Musterprüfung

Ausgabe 202607

Inhalt

Einführung

Dies ist die EXIN Information Security Essentials based on ISO/IEC 27001 (ISE.DE) Musterprüfung. Es gilt die Prüfungsordnung von EXIN.

Die Musterprüfung besteht aus 20 Multiple-Choice-Fragen. Zu jeder Multiple-Choice-Frage werden mehrere Antwortmöglichkeiten angeboten. Es gibt jeweils eine richtige Antwort.

Sie können maximal 20 Punkte erreichen. Jede richtige Antwort zählt 1 Punkt. Um die Prüfung zu bestehen, müssen Sie mindestens 13 Punkte erzielen.

Die Bearbeitungszeit beträgt 30 Minuten.

Viel Erfolg!

Musterprüfung

1 / 20
Was ist der Fokus des Informationsmanagements?

A) Die unterbrechungsfreie Fortführung von Business-Aktivitäten und -Prozessen zu ermöglichen
B) Die Identifizierung und Nutzung des Werts von Informationen sicherzustellen
C) Den Zugriff auf automatisierte Systeme durch Unbefugte zu verhindern
D) Die Informationsflüsse im Unternehmen zu verstehen

2 / 20
Was ist neben Integrität und Vertraulichkeit der dritte Aspekt der Zuverlässigkeit von Informationen?

A) Genauigkeit
B) Verfügbarkeit
C) Vollständigkeit
D) Monetärer Wert

3 / 20
Eine Organisation verfügt über einen Netzwerkdrucker, der im Flur des Unternehmens steht. Viele Mitarbeiter holen ihre Ausdrucke nicht sofort, sondern lassen sie im Drucker liegen.

Wie wirkt sich dies auf die Zuverlässigkeit der Informationen aus?

A) Die Verfügbarkeit der Informationen ist nicht mehr gewährleistet.
B) Die Vertraulichkeit der Informationen ist nicht mehr gewährleistet.
C) Die Integrität der Informationen ist nicht mehr gewährleistet.

4 / 20
Wie lässt sich der Zweck einer Informationssicherheitsrichtlinie **am besten** beschreiben?

A) Eine Informationssicherheitsrichtlinie dokumentiert die Analyse der Risiken und die Suche nach entsprechenden Sicherheitsmaßnahmen.
B) Eine Informationssicherheitsrichtlinie bietet der Organisation Orientierung und Unterstützung hinsichtlich der Informationssicherheit.
C) Eine Informationssicherheitsrichtlinie konkretisiert die Sicherheitsplanung mit den erforderlichen Details.
D) Eine Informationssicherheitsrichtlinie bieten Einblick in Bedrohungen und deren mögliche Folgen.

5 / 20
Sara soll sicherstellen, dass ihre Organisation die Gesetzgebung zum Schutz personenbezogener Daten einhält.

Was sollte Sara **zuerst** tun?

A) Einen Mitarbeiter benennen, der die Manager bei der Einhaltung der Richtlinie unterstützt
B) Die Erhebung und Speicherung personenbezogener Daten verbieten
C) Die Mitarbeitenden für die Übermittlung ihrer personenbezogenen Daten zuständig machen
D) Die Gesetzgebung zum Schutz personenbezogener Daten in einer Datenschutzrichtlinie umsetzen.

6 / 20
Wer ist dafür zuständig, aus der Unternehmensstrategie und den Unternehmenszielen eine Sicherheitsstrategie und Sicherheitsziele abzuleiten?

A) Chief Information Security Officer (CISO)
B) Geschäftsführung
C) Information Security Officer (ISO)
D) Information Security Policy Officer

7 / 20
Welches ist das **beste** Beispiel einer menschlichen Bedrohung?

A) Ein Leck verursacht einen Stromausfall.
B) Ein USB-Stick infiziert ein Netzwerk mit einem Virus.
C) Der Server-Raum ist zu staubig.

8 / 20
In einem Unternehmen gab es einen Brand. Die Feuerwehr war schnell vor Ort und konnte den Brand löschen, bevor er sich ausbreitete und das gesamte Firmengelände abbrannte. Bei dem Brand wurde jedoch der Server zerstört. Die in einem anderen Raum aufbewahrten Backup-Bänder waren geschmolzen und viele weitere Dokumente gingen verloren.

Welchen **indirekten** Schaden hat der Brand verursacht?

A) Verbrannte Computer-Systeme
B) Verbrannte Dokumente
C) Geschmolzene Backup-Bänder
D) Wasserschaden

9 / 20
Die Risikostrategien von Unternehmen können sich je nach Art der Geschäftstätigkeit unterscheiden.

Welche Risikostrategie eignet sich für ein Krankenhaus **am besten**?

A) Risikoakzeptanz
B) Risikovermeidung
C) Risikotragfähigkeit
D) Risikoneutralität

10 / 20
Eine professionell durchgeführte Risikoanalyse bietet viele nützliche Informationen. Eine Risikoanalyse verfolgt mehrere Hauptziele.

Was zählt **nicht** zu den Hauptzielen einer Risikoanalyse?

A) Die Kosten eines Incidents und die Kosten einer Sicherheitsmaßnahme gegeneinander abzuwägen
B) Die relevanten Schwachstellen und Bedrohungen zu bestimmen
C) Die Werte (Assets) und deren wirtschaftlichen Wert zu identifizieren
D) Die Maßnahmen (Measures) und Sicherheitsmaßnahmen zu implementieren

11 / 20
Was ist das Ziel der Klassifizierung von Informationen?

A) Die Kennzeichnung von Informationen, um ihre Erkennbarkeit zu verbessern
B) Die Erstellung eines Handbuchs zum Umgang mit Mobilgeräten
C) Die Gliederung der Informationen nach dem Grad ihrer Vertraulichkeit

12 / 20
Was ist der **wichtigste** Grund für die Trennung der Verantwortlichkeit?

A) Sicherzustellen, dass Mitarbeiter nicht zur gleichen Zeit das Gleiche machen
B) Alle Mitarbeiter gemeinsam für die gemachten Fehler zuständig zu machen
C) Klarzustellen, wer für welche Aufgaben und Tätigkeiten zuständig ist
D) Die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Änderungen auf ein Minimum zu beschränken

13 / 20
In der Geschäftsstelle einer Organisation bricht ein Brand aus. Die Mitarbeiter werden auf andere Geschäftsstellen in der Nähe verteilt und sollen dort weiter arbeiten.

Wo ist eine solche Stand-by-Regelung im Lebenszyklus der Incidents (Incident Cycle) angesiedelt?

A) Zwischen Schaden und Wiederherstellung
B) Zwischen Incident und Schaden
C) Zwischen Wiederherstellung und Bedrohung
D) Zwischen Bedrohung und Incident

14 / 20
Ein Mitarbeiter entdeckt einen Incident.

An wen sollte er diesen **zuerst** melden?

A) An den Helpdesk
B) An den Information Security Manager (ISM)
C) An den Information Security Officer (ISO)
D) An den Vorgesetzten

15 / 20
Welche physische Sicherheitsmaßnahme regelt den Zugriff auf die Informationen einer Organisation?

A) Installation einer Klimaanlage
B) Verbot der Nutzung von USB-Sticks
C) Erfordernis von Benutzernamen und Passwort
D) Verwendung von Sicherheitsglas

16 / 20
Welche Sicherheitsmaßnahme für einen Wert (Asset) erforderlich ist, richtet sich nach dem jeweiligen Wert (Asset).

Wie lässt sich die Sicherheit eines Werts **am besten** gewährleisten?

A) Indem man ein Formular sichert durch ausfüllen und abzeichnen
B) Indem man einen Laptop sichert und diesen einem einzigen Benutzer zuweist
C) Indem man einen USB-Stick mittels Verschlüsselung sichert
D) Indem man eine Internetverbindung mittels Backup sichert

17 / 20
Eine Organisation ändert ihre Richtlinie. Ab sofort haben die Mitarbeitenden auch die Möglichkeit zu Remote- oder Telearbeit.

Welche Sicherheitsmaßnahme sollte nun eingeführt werden?

A) Erstellen von V-Lans zur Segmentierung des Unternehmensnetzwerks
B) Verschlüsselung der Informationen im Unternehmensnetzwerk
C) Einrichtung von Firewalls im Unternehmensnetzwerk
D) Verbindung mit dem Unternehmensnetzwerk über virtuelles privates Netzwerk (VPN)

18 / 20
Die Mitarbeitenden einer Organisation arbeiten an Laptops, die mittels asymmetrischer Kryptographie geschützt sind. Um die Schlüsselverwaltung so wirtschaftlich wie möglich zu gestalten, nutzen alle Berater das selbe Schlüsselpaar.

Bei Gefährdung bestimmter Informationen sind neue Schlüssel bereitzustellen.

In welchem Fall sollten neue Schlüssel bereitgestellt werden?

A) Wenn der private Schlüssel bekannt wird
B) Wenn der öffentliche Schlüssel bekannt wird
C) Wenn die Infrastruktur mit öffentlichem Schlüssel (PKI) bekannt wird

19 / 20
Bei welcher Art von Schadsoftware handelt es sich um ein Programm, das neben seiner offensichtlichen Funktion auch bewusst weitere Aktivitäten ausführt?

A) Logikbombe (Logic Bomb)
B) Spyware
C) Trojaner
D) Wurm

20 / 20
Welche Gesetzgebung oder Rechtsvorschrift im Bereich der Informationssicherheit gilt für alle Organisationen?

A) Datenschutz-Grundverordnung (DSGVO)
B) Geistige Eigentumsrechte
C) ISO/IEC 27001
D) ISO/IEC 27002

Antwortschlüssel

1 / 20
Was ist der Fokus des Informationsmanagements?

A) Die unterbrechungsfreie Fortführung von Business-Aktivitäten und -Prozessen zu ermöglichen
B) Die Identifizierung und Nutzung des Werts von Informationen sicherzustellen
C) Den Zugriff auf automatisierte Systeme durch Unbefugte zu verhindern
D) Die Informationsflüsse im Unternehmen zu verstehen

A) Falsch. Das ist der Fokus des Business Continuity Management (BCM). Ziel des BCM ist, die Störung von Business-Aktivitäten zu vermeiden, wichtige Prozesse vor den Konsequenzen weitreichender Störungen in Informationssystemen zu schützen und eine schnelle Wiederherstellung zu ermöglichen.
B) Richtig. Das Informationsmanagement beschreibt, wie eine Organisation ihre Informationen effizient plant, erhebt, organisiert, nutzt, kontrolliert, verbreitet und entsorgt und wie die Organisation dafür sorgt, dass der Wert von Informationen identifiziert und möglichst vollumfänglich genutzt wird. (Literatur: A, Kapitel 4.9)
C) Falsch. Dies ist der Fokus des Zugangs- und Zugriffsmanagements. Dieses stellt sicher, dass unbefugte Personen oder Prozesse nicht auf automatisierte Systeme, Datenbanken und Programme zugreifen können.
D) Falsch. Dies ist der Fokus der Informationsanalyse. Sie zeichnet ein klares Bild, wie die Organisation mit Informationen umgeht und wie die Informationsflüsse im Unternehmen verlaufen.

2 / 20
Was ist neben Integrität und Vertraulichkeit der dritte Aspekt der Zuverlässigkeit von Informationen?

A) Genauigkeit
B) Verfügbarkeit
C) Vollständigkeit
D) Monetärer Wert

A) Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. Genauigkeit ist Teil der Integrität.
B) Richtig. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. (Literatur: A, Kapitel 3.4.3)
C) Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. Vollständigkeit ist Teil der Integrität.
D) Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit.

3 / 20
Eine Organisation verfügt über einen Netzwerkdrucker, der im Flur des Unternehmens steht. Viele Mitarbeiter holen ihre Ausdrucke nicht sofort, sondern lassen sie im Drucker liegen.

Wie wirkt sich dies auf die Zuverlässigkeit der Informationen aus?

A) Die Verfügbarkeit der Informationen ist nicht mehr gewährleistet.
B) Die Vertraulichkeit der Informationen ist nicht mehr gewährleistet.
C) Die Integrität der Informationen ist nicht mehr gewährleistet.

A) Falsch. Die Informationen sind in dem System, in dem sie erstellt und gedruckt wurden, nach wie vor verfügbar.
B) Richtig. Die Informationen können in die Hände von Personen fallen oder von Personen gelesen werden, die keinen Zugriff auf diese Informationen haben sollten. (Literatur: A, Kapitel 3.4.1)
C) Falsch. Die Informationen sind auf Papier gedruckt, sodass ihre Integrität nach wie vor gewährleistet ist.

4 / 20
Wie lässt sich der Zweck einer Informationssicherheitsrichtlinie **am besten** beschreiben?

A) Eine Informationssicherheitsrichtlinie dokumentiert die Analyse der Risiken und die Suche nach entsprechenden Sicherheitsmaßnahmen.
B) Eine Informationssicherheitsrichtlinie bietet der Organisation Orientierung und Unterstützung hinsichtlich der Informationssicherheit.
C) Eine Informationssicherheitsrichtlinie konkretisiert die Sicherheitsplanung mit den erforderlichen Details.
D) Eine Informationssicherheitsrichtlinie bieten Einblick in Bedrohungen und deren mögliche Folgen.

A) Falsch. Die Analyse der Risiken und die Suche nach Sicherheitsmaßnahmen sind der Zweck der Risikoanalyse und des Risikomanagements.
B) Richtig. Die Geschäftsführung bietet durch ihre Sicherheitsrichtlinie Orientierung und Unterstützung hinsichtlich der Informationssicherheit. (Literatur: A, Kapitel 4.2.1)
C) Falsch. Die Sicherheitsplanung konkretisiert die Informationssicherheitsrichtlinie. Die Planung enthält die gewählten Sicherheitsmaßnahmen, wer für was zuständig ist sowie die Leitlinien zur Umsetzung der Sicherheitsmaßnahmen etc.
D) Falsch. Einblick in Bedrohungen und deren mögliche Folgen ist der Zweck der Bedrohungsanalyse.

5 / 20
Sara soll sicherstellen, dass ihre Organisation die Gesetzgebung zum Schutz personenbezogener Daten einhält.

Was sollte Sara **zuerst** tun?

A) Einen Mitarbeiter benennen, der die Manager bei der Einhaltung der Richtlinie unterstützt
B) Die Erhebung und Speicherung personenbezogener Daten verbieten
C) Die Mitarbeitenden für die Übermittlung ihrer personenbezogenen Daten zuständig machen
D) Die Gesetzgebung zum Schutz personenbezogener Daten in einer Datenschutzrichtlinie umsetzen.

A) Falsch. Ein Mitarbeiter, der die Manager unterstützt, ist für die Einhaltung der Gesetzgebung zum Schutz personenbezogener Daten nicht gefordert. Darüber hinaus sollte die Richtlinie zuerst an die Gesetzgebung angepasst werden.
B) Falsch. Dies ist nicht der beste Weg, um die Gesetzgebung zum Schutz personenbezogener Daten einzuhalten.
C) Falsch. So sorgt man nicht für die Einhaltung der Gesetzgebung zum Schutz personenbezogener Daten.
D) Richtig. Der erste Schritt zur Einhaltung der Gesetzgebung ist die Erstellung einer internen Richtlinie für die Organisation. (Literatur: A, Kapitel 5.1)

6 / 20
Wer ist dafür zuständig, aus der Unternehmensstrategie und den Unternehmenszielen eine Sicherheitsstrategie und Sicherheitsziele abzuleiten?

A) Chief Information Security Officer (CISO)
B) Geschäftsführung
C) Information Security Officer (ISO)
D) Information Security Policy Officer

A) Richtig. Der CISO berichtet an die oberste Geschäftsführung und erarbeitet die allgemeine Sicherheitsstrategie für das gesamte Unternehmen. (Literatur: A, Kapitel 5.2)
B) Falsch. Die Geschäftsführung legt die Unternehmensstrategie fest, auf deren Grundlage der CISO dann die allgemeine Sicherheitsstrategie festlegt.
C) Falsch. Der ISO erarbeitet ausgehend von der Unternehmensrichtlinie die Informationssicherheitsrichtlinie einer Geschäftseinheit und stellt sicher, dass diese eingehalten wird.
D) Falsch. Der Information Security Policy Officer ist für die Pflege der von der Sicherheitsstrategie abgeleiteten Informationssicherheitsrichtlinie zuständig.

7 / 20
Welches ist das **beste** Beispiel einer menschlichen Bedrohung?

A) Ein Leck verursacht einen Stromausfall.
B) Ein USB-Stick infiziert ein Netzwerk mit einem Virus.
C) Der Server-Raum ist zu staubig.

A) Falsch. Ein Leck ist keine menschliche, sondern eine nicht-menschliche Bedrohung.
B) Richtig. Ein USB-Stick wird immer von einem Menschen eingesteckt. Infiziert der USB-Stick das Netzwerk mit einem Virus, handelt es sich um eine menschliche Bedrohung. (Literatur: A, Kapitel 3.9.1)
C) Falsch. Staub ist keine menschliche, sondern eine nicht-menschliche Bedrohung.

8 / 20
In einem Unternehmen gab es einen Brand. Die Feuerwehr war schnell vor Ort und konnte den Brand löschen, bevor er sich ausbreitete und das gesamte Firmengelände abbrannte. Bei dem Brand wurde jedoch der Server zerstört. Die in einem anderen Raum aufbewahrten Backup-Bänder waren geschmolzen und viele weitere Dokumente gingen verloren.

Welchen **indirekten** Schaden hat der Brand verursacht?

A) Verbrannte Computer-Systeme
B) Verbrannte Dokumente
C) Geschmolzene Backup-Bänder
D) Wasserschaden

A) Falsch. Verbrannte Computer-Systeme sind ein direkter Schaden des Brands.
B) Falsch. Verbrannte Dokumente sind ein direkter Schaden des Brands.
C) Falsch. Geschmolzene Backup-Bänder sind ein direkter Schaden des Brands.
D) Richtig. Der durch die Brandlöschung verursachte Wasserschaden ist ein indirekter Schaden des Brands. Er ist eine Nebenwirkung der Löschmaßnahmen, die darauf ausgerichtet waren, die Brandschäden zu minimieren. (Literatur: A, Kapitel 3.10)

9 / 20
Die Risikostrategien von Unternehmen können sich je nach Art der Geschäftstätigkeit unterscheiden.

Welche Risikostrategie eignet sich für ein Krankenhaus **am besten**?

A) Risikoakzeptanz
B) Risikovermeidung
C) Risikotragfähigkeit
D) Risikoneutralität

A) Falsch. Ein Krankenhaus kann Risiken in Form von finanziellen Verlusten oder sterbenden Patienten nicht einfach akzeptieren.
B) Richtig. Krankenhäuser sollten versuchen, Risiken zu vermeiden. (Literatur: A, Kapitel 3.11)
C) Falsch. Risikotragfähigkeit bedeutet, dass bestimmte Risiken akzeptiert werden, beispielsweise wenn die Kosten für Sicherheitsmaßnahmen die Kosten möglicher Schäden übersteigen. Für ein Krankenhaus ist dies nicht die beste Art und Weise, um mit Risiken umzugehen.
D) Falsch. Risikoneutralität bedeutet, dass Maßnahmen (Measures) ergriffen werden, damit sich die Bedrohungen entweder nicht mehr manifestieren oder, falls sie es doch tun, der daraus resultierende Schaden auf ein Minimum begrenzt wird. Da Schaden bei Patienten immer schlecht ist, sollten Krankenhäuser sich für die Risikovermeidung entscheiden.

10 / 20
Eine professionell durchgeführte Risikoanalyse bietet viele nützliche Informationen. Eine Risikoanalyse verfolgt mehrere Hauptziele.

Was zählt **nicht** zu den Hauptzielen einer Risikoanalyse?

A) Die Kosten eines Incidents und die Kosten einer Sicherheitsmaßnahme gegeneinander abzuwägen
B) Die relevanten Schwachstellen und Bedrohungen zu bestimmen
C) Die Werte (Assets) und deren wirtschaftlichen Wert zu identifizieren
D) Die Maßnahmen (Measures) und Sicherheitsmaßnahmen zu implementieren

A) Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
B) Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
C) Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
D) Richtig. Das ist kein Ziel der Risikoanalyse. (Literatur: A, Kapitel 3.7)

11 / 20
Was ist das Ziel der Klassifizierung von Informationen?

A) Die Kennzeichnung von Informationen, um ihre Erkennbarkeit zu verbessern
B) Die Erstellung eines Handbuchs zum Umgang mit Mobilgeräten
C) Die Gliederung der Informationen nach dem Grad ihrer Vertraulichkeit

A) Falsch. Die Kennzeichnung von Informationen ist eine besondere Form der Kategorisierung von Informationen, die nach deren Klassifizierung erfolgt.
B) Falsch. Die Erstellung eines Handbuchs bezieht sich auf die Benutzerrichtlinien. Hierbei handelt es sich nicht um die Klassifizierung von Informationen.
C) Richtig. Bei der Klassifizierung von Informationen werden verschiedene Vertraulichkeitsstufen festgelegt, sodass die Informationen dann entsprechend eingeteilt werden können. (Literatur: A, Kapitel 5.12)

12 / 20
Was ist der **wichtigste** Grund für die Trennung der Verantwortlichkeit?

A) Sicherzustellen, dass Mitarbeiter nicht zur gleichen Zeit das Gleiche machen
B) Alle Mitarbeiter gemeinsam für die gemachten Fehler zuständig zu machen
C) Klarzustellen, wer für welche Aufgaben und Tätigkeiten zuständig ist
D) Die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Änderungen auf ein Minimum zu beschränken

A) Falsch. Die Trennung der Verantwortlichkeit soll unbefugte oder unbeabsichtigte Änderungen und den Missbrauch von Werten (Assets) der Organisation verhindern. Sie legt nicht fest, wann diese Tätigkeiten durchzuführen sind.
B) Falsch. Die Trennung der Verantwortlichkeit trennt Aufgaben und Zuständigkeiten. Sie sorgt nicht für die gemeinsame Verantwortung einer Gruppe von Menschen.
C) Falsch. Die Trennung der Verantwortlichkeiten soll unbefugte oder unbeabsichtigte Änderungen und den Missbrauch von Werten (Assets) der Organisation verhindern. Sie soll nicht klarstellen, wer für was zuständig ist.
D) Richtig. Verantwortlichkeiten müssen getrennt werden, um unbefugte oder unbeabsichtigte Änderungen und den Missbrauch von Werten (Assets) der Organisation zu verhindern. (Literatur: A, Kapitel 5.3)

13 / 20
In der Geschäftsstelle einer Organisation bricht ein Brand aus. Die Mitarbeiter werden auf andere Geschäftsstellen in der Nähe verteilt und sollen dort weiter arbeiten.

Wo ist eine solche Stand-by-Regelung im Lebenszyklus der Incidents (Incident Cycle) angesiedelt?

A) Zwischen Schaden und Wiederherstellung
B) Zwischen Incident und Schaden
C) Zwischen Wiederherstellung und Bedrohung
D) Zwischen Bedrohung und Incident

A) Falsch. Schaden und Wiederherstellung werden durch die Stand-by-Regelung begrenzt.
B) Richtig. Die Stand-by-Regelung ist eine unterdrückende Maßnahme (Measure), um den Schaden zu begrenzen. (Literatur: A., Kapitel 3.8.4)
C) Falsch. Die Wiederherstellung erfolgt erst nachdem die Stand-by-Regelung in die Tat umgesetzt wurde.
D) Falsch. Eine Stand-by-Regelung zu realisieren, ohne dass ein Incident vorliegt, wäre sehr kostspielig.

14 / 20
Ein Mitarbeiter entdeckt einen Incident.

An wen sollte er diesen **zuerst** melden?

A) An den Helpdesk
B) An den Information Security Manager (ISM)
C) An den Information Security Officer (ISO)
D) An den Vorgesetzten

A) Richtig. Normalerweise sollten Incidents zur Bewertung, Einleitung von Sofortmaßnahmen und gegebenenfalls Eskalation zuerst an den Helpdesk gemeldet werden. Incidents sollten nicht sofort vertikal eskaliert werden. (Literatur: A, Kapitel 6.8)
B) Falsch. Incidents sollten nicht sofort vertikal eskaliert werden. Außerdem ist nicht jeder Incident ein Sicherheitsincident. Daher sollte der Incident zuerst vom Helpdesk geprüft werden, um festzustellen, ob es sich um einen Sicherheitsincident handelt.
C) Falsch. Incidents sollten nicht sofort vertikal eskaliert werden. Außerdem ist nicht jeder Incident ein Sicherheitsincident. Daher sollte der Incident zuerst vom Helpdesk geprüft werden, um festzustellen, ob es sich um einen Sicherheitsincident handelt.
D) Falsch. Incidents sollten nicht sofort vertikal eskaliert werden.

15 / 20
Welche physische Sicherheitsmaßnahme regelt den Zugriff auf die Informationen einer Organisation?

A) Installation einer Klimaanlage
B) Verbot der Nutzung von USB-Sticks
C) Erfordernis von Benutzernamen und Passwort
D) Verwendung von Sicherheitsglas

A) Falsch. Klimaanlagen haben nichts mit der Regelung des Zugriffs auf die Informationen einer Organisation zu tun.
B) Falsch. Dies ist eine organisatorische Sicherheitsmaßnahme.
C) Falsch. Dies ist eine technische Sicherheitsmaßnahme.
D) Richtig. Die Verwendung von Sicherheitsglas ist ein Beispiel für eine physische Sicherheitsmaßnahme, um Unbefugten den Zutritt zu einem Gebäude zu verwehren. (Literatur: A, Kapitel 7.4)

16 / 20
Welche Sicherheitsmaßnahme für einen Wert (Asset) erforderlich ist, richtet sich nach dem jeweiligen Wert (Asset).

Wie lässt sich die Sicherheit eines Werts **am besten** gewährleisten?

A) Indem man ein Formular sichert durch ausfüllen und abzeichnen
B) Indem man einen Laptop sichert und diesen einem einzigen Benutzer zuweist
C) Indem man einen USB-Stick mittels Verschlüsselung sichert
D) Indem man eine Internetverbindung mittels Backup sichert

A) Falsch. Ein Stück Papier mit Informationen abzulegen ist keine angemessene Sicherheitsmaßnahme.
B) Falsch. Zwar ist es eindeutig besser, wenn ein Laptop nur von einer einzigen Person benutzt wird, aber das ist nicht die beste Lösung. Die Verwaltung von Benutzerkonten und Password-Kontrollen sind bessere Sicherheitsmaßnahmen.
C) Richtig. Verschlüsselung stellt für einen USB-Stick eine valide Sicherheitsmaßnahme dar. Viele Organisationen nutzen diese Sicherheitsmaßnahme unabhängig von der Klassifizierung der auf dem USB-Stick gespeicherten Informationen. (Literatur: A, Kapitel 8.12)
D) Falsch. Ein Backup zu nutzen ist nicht die beste direkte Lösung, um eine Internetverbindung zu sichern.

17 / 20
Eine Organisation ändert ihre Richtlinie. Ab sofort haben die Mitarbeitenden auch die Möglichkeit zu Remote- oder Telearbeit.

Welche Sicherheitsmaßnahme sollte nun eingeführt werden?

A) Erstellen von V-Lans zur Segmentierung des Unternehmensnetzwerks
B) Verschlüsselung der Informationen im Unternehmensnetzwerk
C) Einrichtung von Firewalls im Unternehmensnetzwerk
D) Verbindung mit dem Unternehmensnetzwerk über virtuelles privates Netzwerk (VPN)

A) Falsch. Die Segmentierung der Netzwerke zur Gewährleistung der Vertraulichkeit und die Trennung der Verantwortlichkeit sollten bereits eingeführt worden sein. Diese beiden Sicherheitsmaßnahmen gelten nicht speziell für die Umstellung der Richtlinie auf Remote- oder Telearbeit.
B) Falsch. Zwar ist Verschlüsselung zum Schutz von Informationen unabdingbar, sie gilt aber nicht speziell dafür, Mitarbeitenden Remote- oder Telearbeit zu ermöglichen.
C) Falsch. Firewalls zwischen dem Unternehmensnetzwerk und der Außenwelt sind zwar wichtig, sollten aber bereits bestehen. Außerdem dienen Firewalls nicht direkt der Sicherung von Remote- oder Televerbindungen.
D) Richtig. Die Nutzung von VPN ist eine Sicherheitsmaßnahme, die ergriffen werden sollte, um Mitarbeitenden Remote- oder Telearbeit zu ermöglichen. (Literatur: A, Kapitel 8.2)

18 / 20
Die Mitarbeitenden einer Organisation arbeiten an Laptops, die mittels asymmetrischer Kryptographie geschützt sind. Um die Schlüsselverwaltung so wirtschaftlich wie möglich zu gestalten, nutzen alle Berater das selbe Schlüsselpaar.

Bei Gefährdung bestimmter Informationen sind neue Schlüssel bereitzustellen.

In welchem Fall sollten neue Schlüssel bereitgestellt werden?

A) Wenn der private Schlüssel bekannt wird
B) Wenn der öffentliche Schlüssel bekannt wird
C) Wenn die Infrastruktur mit öffentlichem Schlüssel (PKI) bekannt wird

A) Richtig. Bei der asymmetrischen Kryptographie ist es wichtig, den privaten Schlüssel geheim zuhalten. Der öffentliche Schlüssel darf bekannt werden. (Literatur: A, Kapitel 8.24.5)
B) Falsch. Der öffentliche Schlüssel darf auf der ganzen Welt bekannt sein. Der private Schlüssel muss geheim gehalten werden, um Integrität und Verfügbarkeit sicherzustellen.
C) Falsch. Die PKI wird genutzt, um die Schlüssel für asymmetrische Verschlüsselungssysteme auszutauschen.

19 / 20
Bei welcher Art von Schadsoftware handelt es sich um ein Programm, das neben seiner offensichtlichen Funktion auch bewusst weitere Aktivitäten ausführt?

A) Logikbombe (Logic Bomb)
B) Spyware
C) Trojaner
D) Wurm

A) Falsch. Eine Logikbombe ist ein Stück Code, das in ein Softwaresystem eingeschleust wird. Treten bestimmte Bedingungen ein, führt der Code eine Funktion aus. Dabei werden nicht immer bösartige Absichten verfolgt. Eine Logikbombe führt nicht immer sekundäre Aktivitäten aus.
B) Falsch. Spyware ist ein Computer-Programm, das Informationen über den Benutzer des Computers sammelt und diese an eine andere Partei schickt.
C) Richtig. Ein Trojaner ist ein Programm, das neben seiner eigentlichen Funktion, absichtlich und vom Computer-Benutzer unbemerkt, weitere Aktivitäten ausführt, die der Integrität des infizierten Systems schaden können. (Literatur: A, Kapitel 8.7.2)
D) Falsch. Ein Wurm erstellt ein Netzwerk aus infizierten Computern, indem er sich selbst repliziert.

20 / 20
Welche Gesetzgebung oder Rechtsvorschrift im Bereich der Informationssicherheit gilt für alle Organisationen?

A) Datenschutz-Grundverordnung (DSGVO)
B) Geistige Eigentumsrechte
C) ISO/IEC 27001
D) ISO/IEC 27002

A) Richtig. Alle Organisationen sollten über eine Richtlinie und über Verfahren zum Schutz personenbezogener Daten verfügen. Alle Mitarbeiter, die personenbezogene Daten verarbeiten, sollten diese Richtlinie und die Verfahren kennen. (Literatur: A, Kapitel 5.33)
B) Falsch. Diese Vorschrift hat nichts mit der Informationssicherheit von Organisationen zu tun.
C) Falsch. Hierbei handelt es sich um eine Norm, die Organisationen einen Leitfaden für die Einführung von Informationssicherheitsprozessen an die Hand gibt.
D) Falsch. Diese Norm mit dem Titel ‚Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmaßnahmen' enthält Leitlinien zur Informationssicherheitsrichtlinie und zu Sicherheitsmaßnahmen.

Beurteilung

Die richtigen Antworten auf die Fragen in dieser Musterprüfung finden Sie in nachstehender Tabelle.

Frage	Antwort	Frage	Antwort
1	B	**11**	C
2	B	**12**	D
3	B	**13**	B
4	B	**14**	A
5	D	**15**	D
6	A	**16**	C
7	B	**17**	D
8	D	**18**	A
9	B	**19**	C
10	D	**20**	A

Certified for what's next

Kontakt EXIN

www.exin.com