EC Council Certified Chief Information Security Officer (CCISO) (German Version)

1. Welcher der folgenden ist der BESTE Indikator für ein erfolgreiches Projekt?

A. Es liegt bei oder unter den im Basisbudget geplanten Ausgaben

B. Es erfüllt die meisten Spezifikationen, die in der genehmigten Projektdefinition aufgeführt sind

C. Die Ergebnisse werden von den wichtigsten Stakeholdern akzeptiert

D. Es wird im Vergleich zum Basisprojektplan termingerecht oder früher abgeschlossen

Answer(s): C

---

2. Szenario: Ihre Organisation verwendet Single Sign-On (nur Benutzername und Kennwort), um Ihren Mitarbeitern den Zugriff auf Organisationssysteme und -daten zu erleichtern. Die Berechtigung zu einzelnen Systemen und Datenbanken wird von Vorgesetzten und Dateneigentümern geprüft und genehmigt, um sicherzustellen, dass nur zugelassenes Personal bestimmte Anwendungen verwenden oder Informationen abrufen kann. Alle Mitarbeiter haben Zugriff auf ihre eigenen Personalinformationen, einschließlich der Möglichkeit, ihre Bankverbindung und Kontoinformationen sowie andere persönliche Daten über die Employee Self-Service-Anwendung zu ändern. Alle Mitarbeiter haben Zugriff auf das Organisations-VPN.

A. Professionelle Benutzerschulung zu Phishing, durchgeführt von einem angesehenen Anbieter

B. Mehrfaktor-Authentifizierung unter Verwendung von Hardtoken

C. Passwortänderungen alle 90 Tage erzwingen

D. Verringerung der Anzahl der Mitarbeiter mit Administratorrechten

Answer(s): B

3. Szenario: Ihre Unternehmenssysteme werden seit mehr als einer Woche ständig von fremden IP-Adressen untersucht und angegriffen. Ihr Sicherheitsteam und Ihre Sicherheitsinfrastruktur haben sich unter der Belastung gut bewährt. Sie sind zuversichtlich, dass Ihre Verteidigung dem Test standgehalten hat, aber es gehen Gerüchte um, dass sensible Kundendaten gestohlen wurden und nun von kriminellen Elementen im Internet verkauft werden. Während Ihrer Untersuchung der angeblichen Kompromittierung stellen Sie fest, dass Daten kompromittiert wurden, und Sie haben das Repository gestohlener Daten auf einem Server entdeckt, der sich im Ausland befindet. Ihr Team hat nun vollen Zugriff auf die Daten auf dem fremden Server.

A. Wenden Sie sich an Ihre örtliche Strafverfolgungsbehörde

B. Zerstöre das Depot gestohlener Daten

C. Vertrag mit einer Kreditauskunftei über kostenpflichtige Überwachungsdienste für betroffene Kunden

D. Beraten Sie sich mit anderen C-Level-Führungskräften, um einen Aktionsplan zu entwickeln

Answer(s): D

---

4. Die Risikobereitschaft wird typischerweise durch welche der folgenden organisatorischen Funktionen bestimmt?

A. Audit und Compliance

B. Vorstand

C. Geschäftseinheiten

D. Sicherheit

Answer(s): B

---

5. File Integrity Monitoring (FIM) gilt als a

A. Sicherheitsdetektivkontrolle

B. Software-Segmentierungssteuerung

C. Netzwerkbasierte präventive Sicherheitskontrolle

D. Benutzersegmentierungssteuerung

Answer(s): A

---

6. Die BESTE Organisation, die eine umfassende, unabhängige und zertifizierbare Perspektive auf etablierte Sicherheitskontrollen in einer Umgebung bietet, ist

A. Externe Prüfung

B. Internes Audit

C. Penetrationstester

D. Forensische Experten

Answer(s): A

---

7. SZENARIO: Kritische Server zeigen Anzeichen von fehlerhaftem Verhalten im Intranet Ihrer Organisation. Erste Informationen deuten darauf hin, dass die Systeme von außen angegriffen werden. Als Chief Information Security Officer (CISO) beschließen Sie, das Incident Response Team (IRT) einzusetzen, um die Details dieses Vorfalls zu ermitteln und gemäß den dem Team verfügbaren Informationen Maßnahmen zu ergreifen.

A. Regelmäßige Mitteilung des Vorfallstatus an Führungskräfte

B. Bewahrung von Informationen

C. Beseitigung von Malware und Systemwiederherstellung

D. Ermittlung der Angriffsquelle

Answer(s): B

---

8. Was stellt die RICHTIGE Aufgabentrennung im Unternehmensumfeld dar?

A. Entwickler und Netzwerkteams haben beide Administratorrechte auf Servern

B. Informationssicherheits- und Identitätszugriffsverwaltungsteams erfüllen zwei unterschiedliche Funktionen

C. Finance hat Zugriff auf Personaldaten

D. Informationssicherheits- und Netzwerkteams erfüllen zwei unterschiedliche Funktionen

Answer(s): D

---

9. Welche Angriffsart erfordert den geringsten technischen Aufwand und hat die höchste Erfolgsquote?

A. Kriegstreiben

B. Betriebssystemangriffe

C. Sozialtechnik

D. Schrumpffolienangriff

Answer(s): C

---

10. Der Vorstand hat den CISO einer Organisation aufgefordert, Key Performance Indicators (KPI) zu definieren, um die Effektivität des Security Awareness-Programms zu messen, das Call Center-Mitarbeitern zur Verfügung gestellt wird. Welcher der folgenden kann als KPI verwendet werden?

A. Anzahl erfolgreicher Social-Engineering-Versuche im Callcenter

B. Anzahl der Anrufer, die Sicherheitsprobleme melden.

C. Anzahl der Anrufer, die das Gespräch verlassen, bevor sie mit einem Vertreter gesprochen haben

D. Anzahl der Anrufer, die einen mangelnden Kundenservice des Callcenters melden

Answer(s): A

---

11. Welche der folgenden Informationen würden am ehesten auf Vorstandsebene innerhalb einer Organisation gemeldet werden?

A. Die Fähigkeiten eines Sicherheitsprogramms in Bezug auf die personelle Unterstützung

B. Signifikante Risiken und Sicherheitsvorfälle, die seit der letzten Mitgliederversammlung entdeckt wurden

C. Systemscan-Trends und -Ergebnisse in Bezug auf interne und externe Bedrohungsquellen

D. Anzahl und Arten von Cyberangriffen, die die Organisation seit der letzten Mitgliederversammlung erlebt hat

Answer(s): B

---

12. Um sicherzustellen, dass die Handlungen aller Mitarbeiter, Anwendungen und Systeme den Regeln und Vorschriften der Organisation entsprechen, kann man sie am BESTEN wie folgt beschreiben?

A. Compliance-Management

B. Risikomanagement

C. Sicherheitsmanagement

D. Vermögensverwaltung

Answer(s): C

---

13. Eine Organisation hat einen Change-Management-Prozess für alle Änderungen an der IT-Produktionsumgebung implementiert. Dieser Change-Management-Prozess folgt Best Practices

und soll dazu beitragen, die Verfügbarkeit und Integrität der IT-Umgebung der Organisation zu stabilisieren. Welche der folgenden Methoden kann verwendet werden, um die Effektivität dieses neu implementierten Prozesses zu messen:

A. Anzahl der bearbeiteten Änderungsaufträge

B. Anzahl und Dauer geplanter Ausfälle

C. Anzahl der abgelehnten Änderungsaufträge

D. Anzahl der ungeplanten Ausfälle

Answer(s): D

---

14. Szenario: Sie sind der CISO und haben gerade Ihre erste Risikobewertung für Ihr Unternehmen abgeschlossen. Sie finden viele Risiken ohne Sicherheitskontrollen und einige Risiken mit unzureichenden Kontrollen. Sie weisen Ihren Mitarbeitern Arbeit zu, um vorhandene Sicherheitskontrollen zu erstellen oder anzupassen, um sicherzustellen, dass sie für die Anforderungen der Risikominderung angemessen sind.

A. Jährlich

B. Vierteljährlich

C. Halbjährlich

D. Niemals

Answer(s): D

---

15. Welche der folgenden Methoden stellt die BESTE Methode dar, um die Ausrichtung des Sicherheitsprogramms an den Geschäftsanforderungen sicherzustellen?

A. Erstellen Sie Sicherheitskonsortien, wie z. B. strategische Sicherheitsplanungsgruppen, die die Beteiligung von Geschäftseinheiten einschließen

B. Stellen Sie sicher, dass die Sicherheitsimplementierungen vor der Einführung der Produktion Business Unit-Tests und funktionale Validierungen umfassen

C. Erstellen Sie ein umfassendes Sicherheitsbewusstseinsprogramm und stellen Sie den Geschäftsbereichen Erfolgskennzahlen zur Verfügung

D. Stellen Sie sicher, dass die Organisation durch klares Sponsoring oder die Schaffung einer CISO-Rolle über eine starke Sicherheitsvertretung auf Führungsebene verfügt

Answer(s): A

---

16. Welche der folgenden Punkte ist am wichtigsten, wenn die Sicherheitsverantwortlichen einer Organisation die Sicherheit so ausrichten müssen, dass sie die Kultur einer Organisation beeinflusst?

A. Besitzt einen starken technischen Hintergrund

B. Hat einen starken Auditing-Hintergrund

C. Alle Vorschriften verstehen, die die Organisation betreffen

D. Die Geschäftsziele der Organisation verstehen

Answer(s): D

---

17. Welche der folgenden Aussagen zu den Kapitalausgaben ist richtig?

A. Kapitalausgaben sind in der Regel langfristige Investitionen, deren Wert durch ihre Nutzung realisiert wird.

B. Sie lassen sich leicht durch den Verzicht auf die Nutzung reduzieren, z. B. durch die Reduzierung der Energie für die Beleuchtung von Arbeitsbereichen außerhalb der Arbeitszeiten.

C. Kapitalausgaben können niemals durch Betriebsausgaben ersetzt werden

D. Die Organisation kann die Anschaffungskosten in der Regel durch den Verkauf dieser Art von Vermögenswerten zurückgewinnen.

Answer(s): B

---

18. Die jährliche Verlusterwartung wird aus der Funktion welcher beiden Faktoren abgeleitet?

A. Jährliche Eintrittsrate und Einzelschadenerwartung

B. Einzelverlusterwartung und Risikofaktor

C. Schutzwert und jährliche Häufigkeit des Auftretens

D. Jährliche Häufigkeit und Vermögenswert

Answer(s): A

---

19. Welche Beziehung besteht zwischen Informationsschutz und der Einhaltung gesetzlicher Vorschriften?

A. Es gibt keine Beziehung zwischen den beiden.

B. Dass alle Informationen in einer Organisation gleichermaßen geschützt werden müssen.

C. Dass der Schutz einiger Informationen, wie z. B. Personalausweisinformationen, gesetzlich vorgeschrieben ist und andere Informationen, wie z. B. Geschäftsgeheimnisse, aufgrund geschäftlicher Anforderungen geschützt werden.

D. Die Informationen, die gesetzlich geschützt werden müssen, müssen nicht in der Datenklassifizierungsrichtlinie der Organisation angegeben werden.

Answer(s): C

---

20. Was muss als Erstes erledigt werden, um ein Sicherheitsprogramm für Ihr Unternehmen zu erstellen?

A. Geschäftskontinuitätsplan

B. Budget des Sicherheitsprogramms

C. Risikobewertung

D. Compliance- und Regulierungsanalyse

Answer(s): C
