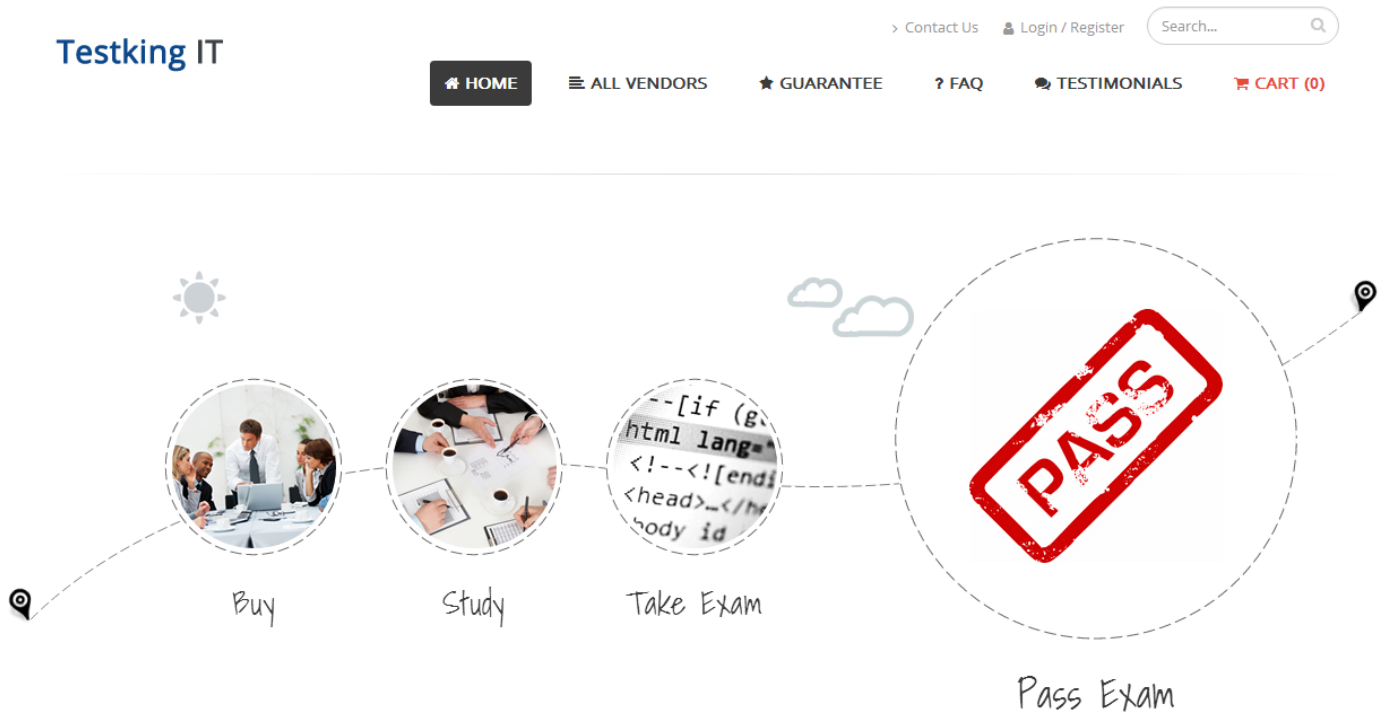
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **NIS-2-Directive-Lead-Implementer-German**

Title : PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer Deutsch Version)

Vendor : PECB

Version : DEMO

QUESTION NO: 1

Szenario 8: Die FoodSafe Corporation ist ein renommiertes Lebensmittelunternehmen in Wien, Österreich, das sich auf die Herstellung vielfältiger Produkte spezialisiert hat – von herzhaften Snacks bis hin zu handwerklich hergestellten Desserts. Da das Unternehmen den Bestimmungen der NIS-2-Richtlinie unterliegt, setzt die FoodSafe Corporation verschiedene Cybersicherheitsprüfungen ein, um die Integrität und Sicherheit ihrer Lebensmittelproduktionsprozesse zu gewährleisten.

Um eine effektive Schwachstellenanalyse durchzuführen, nutzt die FoodSafe Corporation ein Schwachstellenanalyse-Tool, um Sicherheitslücken auf Netzwerkgeräten wie Servern und Workstations aufzudecken. Darüber hinaus hat die FoodSafe Corporation bewusst klare Testziele definiert und während der Analysephase die Zustimmung des Top-Managements eingeholt. Dieser strukturierte Ansatz gewährleistet, dass die Schwachstellenanalysen mit klaren Zielen durchgeführt werden und das Management-Team aktiv in den Analyseprozess eingebunden ist und ihn unterstützt. Dies unterstreicht das Engagement des Unternehmens für höchste Cybersicherheitsstandards.

Im Einklang mit der NIS-2-Richtlinie hat die FoodSafe Corporation Audits in ihre Kernaktivitäten integriert. Diese beginnen mit einer internen Bewertung, gefolgt von einem zusätzlichen Audit durch ihre Partner. Um die Effektivität dieser Audits zu gewährleisten, hat das Unternehmen die operativen Bereiche, Verfahren und Richtlinien sorgfältig identifiziert. Allerdings verzichtete die FoodSafe Corporation im Rahmen ihres internen Compliance-Auditprozesses auf einen strukturierten Auditzeitplan. Obwohl das Organigramm der FoodSafe Corporation die Position des Auditteams nicht eindeutig ausweist, ist der interne Auditprozess gut strukturiert. Die Auditoren machen sich mit den etablierten Richtlinien und Verfahren vertraut, um ein umfassendes Verständnis ihrer Arbeitsabläufe zu erlangen. Sie führen darüber hinaus Gespräche mit den Mitarbeitern, um ihre Erkenntnisse zu vertiefen und sicherzustellen, dass keine wichtigen Details übersehen werden.

Anschließend erstellen die Auditoren der FoodSafe Corporation einen umfassenden Bericht über ihre Feststellungen, der als Grundlage für notwendige Änderungen und Verbesserungen im Unternehmen dient. Die Auditoren verfolgen außerdem die Umsetzung von Maßnahmenplänen, die auf festgestellte Abweichungen und Verbesserungsmöglichkeiten reagieren.

Das Unternehmen hat kürzlich sein Angebot um neue Produkte und Dienstleistungen erweitert, was Auswirkungen auf sein Cybersicherheitsprogramm hatte. Das Cybersicherheitsteam musste sich daher anpassen und die sichere Integration der Erweiterungen in die bestehende Infrastruktur gewährleisten. FoodSafe Corporation engagiert sich für die Optimierung seiner Überwachungs- und Messprozesse, um Produktqualität und betriebliche Effizienz sicherzustellen. Dabei berücksichtigt das Unternehmen sorgfältig seine Zielgruppe und wählt geeignete Methoden zur Berichterstattung über die Überwachungs- und Messergebnisse. Dies umfasst die Integration zusätzlicher grafischer Elemente und die Kennzeichnung von Endpunkten in die Berichte, um die Daten übersichtlicher und intuitiver darzustellen und so letztendlich eine bessere Entscheidungsfindung im Unternehmen zu ermöglichen.

Laut Szenario 8 verfolgen interne Auditoren Maßnahmenpläne als Reaktion auf Abweichungen oder Verbesserungsmöglichkeiten. Entspricht dies den Best Practices?

A. Nein, die Korrekturen und Korrekturmaßnahmen sollten vom

Informationssicherheitsbeauftragten geprüft werden.

B. Ja, der interne Prüfer sollte die als Reaktion auf Abweichungen eingereichten Maßnahmenpläne weiterverfolgen.

C. Ja, der interne Revisor ist dafür verantwortlich, den Fortschritt der Maßnahmenpläne zu verfolgen und sicherzustellen, dass sie alle unverzüglich umgesetzt werden.

Answer: B

QUESTION NO: 2

Szenario 5: Astral Nexus Power mit Sitz in Altenberg ist ein innovatives Unternehmen, das von visionären Ingenieuren und Wissenschaftlern gegründet wurde und sich auf zukunftsweisende Technologien im Stromsektor konzentriert. Der Fokus liegt auf der Entwicklung von Energiespeicherlösungen der nächsten Generation, die auf modernsten Quantenmaterialien basieren. Das Unternehmen hat die entscheidende Bedeutung der Sicherung seiner Energieinfrastruktur erkannt und die Anforderungen der NIS-2-Richtlinie übernommen. Darüber hinaus arbeitet es kontinuierlich mit Cybersicherheitsexperten zusammen, um seine digitalen Systeme zu stärken, sich vor Cyberbedrohungen zu schützen und die Integrität des Stromnetzes zu gewährleisten. Durch die Integration fortschrittlicher Sicherheitsprotokolle trägt das Unternehmen zur allgemeinen Resilienz und Stabilität der europäischen Energielandschaft bei.

Um die Anforderungen der NIS-2-Richtlinie zu erfüllen, leitete das Unternehmen einen umfassenden Transformationsprozess ein. Dieser begann mit einer eingehenden Analyse der Unternehmensstruktur und des Unternehmensumfelds, wodurch unter anderem die Rollen und Verantwortlichkeiten im Bereich Sicherheit klar definiert werden konnten. Das Unternehmen hat einen Chief Information Security Officer (CISO) ernannt, der die strategische Ausrichtung der Cybersicherheit festlegt und den Schutz der Informationswerte gewährleistet. Der CISO berichtet direkt an den CEO von Astral Nexus Power, was zu fundierteren Entscheidungen hinsichtlich Risiken, Ressourcen und Investitionen beiträgt. Zur effektiven Wahrnehmung der Aufgaben und Verantwortlichkeiten im Bereich Informationssicherheit hat das Unternehmen ein Cybersicherheitsteam eingerichtet, das aus Mitarbeitern des Unternehmens und einem externen Cybersicherheitsberater besteht.

Astral Nexus Power legt großen Wert auf ein effektives Asset-Management. Das Unternehmen identifiziert und kategorisiert seine digitalen Assets systematisch, erstellt ein Inventar und bewertet die mit jedem Asset verbundenen Risiken. Darüber hinaus überwacht und wartet es die Assets und verfügt über einen Prozess zur kontinuierlichen Verbesserung. Das Unternehmen hat außerdem sein IT-Sicherheits-Incident-Response-Team (CSIRT) mit der Überwachung seiner internen und externen, internetfähigen Assets beauftragt, was zur Minimierung der Unternehmensrisiken beiträgt.

Darüber hinaus initiiert das Unternehmen einen umfassenden Prozess zur Risikoidentifizierung, -analyse, -bewertung und -behandlung. Durch die Identifizierung von Betriebsszenarien, die anschließend hinsichtlich Anlagen, Bedrohungen und Schwachstellen detailliert beschrieben werden, gewährleistet das Unternehmen eine umfassende Identifizierung und ein tiefes Verständnis potenzieller Risiken. Dieses Verständnis bildet die Grundlage für die Auswahl und Entwicklung von Risikobehandlungsstrategien, die anschließend mit den Stakeholdern kommuniziert und abgestimmt werden. Das Engagement von Astral Nexus Power wird zudem durch die sorgfältige Dokumentation und

Berichterstattung dieser Maßnahmen unterstrichen, wodurch Transparenz und Verantwortlichkeit gefördert werden.
Welche der folgenden Aussagen veranschaulicht am besten, basierend auf Szenario 5, das Engagement von Astral Nexus Power für die Erfüllung der Anforderungen der NIS-2-Richtlinie in Bezug auf das Anlagenmanagement?

A. Das tiefgreifende Verständnis des Unternehmens für seine Struktur und seinen Kontext

B. Überwachung der internetbasierten Anlagen des Unternehmens innerhalb und außerhalb des Firmengeländes durch CSIRT.

C. Die klare Festlegung der Rollen und Verantwortlichkeiten im Unternehmen.

Answer: B

QUESTION NO: 3

Szenario 8: Die FoodSafe Corporation ist ein renommiertes Lebensmittelunternehmen in Wien, Österreich, das sich auf die Herstellung vielfältiger Produkte spezialisiert hat – von herzhaften Snacks bis hin zu handwerklich hergestellten Desserts. Da das Unternehmen den Bestimmungen der NIS-2-Richtlinie unterliegt, setzt die FoodSafe Corporation verschiedene Cybersicherheitsprüfungen ein, um die Integrität und Sicherheit ihrer Lebensmittelproduktionsprozesse zu gewährleisten.
Um eine effektive Schwachstellenanalyse durchzuführen, nutzt die FoodSafe Corporation ein Schwachstellenanalyse-Tool, um Sicherheitslücken auf Netzwerkgeräten wie Servern und Workstations aufzudecken. Darüber hinaus hat die FoodSafe Corporation bewusst klare Testziele definiert und während der Analysephase die Zustimmung des Top-Managements eingeholt. Dieser strukturierte Ansatz gewährleistet, dass die Schwachstellenanalysen mit klaren Zielen durchgeführt werden und das Management-Team aktiv in den Analyseprozess eingebunden ist und ihn unterstützt. Dies unterstreicht das Engagement des Unternehmens für höchste Cybersicherheitsstandards.
Im Einklang mit der NIS-2-Richtlinie hat die FoodSafe Corporation Audits in ihre Kernaktivitäten integriert. Diese beginnen mit einer internen Bewertung, gefolgt von einem zusätzlichen Audit durch ihre Partner. Um die Effektivität dieser Audits zu gewährleisten, hat das Unternehmen die operativen Bereiche, Verfahren und Richtlinien sorgfältig identifiziert. Allerdings verzichtete die FoodSafe Corporation im Rahmen ihres internen Compliance-Auditprozesses auf einen strukturierten Auditzeitplan. Obwohl das Organigramm der FoodSafe Corporation die Position des Auditteams nicht eindeutig ausweist, ist der interne Auditprozess gut strukturiert. Die Auditoren machen sich mit den etablierten Richtlinien und Verfahren vertraut, um ein umfassendes Verständnis ihrer Arbeitsabläufe zu erlangen. Sie führen darüber hinaus Gespräche mit den Mitarbeitern, um ihre Erkenntnisse zu vertiefen und sicherzustellen, dass keine wichtigen Details übersehen werden.
Anschließend erstellen die Auditoren der FoodSafe Corporation einen umfassenden Bericht über ihre Feststellungen, der als Grundlage für notwendige Änderungen und Verbesserungen im Unternehmen dient. Die Auditoren verfolgen außerdem die Umsetzung von Maßnahmenplänen, die auf festgestellte Abweichungen und Verbesserungsmöglichkeiten reagieren.
Das Unternehmen hat kürzlich sein Angebot um neue Produkte und Dienstleistungen erweitert, was Auswirkungen auf sein Cybersicherheitsprogramm hatte. Das Cybersicherheitsteam musste sich daher anpassen und die sichere Integration der

Erweiterungen in die bestehende Infrastruktur gewährleisten. FoodSafe Corporation engagiert sich für die Optimierung seiner Überwachungs- und Messprozesse, um Produktqualität und betriebliche Effizienz sicherzustellen. Dabei berücksichtigt das Unternehmen sorgfältig seine Zielgruppe und wählt geeignete Methoden zur Berichterstattung über die Überwachungs- und Messergebnisse. Dies umfasst die Integration zusätzlicher grafischer Elemente und die Kennzeichnung von Endpunkten in die Berichte, um die Daten übersichtlicher und intuitiver darzustellen und so letztendlich eine bessere Entscheidungsfindung im Unternehmen zu ermöglichen.
Hat die FoodSafe Corporation auf Basis von Szenario 8 die Entdeckungsphase von Penetrationstests gemäß NIST SP 800-115 definiert?

A. Nein, in der Entdeckungsphase werden die Tests eingeleitet und eine Schwachstellenanalyse durchgeführt.

B. Nein, die Entdeckungsphase ist der Prozess der Identifizierung möglicher Angriffe durch den Versuch, Schwachstellen auszunutzen.

C. Ja, die Entdeckungsphase ist korrekt definiert

Answer: C

QUESTION NO: 4

Szenario 4: StellarTech ist ein Technologieunternehmen, das innovative Lösungen für eine vernetzte Welt anbietet. Das Portfolio umfasst wegweisende IoT-Geräte, leistungsstarke Softwareanwendungen und hochmoderne Kommunikationssysteme. Angesichts der sich ständig weiterentwickelnden Cybersicherheitslandschaft und der Notwendigkeit, digitale Resilienz zu gewährleisten, hat StellarTech beschlossen, ein Cybersicherheitsprogramm gemäß den Anforderungen der NIS-2-Richtlinie einzuführen. Das Unternehmen hat Nick, einen erfahrenen Informationssicherheitsmanager, mit der erfolgreichen Umsetzung dieser Anforderungen beauftragt. Nick leitete den Implementierungsprozess mit einer gründlichen Analyse der Organisationsstruktur von StellarTech ein. Er stellte fest, dass das Unternehmen ein klar definiertes Modell anwendet, das die Zuordnung von Bereichen nach Fachgebieten oder operativen Funktionen ermöglicht und eine klare Rollenverteilung sowie eindeutige Verantwortlichkeiten gewährleistet.
Um die Anforderungen der NIS-2-Richtlinie zu erfüllen, haben Nick und sein Team ein Anlagenmanagementsystem implementiert und eine Anlagenmanagementrichtlinie mit festgelegten Zielen und Prozessen zur Zielerreichung entwickelt. Im Rahmen des Anlagenmanagementprozesses identifiziert, erfasst und pflegt das Unternehmen alle Anlagen, die unter das System fallen.
Um Risiken effektiv zu managen, verfolgt das Unternehmen einen strukturierten Ansatz. Dieser umfasst die Definition von Umfang und Parametern für Risikomanagement, Risikobewertung, Risikobehandlung, Risikoakzeptanz, Risikokommunikation, Sensibilisierung und Beratung sowie Risikoüberwachung und -prüfung. Dieser Ansatz ermöglicht die Anwendung von Cybersicherheitspraktiken auf Basis vergangener und aktueller Cybersicherheitsaktivitäten, einschließlich gewonnener Erkenntnisse und prädiktiver Indikatoren. Das unternehmensweite Risikomanagementprogramm von StellarTech orientiert sich an den Zielen der Geschäftsleitung, die Risikomanagement wie ein finanzielles Risiko behandelt. Das Budget ist an die Risikolandschaft angepasst, während die Geschäftsbereiche die Vision der Geschäftsleitung mit einem ausgeprägten Bewusstsein für

systemweite Risiken umsetzen. Das Unternehmen teilt Informationen in Echtzeit, versteht seine Rolle im größeren Ökosystem und trägt aktiv zum Risikoverständnis bei. StellarTechs agile Reaktion auf sich entwickelnde Bedrohungen und der Fokus auf proaktive Kommunikation unterstreichen das Engagement für exzellente Cybersicherheit und Resilienz.
Im vergangenen Monat führte das Unternehmen eine umfassende Risikoanalyse durch. Dabei wurde eine potenzielle Bedrohung durch eine ausgeklügelte Form von Cyberangriffen identifiziert, die gezielt IoT-Geräte ins Visier nehmen. Obwohl diese Bedrohung theoretisch möglich ist, wurde ihr Eintritt aufgrund der robusten Sicherheitsmaßnahmen des Unternehmens, des Fehlens vorheriger Vorfälle und seiner bestehenden strengen Cybersicherheitspraktiken als äußerst unwahrscheinlich eingestuft.
Beantworten Sie anhand des obigen Szenarios die folgende Frage:
Welches Organisationsmodell hat StellarTech gewählt?

A. Divisional

B. Matrix

C. Funktionell

Answer: C

QUESTION NO: 5

Szenario 3: SafePost, gegründet 2001, ist ein renommiertes Post- und Kurierunternehmen mit Hauptsitz in Brüssel, Belgien. Im Laufe der Jahre hat es sich zu einem wichtigen Akteur im Logistik- und Kuriersektor der Region entwickelt. Mit über 500 Mitarbeitern ist das Unternehmen stolz auf seine effizienten und zuverlässigen Dienstleistungen für Privat- und Geschäftskunden. SafePost hat die Bedeutung von Cybersicherheit in einer zunehmend digitalisierten Welt erkannt und bedeutende Schritte unternommen, um seine Geschäftstätigkeit an regulatorische Vorgaben wie die NIS-2-Richtlinie anzupassen.
SafePost erkannte die Bedeutung einer gründlichen Analyse der Marktkräfte und -chancen für seine Cybersicherheitsstrategie. Daher wählte das Unternehmen einen Ansatz, der die Analyse der Marktkräfte und -chancen in den vier folgenden Bereichen ermöglichte: Politik, Wirtschaft, Gesellschaft und Technologie. Die Ergebnisse der Analyse halfen SafePost, aufkommende Bedrohungen vorherzusehen und seine Sicherheitsmaßnahmen an die sich wandelnde Landschaft der Post- und Kurierbranche anzupassen.
Um die Anforderungen der NIS-2-Richtlinie zu erfüllen, hat SafePost umfassende Cybersicherheitsmaßnahmen und -verfahren implementiert, die dokumentiert und in Schulungen vermittelt wurden. Diese Verfahren werden jedoch nur für einzelne Projekte angewendet und sind noch nicht unternehmensweit implementiert. Darüber hinaus hat das Risikomanagement-Team von SafePost mehrere Maßnahmen zum Cybersicherheitsrisikomanagement entwickelt und genehmigt, um potenzielle Risiken zu minimieren, Kundendaten zu schützen und die Geschäftskontinuität zu gewährleisten.
Darüber hinaus hat SafePost eine Cybersicherheitsrichtlinie entwickelt, die Leitlinien und Verfahren zum Schutz digitaler Assets und sensibler Daten sowie zur Definition der Rollen und Verantwortlichkeiten der Mitarbeiter bei der Aufrechterhaltung der Sicherheit enthält. Diese Richtlinie unterstützt das Unternehmen, indem sie einen strukturierten Rahmen zur Identifizierung und Minderung von Cybersicherheitsrisiken bietet, die Einhaltung von Vorschriften sicherstellt und eine Kultur des Sicherheitsbewusstseins unter den Mitarbeitern

fördert. Dies verbessert letztendlich die allgemeine Cybersicherheit und reduziert die Wahrscheinlichkeit von Cyberangriffen.
Während SafePost sich weiterhin den dynamischen Marktkräften und -chancen stellt, bleibt das Unternehmen seinem Anspruch treu, die höchsten Standards der Cybersicherheit einzuhalten, um die Interessen seiner Kunden zu schützen und seine Position als vertrauenswürdiger Marktführer in der Post- und Kurierbranche zu behaupten.
Beantworten Sie anhand des obigen Szenarios die folgende Frage:
Warum gilt die NIS-2-Richtlinie für SafePost?
A. Da die Richtlinie für Unternehmen gilt, die Postdienstleistungen innerhalb der Europäischen Union anbieten
B. Da die Richtlinie nur für Unternehmen mit mehr als 500 Beschäftigten gilt, die Postdienstleistungen innerhalb der Europäischen Union erbringen.
C. Da die Richtlinie für Einrichtungen gilt, die Vertrauensdienste im Sinne der EU-Vorschriften innerhalb der Europäischen Union anbieten
Answer: A

QUESTION NO: 6
Welche Aussage bezüglich EU-CyCLONe ist korrekt?
A. Es dient als Brücke zwischen operativer und politischer Ebene bei Großereignissen und Krisen.
B. Es dient als Brücke zwischen technischer und politischer Ebene bei Großereignissen und Krisen.
C. Es dient als Brücke zwischen operativer und technischer Ebene bei Großereignissen und Krisen.
Answer: B

QUESTION NO: 7
Worin besteht der Hauptunterschied zwischen Tier-2- und Tier-3-Disaster-Recovery -Strategien?
A. Stufe 2 umfasst die elektronische Speicherung kritischer Daten, während Stufe 3 auf externe Datenspeicher setzt.
B. Tier 2 nutzt Kuriere für den Datentransport zwischen den Zentren, während Tier 3 die elektronische Speicherung kritischer Daten verwendet.
C. Stufe 2 schreibt zwei Standorte mit Peer-to-Peer-Verbindungen vor, während Stufe 3 den Fokus auf die Verbesserung des Datentransfers legt.
Answer: B

QUESTION NO: 8
Was sollte eine Cybersicherheitsrichtlinie hinsichtlich des Umgangs mit sensiblen Informationen festlegen?
A. Richtlinien, die erklären, wie alle sensiblen Daten endgültig gelöscht werden können
B. Richtlinien für die Freigabe von Berechtigungen und Datenmaskierungstechniken bei Bedrohungen
C. Leitfaden zum Teilen sensibler Informationen auf Social-Media-Plattformen

Answer: B