hat**

**FRAGE 51 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 03**

**Welches der folgenden Elemente ist ein gültiges Element in einem Attack-Tree?**

**Wählen Sie eine Antwort:**

**Quelle**

**Knoten Datenfluss Akteur**

**Die richtige Antwort ist: Knoten**

**Welche Sicherheitseigenschaft sollte ein System laut STRIDE haben?**

**Wählen Sie eine Antwort:**

**Sauberkeit**

**Integrität Einfachheit Spoofing**

**Die richtige Antwort ist: Integrität**

**FRAGE 53 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 03**

**Welche Bedrohung ist in LINDDUN und in STRIDE die gleiche?**

**Wählen Sie eine Antwort:**

**Spoofing**

**Unkenntnis**

**Offenlegung von Informationen Verknüpfbarkeit**

**Die richtige Antwort ist: Offenlegung von Informationen**

**Ein Benutzer kann seine Benutzer-ID ändern, um sich als ein anderer Benutzer auszugeben. Welche**

**STRIDE-Bedrohung beschreibt dies?**

**Wählen Sie eine Antwort:**

**Offenlegung von Informationen**

**Verknüpfbarkeit Spoofing**

**Erweiterung der Berechtigungen**

**Die richtige Antwort ist: Spoofing**

**FRAGE 55 VON 78**

**DLMCSECRAM01\_E\_MC\_mittel/Lektion 03**

**Durch einen Bug in einer Software ist ein Benutzer in der Lage, die Daten anderer Benutzer:innen zu verändern.**

**Welche STRIDE-Bedrohung beschreibt dies?**

**Wählen Sie eine Antwort:**

**Denial-of-Service**

**Spoofing**

**Erweiterung der Berechtigungen Manipulation**

**Die richtige Antwort ist: Manipulation**

**FRAGE 56 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 03**

**Ein Knoten in einem Attack-Tree enthält die Bedrohung „sich als Mitarbeiter ausgeben“.**

**Was ist ein gültiger Unterknoten für diese Bedrohung?**

**Wählen Sie eine Antwort:**

**Überflutung des Servers mit Anfragen**

**Diebstahl einer Mitarbeiterkarte**

**Hinderung eines Mitarbeiters, zur Arbeit zu gehen Unaufgefordertes Anrufen bei dem Unternehmen als Lieferant**

**Die richtige Antwort ist: Diebstahl einer Mitarbeiterkarte**

**FRAGE 57 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 03**

**Was ist ein korrektes Datenflussdiagramm?**

**Wählen Sie eine Antwort:**

**Die richtige Antwort ist:**

**Welche NIST-Veröffentlichung stellt ein Risikomanagement-Framework bereit?**

**Wählen Sie eine Antwort:**

**Special Publication 300-80**

**Special Publication 100-03**

**Special Publication 420-69**

**Special Publication 800-37**

**Die richtige Antwort ist: Special Publication 800-37**

**FRAGE 59 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 04**

**Was ist die dritte Ebene des organisationsweiten Risikomanagements nach NIST?**

**Wählen Sie eine Antwort:**

**Projekt**

**Informationssystem Mission/Geschäftsprozess Organisation**

**Die richtige Antwort ist: Informationssystem**

**Was wird in BSI 100-3 beschrieben?**

**Wählen Sie eine Antwort:**

**Bedrohungsmanagement auf der Grundlage von IT-Grundschutz**

**Risikobewertung auf der Grundlage von IT-Grundschutz Risikomanagement auf der Grundlage von IT-Grundschutz**

**Threat Modeling auf der Grundlage von IT-Grundschutz**

**Die richtige Antwort ist: Risikobewertung auf der Grundlage von IT-Grundschutz**

**FRAGE 61 VON 78**

**DLMCSECRAM01\_E\_MC\_mittel/Lektion 04**

**Die folgende Minderungsmaßnahme wird definiert. Welcher Strategie kann diese nach**

**BSI zugeordnet werden?**

**Die IT-Infrastruktur wird in einem anderen Rechenzentrum in einem anderen Land dupliziert.**

**Wählen Sie eine Antwort:**

**Risikotransfer**

**Risikoakzeptanz**

**Risikominderung durch zusätzliche Sicherheitsmaßnahmen Risikovermeidung durch Umstrukturierung**

**Die richtige Antwort ist: Risikoreduzierung durch zusätzliche Sicherheitsmaßnahmen**

**Eine Organisation plant ihr Risikomanagement gemäß der ISO/IEC**

**27005. Derzeit wird der Geltungsbereich des Prozesses ermittelt. Welchem Schritt in ISO/IEC 27005 entspricht dies?**

**Wählen Sie eine Antwort:**

**Kontextermittlung**

**Risikobewertung Risikokommunikation Risikobehandlung**

**Die richtige Antwort ist: Kontextermittlung**

**FRAGE 63 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 04**

**In welche NIST-Risikomanagementkategorie kann die folgende Richtlinie eingeordnet**

**werden:**

**Organisationsweite Foren einrichten, um alle Arten und Quellen von Risiken zu berücksichtigen.**

**Wählen Sie eine Antwort:**

**Projekt**

**Organisation Mission/Geschäftsprozess Informationssystem**

**Die richtige Antwort ist: Organisation**

**FRAGE 64 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 04**

**In welche NIST-Risikomanagementkategorie kann die folgende Richtlinie eingeordnet**

**werden:**

**Zuweisung von Management-, Betriebs- und technischen Sicherheitsmaßnahmen zu Informationssystemen und Betriebsumgebungen, wie in der Informationssicherheitsarchitektur definiert.**

**Wählen Sie eine Antwort:**

**Informationssystem**

**Mission/Geschäftsprozess Organisation**

**Projekt**

**Die richtige Antwort ist: Mission/Geschäftsprozess**

**FRAGE 65 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 05**

**Was ist ein primäres Asset?**

**Wählen Sie eine Antwort:**

**Personal**

**Prozesse**

**Kryptografisches Material Geistiges Eigentum**

**Die richtige Antwort ist: Geistiges Eigentum**

**Welcher Diagrammtyp zeigt den logischen Ablauf einer Anwendung?**

**Wählen Sie eine Antwort:**

**Sequenzdiagramm**

**Klassendiagramm Datenflussdiagramm**

**Bereitstellungsdiagramm**

**Die richtige Antwort ist: Datenflussdiagramm**

**FRAGE 67 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 05**

**Wie können Black-Swan-Ereignisse gemindert werden?**

**Wählen Sie eine Antwort:**

**Das ist nicht möglich.**

**Abschluss einer Versicherung. Eintrittswahrscheinlichkeit verringern. Auswirkungen eindämmen.**

**Die richtige Antwort ist: Auswirkungen eindämmen.**

**Was sollte bei einer Risikobewertung stets getan werden?**

**Wählen Sie eine Antwort:**

**Mindestens ein kritisches Risiko finden**

**Auf menschliche böswillige Ereignisse konzentrieren Mindestens 5 Assets definieren**

**Bewertung dokumentieren**

**Die richtige Antwort ist: Bewertung dokumentieren**

**FRAGE 69 VON 78**

**DLMCSECRAM01\_E\_MC\_mittel/Lektion 05**

**Im Risikomanagementprozess kann ein Anforderungskatalog hilfreich sein. Bei**

**welchem Teil des Prozesses ist ein solcher Katalog am nützlichsten?**

**Wählen Sie eine Antwort:**

**Bewertungsvorbereitung**

**Threat Modeling Risikominderungsvorschlag**

**Dokumentation und Berichterstattung**

**Die richtige Antwort ist: Threat Modeling**

**FRAGE 70 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 05**

**Eine selbstentwickelte Webanwendung läuft in einer öffentlichen Cloud. Welche Bestandteile sollten**

**im Geltungsbereich liegen?**

**Wählen Sie eine Antwort:**

**Das Rechenzentrum**

**Der Browser des Benutzers**

**Die selbst entwickelten Teile**

**Das System, auf dem die Cloud läuft**

**Die richtige Antwort ist: Die selbst entwickelten Teile**

**FRAGE 71 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 05**

**In welcher Asset-Kategorie befindet sich der Systemadministrator?**

**Wählen Sie eine Antwort:**

**Geschäftliches Asset**

**Menschliches Asset Primäres Asset Unterstützende Assets**

**Die richtige Antwort ist: Unterstützende Assets**

**Was ist Resilience Engineering?**

**Wählen Sie eine Antwort:**

**Resilience Engineering ist die Planung des Incident-Response-Prozesses.**

**Resilience Engineering ist die Implementierung von Sicherheitslösungen in bestehende Systeme. Resilience Engineering ist das Threat Modeling für jede Anwendung.**

**Resilience Engineering ist der Entwurf und die Implementierung von Systemen mit einem Schwerpunkt auf Sicherheit.**

**Die richtige Antwort ist: Resilience Engineering ist der Entwurf und die Implementierung von Systemen mit einem Schwerpunkt auf Sicherheit.**

**FRAGE 73 VON 78**

**DLMCSECRAM01\_E\_MC\_leicht/Lektion 06**

**Was ist das Ziel eines IDS?**

**Wählen Sie eine Antwort:**

**Alle Sicherheitsereignisse zu korrelieren und zu protokollieren**

**Fehlverhalten von Mitarbeitenden zu erkennen Eingehenden Netzwerkverkehr zu blockieren**

**Eindringlinge in das Netzwerk zu erkennen**

**Die richtige Antwort ist: Eindringlinge in das Netzwerk zu erkennen**

**Was sollte für eine sinnvolle Risikomanagementrichtlinie definiert werden?**

**Wählen Sie eine Antwort:**

**Risikohunger**

**Risikofreiheit Risikointegrität Risikobereitschaft**

**Die richtige Antwort ist: Risikobereitschaft**

**FRAGE 75 VON 78**

**DLMCSECRAM01\_E\_MC\_mittel/Lektion 06**

**Was sollte Bestandteil einer Risikomanagementschulung sein?**

**Wählen Sie eine Antwort:**

**Risiken präsentieren**

**Sicherheitsüberprüfungen durchführen Sicheren Code schreiben**

**Entwickler:innen managen**

**Die richtige Antwort ist: Sicherheitsüberprüfungen durchführen**

**In die neuen Systeme wird eine sinnvolle Infrastruktur für die Protokollierung implementiert. Welche Art von**

**Maßnahme ist dies im Resilience-Engineering-Prozess?**

**Wählen Sie eine Antwort:**

**Schutzmaßnahme**

**Erkennungsmaßnahme Widerstandsmaßnahme Kompensationsmaßnahme**

**Die richtige Antwort ist: Erkennungsmaßnahme**

**FRAGE 77 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 06**

**Was ist der Grund für den Abschluss einer Cyber-Versicherung?**

**Wählen Sie eine Antwort:**

**Ein Häkchen auf der HIPAA-Checkliste zu machen**

**Vervollständigung der bestehenden Cybersicherheitsstrategie**

**Verlagerung der Notwendigkeit der Implementierung von Sicherheitsmaßnahmen Erhalt eines Freifahrtscheins**

**Die richtige Antwort ist: Vervollständigung der bestehenden Cybersicherheitsstrategie**

**FRAGE 78 VON 78**

**DLMCSECRAM01\_E\_MC\_schwer/Lektion 06**

**In einer Organisation findet eine Präsentation statt, in der über Änderungen in der**

**Software informiert wird, um eine Schwachstelle zu mindern. In welchem Schritt des Vorfallsprozesses wird dies normalerweise getan?**

**Wählen Sie eine Antwort:**

**Technische Vorbereitung**

**Organisatorische Vorbereitung Behandlung**

**Nachbearbeitung**

**Die richtige Antwort ist: Nachbearbeitung**