

**FRAGE 1 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 01**



Wodurch ist ein Root Kit charakterisiert und welche Funktionalitäten bietet dieses? Erklären Sie kurz.

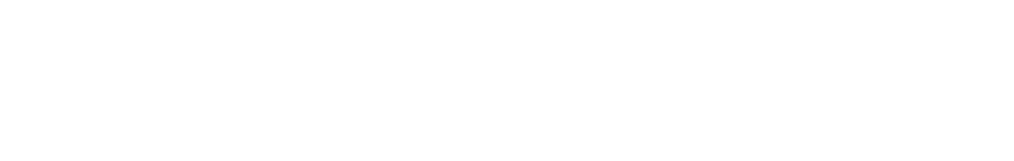
Ein Root Kit kann einen Computer komplett kontrollieren. Der Name stammt vom Benutzer administrativer Rechte auf Linux-Systemen und beschreibt damit die Grundfunktionalität von Root Kits: das Erlangen erhöhter Rechte auf einem Computer und damit die komplette Kontrolle zu übernehmen. [3 Punkte]

Neben dem Erlangen der erhöhten Rechte können Root Kits sich selbst verstecken, indem sie sich in legitime Prozesse migrieren oder ihre Funktion ohne Datei bereitstellen. Außerdem kann ein dauerhafter Zugang gesichert werden, indem Hintertüren in Systeme eingebaut werden. Meist bieten Root Kits auch die Möglichkeit, weitere Module nachzuladen. [3 Punkte]



**FRAGE 3 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 01**



Was ist die namensgebende Eigenschaft einer Ransomware? Nennen und beschreiben Sie kurz zwei Vorgehensweisen für eine Ransomware.

Eine Ransomware versucht ein Ransom (Lösegeld) zu erpressen, indem Angriffe auf Computer und Systeme gestartet werden. Diese werden erst beendet, wenn das Lösegeld gezahlt wird. [2 Punkte]

[2 Punkte je Vorgehensweise]

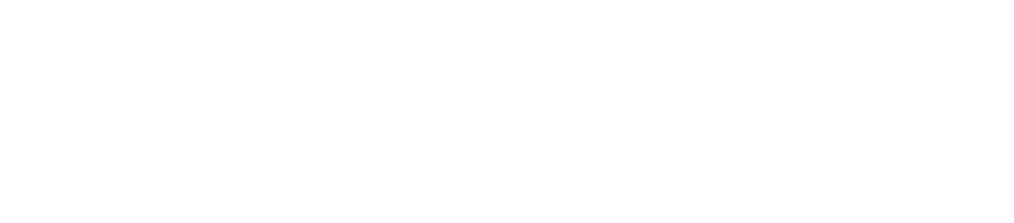
DoS-Angriff: Hier werden Systeme blockiert indem massenhaft Zugriffe erzeugt werden. Diese Blockade endet erst, wenn das Lösegeld gezahlt wurde.

Verschlüsselungstrojaner: Ein Trojaner verschlüsselt alle Daten einer Organisation, sodass diese für die Organisation unzugänglich sind. Der Schlüssel wird angeblich erst herausgegeben, wenn das Lösegeld ausgezahlt wird.



**FRAGE 4 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 01**



Beschreiben Sie kurz die Unterschiede zwischen den Begriffen Computerkriminalität und Internetkriminalität. Zu welchem englischen Begriff werden diese beiden zusammengefasst? Argumentieren Sie kurz, inwieweit die Unterscheidung der beiden deutschen Begriffe unter den aktuellen Entwicklungen Sinn ergibt?

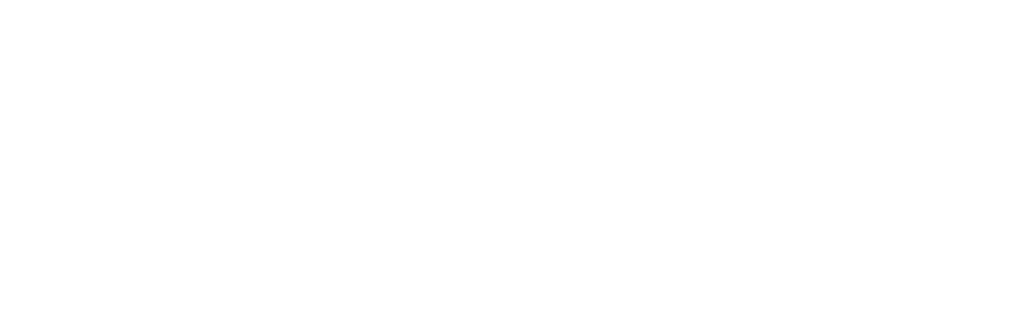
Für die Begriffe Computer- bzw. Internetkriminalität gibt es keine einheitliche Definition. Im Allgemeinen werden unter Computerkriminalität alle Taten verstanden, welche sich gegen Computer richten oder einen Computer als Werkzeug nutzen. [2 Punkte]

Die Internetkriminalität umfasst wiederum alle Taten, welche das Internet nutzen. [2 Punkte] Cybercrime fasst beide zusammen. [1 Punkt]

Da für Letzteres immer ein Computer bzw. moderne Informations- und Kommunikationstechnik genutzt wird, gehen diese beiden Begriffe ineinander über und werden im Englischen zusammengefasst als Cybercrime übersetzt. [1 Punkt]



**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 01**



Nennen und beschreiben Sie kurz die fünf Ebenen auf denen die Schwachstellen eingeordnet werden können und ordnen Sie anschließend das folgende Beispiel in eine der Ebenen ein. Begründungen Sie Ihre Wahl. Beispiel:

Beim Hochfahren einer bestimmten Charge Laptops wird bei der Initialisierung der USB-Schnittstellen ein eventuell angeschlossenes Gerät analysiert und dabei wird unter Umständen ein Programmcode auf dem USB-Gerät ausgeführt. Damit kann ein Angreifer erhöhte Rechte erlangen.

5 Ebenen [15 Punkte; 3 je Ebene + Beschreibung]:

Schwachstellen auf Chip- oder Firmware-Ebene betrifft Schwachstellen auf Prozessoren oder der Firmware. Die Firmware ist dabei die Software, welche auf niedriger Ebene Funktionen der Hardware bereitstellt.

Schwachstellen auf Betriebssystemebene Schwachstellen auf Betriebssystemebene betrifft die Software, welche alle Hardwareressourcen für die Anwendungssoftware zur Verfügung stellt.

Schwachstellen auf Netzwerk- und Serverebene

Hier sind Schwachstellen angesiedelt, welche auf der Kommunikation zwischen Systemen in einem Netzwerk basieren oder Serverfunktionalitäten eines Systems ausnutzen.

Schwachstellen auf Anwendungsebene

Hier sind Schwachstellen angesiedelt, welche Anwendungen ausnutzen. Anwendungen sind dabei alle Programme, welche auf einem Betriebssystem laufen und Ressourcen über dieses bereitgestellt bekommen.

Schwachstellen auf Organisationsebene

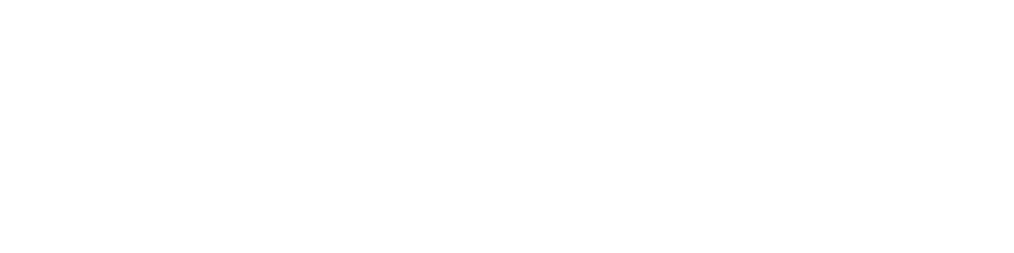
Schwachstellen auf Organisationsebene beziehen sich auf Richtlinien, Ablauf- und Aufbauorganisation.

Bsp. kann eingeordnet werden unter: Firmware oder Betriebssystem. Begründung ist wichtig. Offensichtlich führt die Software, welche das USB-Geräte dem restlichen System zur Verfügung stellen will, Programmcodes auf dem Gerät aus. Normalerweise soll diese Software lediglich das Gerät erkennen und analysieren, aber in diesem Fall wird durch eine Schwachstelle ein Code ausgeführt.

Diese Software wird als Firmware bezeichnet, da sie auf einem niedrigen Level Hardwarefunktionen bereitstellt, also ist dies eine Schwachstelle auf Firmware-Ebene. [3 Punkte]



**DLMIMWCK01\_Offen\_mittel/Lektion 01**



Der Vorsitzende einer Organisation berichtet von vermehrten Kontaktanfragen an ihn auf sozialen Netzwerken von Personen, die ihm unbekannt sind.

Welche Angriffsart könnte hier verfolgt werden und was ist das Ziel der Angreifer? Nennen Sie drei beispielhafte Ziele des Angreifers mit dieser Aktion.

Es wird versucht, Informationen über eine Person zu sammeln und sie ihm zu entlocken. Da die anvisierte Person ein hochwertiges Ziel ist, da durch den Zugang zum Vorsitzenden einer Organisation wertvolle Informationen erlangt oder evtl. hohe Geldbeträge angewiesen werden können, qualifiziert sich dieser Angriff als Whaling. Whaling beschreibt den Angriff auf "Wale" also hochwertige Ziele. [3 Punkte]

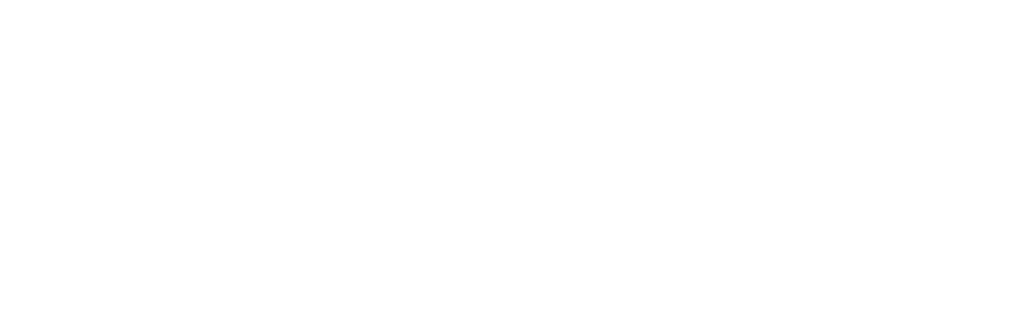
Mit den Informationen eines hochwertigen Ziels können: [1 Punkt je Beispiel; max. 3 Punkte] CEO-Fraud,

Diebstahl sensibler Daten und

Erlangung von Zugangsdaten betrieben werden.



**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 01**



Nennen Sie die fünf Ebenen, auf denen die Schwachstellen eingeordnet werden können und ordnen Sie anschließend das folgende Beispiel in eine der Ebenen ein. Begründen Sie Ihre Wahl.

Beispiel:

Während des Updates öffnet eine Anwendung der Lohnbuchhaltung einen TCP-Port, um auf Abhängigkeiten des Updates zu prüfen. Sendet ein Angreifer bestimmte Anfragen an diesen Port, sendet die Anwendung sensible Informationen als Antwort zurück.

5 Ebenen [15 Punkte; 3 je Ebene + Beschreibung]: Schwachstellen auf Chip- oder Firmware-Ebene

Betrifft Schwachstellen auf Prozessoren oder der Firmware. Die Firmware ist dabei die Software, welche auf niedriger Ebene Funktionen der Hardware bereitstellt.

Schwachstellen auf Betriebssystemebene

Schwachstellen auf Betriebssystemebene betrifft die Software, welche alle Hardwareressourcen für die Anwendungssoftware zur Verfügung stellt.

Schwachstellen auf Netzwerk- und Serverebene

Hier sind Schwachstellen angesiedelt, welche auf der Kommunikation zwischen Systemen in einem Netzwerk basieren oder Serverfunktionalitäten eines Systems ausnutzen.

Schwachstellen auf Anwendungsebene

Hier sind Schwachstellen angesiedelt, welche Anwendungen ausnutzen. Anwendungen sind dabei alle Programme, welche auf einem Betriebssystem laufen und Ressourcen über dieses bereitgestellt bekommen.

Schwachstellen auf Organisationsebene

Schwachstellen auf Organisationsebene beziehen sich auf Richtlinien, Ablauf- und Aufbauorganisation.

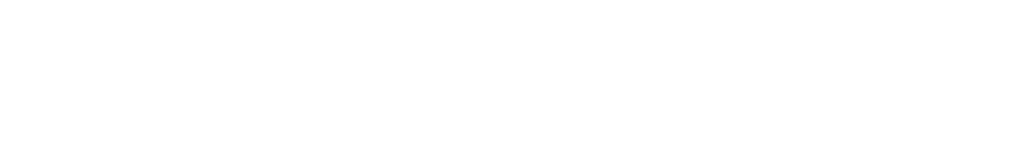
Bsp. kann eingeordnet werden unter: Netzwerk oder Anwendung. Begründung ist wichtig. Offensichtlich verarbeitet die Anwendung die Daten, welche auf dem Port zugesandt werden, nicht korrekt bzw. die zugesandten Daten und deren Sender werden nicht auf Authentizität überprüft.

Somit liegt die Schwachstelle in der Lohnbuchhaltungssoftware und damit in der Anwendungsebene vor. [3 Punkte]



**FRAGE 14 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 02**



Als Reaktion auf Nichtanwendbarkeit welche Paragrafen wurde der § 269 StGB eingeführt?

Nennen Sie den Grund, warum dies notwendig war.

Nichtanwendbarkeit von §267 StGB auf Fälschung beweiserheblicher digitaler Daten. [3 Punkte]

§ 267 StGB umfasst die Fälschung physischer Urkunden, aber nicht digitaler. Dafür wurde §269 StGB erstellt. [3 Punkte]



**FRAGE 15 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 02**



Wie ist Identität im Zusammenhang mit Indentitätsmissbrauch definiert? Nennen Sie vier Beispiele für eine Identitätskennzeichnung.

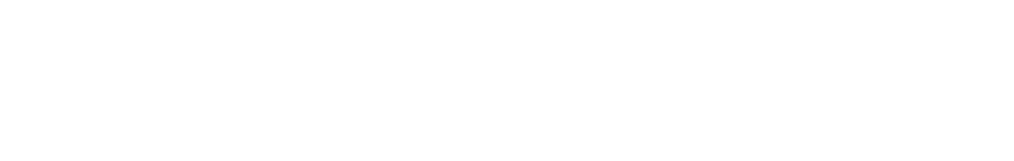
Prinzipiell klärt die Identität, wer jemand ist. Dazu umfasst die Identität eindeutig kennzeichnende Merkmale, welche eine Person oder Organisation identifizieren. [2 Punkte]

SteuerID, Ausweis, Benutzername/Passwort, Name + Geburtsdatum, Name + Anschrift, kryptografischer Schlüssel,... [max. 4 Punkte; 1 Punkt je Beispiel]



**FRAGE 17 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 02**



Warum ist der Straftatbestand des Diebstahls **nicht** auf Identitätsdiebstahl zutreffend?

Besteht hier eine Strafbarkeitslücke? Begründen Sie Ihre Antwort.

§ 242 StGB Diebstahl ist nur auf bewegliche Dinge anwendbar. Eine Identität im Bezug auf Computerkriminalität ist ein digitales Gut, meist in Form von Benutzername/Passwort oder kryptografischen Schlüsseln. Aus diesem Grund ist dieser nicht auf Identitäten anwendbar. [3 Punkte]

Keine Strafbarkeitslücke, da mehrere andere Paragrafen Identitätsdiebstahl abdecken bspw. §§ 202a,b,c StGB, § 42 BDSG, § 238 StGB [3 Punkte, zwei Beispielparagrafen notwendig].



**FRAGE 16 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 02**



Sie arbeiten in eigener Organisation als Informationssicherheitsbeauftragter und stellen fest, dass einige der Office365-Konten der Organisation für bösartige Zwecke von einem Angreifer missbraucht werden. Sie finden heraus, dass einige E-Mailadressen inklusive Passwort Opfer eines Datenklaus geworden sind. Unter welchen Strafrechtsparagrafen fällt diese Tat? Begründen Sie Ihre Wahl. Wie können Sie herausfinden, welche Benutzerkonten betroffen sind? Welche Maßnahmen würden Sie anschließend ergreifen? Nennen Sie vier Maßnahmen und begründen Sie auch hier Ihre Wahl.

§ 202a, § 202b, § 202c möglich.

§ 202a StgB ist hier beispielsweise anwendbar, da ein Datenklau vorliegt und der § 202a das Ausspähen von Daten unter Strafe stellt. Es sind aber auch andere Paragrafen anwendbar. [3 Punkte]

Es existieren Dienste, wie haveibeenpwned oder das Hasso-Plattner-Institut, welche Daten aus Datendiebstählen durchsuchbar machen. Hier kann nach Domänen oder einzelnen Benutzernamen gesucht werden. Mit diesen Diensten kann herausgefunden werden, ob eine E- Mail-Adresse oder ein Passwort Opfer des Diebstahls geworden ist. [3 Punkte]

Schulungen: Mitarbeiter müssen im richtigen Umgang mit Diensten, wie O365, geschult werden, um Bedienfehler auszuschließen und das normale Verhalten der Software zu erlernen, z. B. wann Makros erlaubt werden müssen.

Sensibilisierungen: Mitarbeiter müssen für Risiken, wie den Diebstahl ihrer Zugangsdaten, sensibilisiert werden.

Außerdem muss eine Awareness geschaffen werden dafür, dass Zugangsdaten nicht mehrfach verwendet werden dürfen, vor allem, wenn die Zugangsdaten für administrative oder andere kritische Dienste verwendet werden.

MFA: Die Nutzung von Mehrfaktor-Authentifizierung hilft dabei, Zugänge zu Diensten zu schützen, da immer der zweite Faktor benötigt wird.

Regelmäßig haveibeenpwned prüfen: Außerdem kann regelmäßig haveibeenpwned geprüft werden, sodass ein Datendiebstahl sofort auffällt, bevor ein Angreifer die Daten aktiv ausnutzt. [3 Punkte je Maßnahmen + Begründung]



**FRAGE 20 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 02**



Welcher Paragraf außerhalb des StGB ist relevant für einen Identitätsdiebstahl und was sagt dieser Paragraf aus?

Der § 42 des Bundesdatenschutzgesetzes ist ebenfalls für den Identitätsdiebstahl ausschlaggebend. [2 Punkte]

Der § 42 BDSG stellt auf die massenweise, gewerbsmäßige Weitergabe und unberechtigte Veröffentlichung von Daten ab. Damit ist dieser Paragraf hauptsächlich für personenbezogene Daten entworfen wurden. [2 Punkte]

Beim § 42 BDSG steht außerdem die Veröffentlichung mit Schädigungsabsicht im Vordergrund. [2 Punkte]



**FRAGE 25 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 02**



Sie arbeiten in einer Organisation als Informationssicherheitsbeauftragter und stellen fest, dass die Zugangsdaten zu GitHub-Repositories von einem Konkurrenten gestohlen wurden. Diese Tat liegt schon einige Zeit zurück und der Quellcode wird bereits in der Software des Konkurrenten genutzt. Mithilfe welcher Gesetzesparagrafen können Sie gegen die Nutzung des Quellcodes durch den Konkurrenten vorgehen? Nennen Sie zwei Paragrafen und begründen Sie Ihre Wahl. Welche grundsätzliche Problematik besteht beim Schutz von Quellcodes? Nennen Sie drei Maßnahmen, welche Sie zum Schutz des Quellcodes ergreifen würden.

Begründen Sie auch hier Ihre Wahl.

§ 142 PatG oder §§ 106–108 UrhG. [1 Punkt]

Es kann versucht werden, Software patentrechtlich zu schützen. In diesem Fall kann der § 142 PatG genutzt werden, um gegen die Verwendung durch den Konkurrenten vorzugehen.

Außerdem ist Software immer durch das Urheberrecht geschützt und es kann somit nach §§ 106– 108 UrhG vorgegangen werden. [2 Punkte]

Computerprogramme sind patentrechtlich nicht schützbar. Dies ist in § 1 Abs. 4 PatG Art. 52 EPÜ niedergeschrieben. "Computer-implementierte Erfindungen" hingegen sind patentierbar. Dies sind Computerprogramme, welche konkrete technische Probleme lösen. Die Abgrenzung zwischen diesen beiden patentrechtliche Konstrukten ist unscharf. Beim Diebstahl von Quellcodes oder Software ist also immer zu prüfen, ob ein Patent für eine computer-implementierte Erfindung vorliegt oder ob das Urheberrecht am Quellcode in Betracht gezogen wird. [3 Punkte]

[1 Punkt je Bsp. und 3 Pkt. je Begründung; max. 12 Pkt] Sicherheitsüberprüfung der Entwickler:

Entwickler haben täglich Zugang zum Quellcode und damit auch die Möglichkeit, diesen zu entwenden. Ein Entwickler sollte vor der Einstellung immer überprüft werden inkl.

Führungszeugnis, sodass frühere Straftaten aufgedeckt werden und keine Entwickler angeheuert werden, welche in der Vergangenheit evtl. bereits Geheimnisverrat begangen haben.

MFA:

Sofern der Abfluss des Quellcodes evtl. über gestohlene Passwörter funktioniert hat, sollte eine Mehrfaktorauthentifizierung eingeführt werden. Die stellt sicher, dass selbst wenn ein Passwort gestohlen wird, kein Zugriff auf den Quellcode durch Fremde gegeben ist.

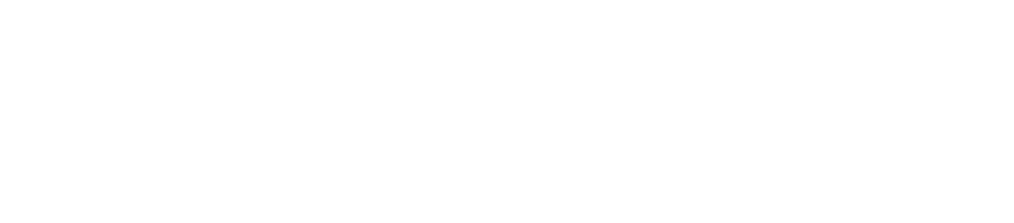
Überprüfung auf öffentlich zugängliche Dienste:

In modernen Entwicklungsumgebunden wird Quellcode in Quellcodeverwaltungssystemen, wie GitHub, organisiert. Hier muss geprüft werden, ob diese richtig konfiguriert sind. Bei Clouddiensten ist es durchaus möglich, dass Quellcodes öffentlich zur Verfügung gestellt wird, wenn Standardeinstellungen verwendet werden.



**FRAGE 26 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 03**



Sie arbeiten in einem Unternehmen, welches hochkomplexe medizinische Produkte herstellt. Eines der größten Risiken stellt ein Datendiebstahl für Sie dar.

Welche Aspekte sollten bedacht werden, bevor IoT-Geräte im Unternehmen eingesetzt werden? Nennen Sie drei Aspekte.

IoT-Geräte erhöhen die Menge und Art der anfallenden Daten. IoT-Geräte erhöhen die Angriffsfläche.

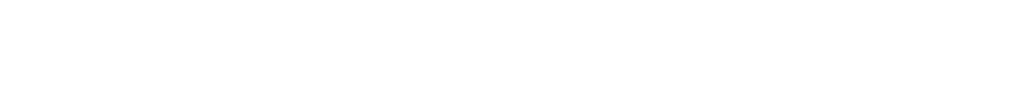
IoT-Geräte sind meist schlecht abgesichert.

… [6 Punkte; 2 Punkte pro Aspekt]



**FRAGE 27 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 03**



Was ist ein Decryptor und wofür wird dieser eingesetzt?

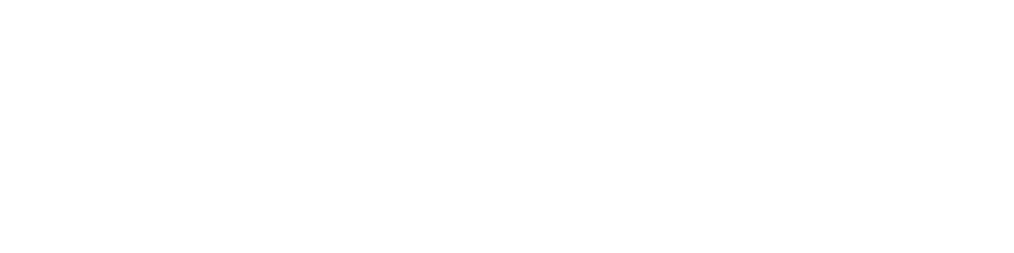
Eine Software zum Entschlüsseln von Dateien ohne den Schlüssel. Auch Schadsoftware weist Fehler auf und es gibt Sicherheitsforscher, welche diese Lücken analysieren und ausnutzen. Hier können dann Decryptoren geschrieben werden, welche durch Verschlüsselungstrojaner verschlüsselte Dateien ohne Kenntnis des Schlüssels entschlüsseln. [3 Punkte]

Der Vorteil von Decryptoren liegt darin, dass das Opfer eines Verschlüsselungstrojaners kein Lösegeld zahlen muss und auch keine weiteren Maßnahmen, wie Backups, bereithalten muss, sofern ein Decryptor für den eingesetzten Verschlüsselungstrojaner vorliegt, da die Originaldaten wieder entschlüsselt werden können. [3 Punkte]



**FRAGE 29 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 03**



Sie haben heute früh in der Zeitung gelesen, dass eine Schwachstelle in aktuellen Routern für den Heimgebrauch dazu verwendet werden kann, ein Botnetz aufzuspannen.

Erläutern Sie, was eine Compoutersabotage kennzeichnet.

Beschreiben Sie anhand des Beispiels, wie Botnetze für Computersabotage eingesetzt werden können.

Danach umfasst Computersabotage alle Taten, welche Datenverarbeitungen, welche für einen Anderen von wesentlicher Bedeutung sind, stören. [2 Punkte]

Botnetze können für DDoS-Attacken genutzt werden. [1 Punkt]

Botnetze bestehen aus Millionen einzelner Bots, welche leicht eine DDoS-Attacke starten können, da diese koordiniert durch einen C&C-Server arbeiten. Übernimmt ein Angreifer die Router über die Schwachstelle wird ein Botnetz innerhalb von Sekunden erbaut und kann genutzt werden. [ 3 Punkte]



**FRAGE 31 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 03**



Wie ist Industriespionage definiert und was ist der Unterschied zur Wirtschaftsspionage?

Industriespionage beschreibt das Ausspähen eines Unternehmens durch einen Konkurrenten oder eine Einzelperson.

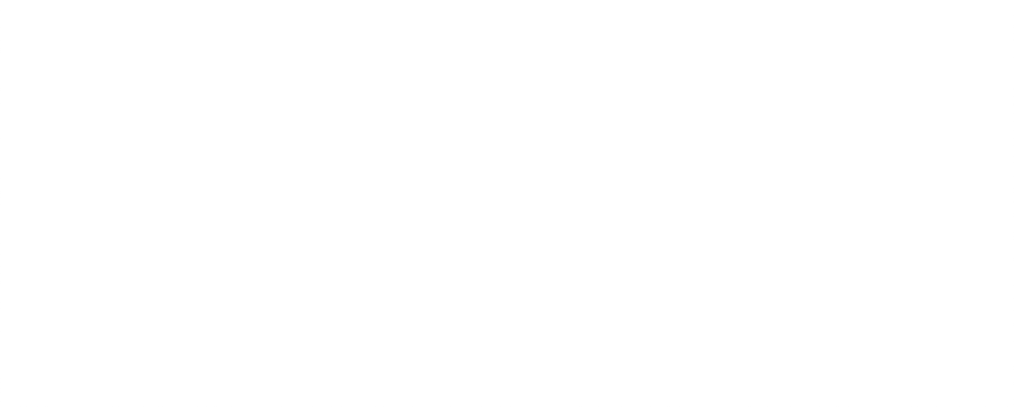
Industriespionage besitzt mehrere Synonyme, wie Konkurrenzausspähung, Betriebsspionage oder Werksspionage. Strafrechtlich verankert ist die Industriespionage im § 17 UWG, Verrat von Geschäfts- oder Betriebsgeheimnissen, oder im digitalen Umfeld der § 202a StGB, das Ausspähen von Daten. [3 Punkte]

Wirtschaftsspionage verfolgt das gleiche Ziel wie Industriespionage, ist aber staatlich gelenkt. [3 Punkte]



**FRAGE 27 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 03**



Systeme in einem Unternehmen werden von einer Schadsoftware über mehrere manipulierte E-Mails infiziert. Bei der Nachbearbeitung des Vorfalls wird festgestellt, dass die E-Mail in schlechtem Englisch verfasst war und von einem Ansprechpartner kam, welcher **nichts** mit dem Unternehmen zu tun hatte.

In welche strukturelle Unterart von Cyberangriffen im eigentlichen Sinn würden Sie die Attacke einordnen? Nennen und erläutern Sie zwei Gründe für Ihre Antwort.

Welche Maßnahmen können ergriffen werden, damit dies **nicht** wieder geschieht? Nennen und beschreiben Sie zwei Maßnahmen.

Welche weiteren strukturellen Unterarten gibt es? Beschreiben Sie diese.

Dies war ein ungerichteter Angriff, da das Unternehmen offensichtlich von E-Mails getroffen wurde, welche massenweise versendet werden. Das bedeutet, der Angriff wurde ungerichtet an viele potenzielle Opfer gestartet, in der Hoffnung, dass ein geringer Prozentsatz dem Angriff zum Opfer fällt. [3 Punkte]

Indizien, die auf einen ungerichteten Angriff schließen lassen, sind beispielsweise die E-Mail in einem schlechten Englisch. Dies ist ein Hinweis darauf, dass kein gezielter Angriff vorliegt.

Besonders, wenn diese E-Mails an nicht-englischsprachige Organisationen versendet wird. Weitere Hinweise darauf können fehlende Korrespondenz mit dem Absender sein. [3 Punkte] Spamfilter:

Ein Spamfilter kann massenweise versandte E-Mails über verschiedene Mechanismen herausfiltern oder diese [verdächtigen] markieren. So wird der Fokus der Mitarbeiter auf diese E- Mail gezogen oder sie erreicht ihn gar nicht.

Schulungen:

Mitarbeiter können geschult werden, wie gefälschte E-Mails aussehen, beispielsweise mit Fehlern in der Grammatik oder wenn wenig Informationen über das Thema oder den Ansprechpartner verfügbar sind.

[3 Punkte je Beispiel + Begründung]

Man spricht von zielgerichteten Angriffen, wenn sich der Täter ein bestimmtes

Opfer aussucht. Das Opfer kann dem Täter gegenüber bekannt oder unbekannt sein. Ein klassisches Beispiel für diesen Angriff ist: Herr Meier möchte seinem ehemaligen Arbeitgeber schaden, da er ihn entlassen hat. Daher schickt er seiner ehemaligen Kollegin einen Virus. Diese öffnet den Virus, der das ganze IT-Netzwerk der Firma angreift. Immer häufiger kommen skalpellartige Angriffe zum Einsatz. Diese Angriffsform setzt eine intensive Vorbereitung voraus und möchte zumeist Infrastruktur zerstören. Es werden gezielt Informationen über Infrastruktur, Organisation und Personen gesammelt. [3 Punkte je andere Unterart]



**FRAGE 35 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 03**



Als Geschäftsführer eines Maschinenbauunternehmens erfahren Sie von einer Attacke einer Ransomware auf ein ähnlich gelagertes Unternehmen. Sie fragen sich, ob Sie ausreichend geschützt sind. Nach Rückfragen beim IT-Administrator listet dieser Ihnen Ihre Sicherungsintervalle folgendermaßen auf:

Konstruktionsdaten – wöchentlich – im Safe verschlossen Lagerdatenbank – täglich – auf Serverfestplatte Kundendaten – wöchentlich – auf Serverfestplatte Buchhaltung – wöchentlich – im Safe verschlossen

Wie funktionieren aktuelle Ransomware-Angriffe? Nennen Sie drei Maßnahmen gegen solche Angriffe.

Welche Kriterien muss ein Backup als Maßnahme gegen einen Ransomware-Angriff erfüllen?

Diskutieren Sie, ob die Eigenschaften der Sicherung ein wirkungsvoller Schutz gegen Ransomware-Angriffe sind und beschrieben Sie drei Kritikpunkte.

Ransomware-Angriffe sind aktuell meist Verschlüsselungstrojaner. Die Angreifer verschlüsseln alle erreichbaren Daten und geben Schlüssel nur gegen Lösegeld heraus. [3 Punkte] Maßnahmen gegen Ransmware Angriffe sind Backups, immer aktuelle Patches und Sensibilisierung der Mitarbeiter für das Einfallstor von Ransomware: E-Mails mit schadhaftem Anhang. [3 Punkte]

Offline, vollständig und aktuell. [3 Punkte]

Dem Studenten überlassen, wichtig ist Begründung. Beispielsweise: Konstruktion wöchentlich ausreichend? (hier ist täglich notwendig!)

Lagerdaten täglich ist ausreichend, aber online Backup bringt nichts bei Ransomware! Buchhaltung wöchentlich ausreichend? (hier geht es um steuerlich relevante Daten und hohe Wiederherstellungskosten!)

[3 Punkte je Kritikpunkt + Beschreibung]



**FRAGE 38 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 04**



Auf welche Komponente weist ein offener Port für MySQL hin? Beschreiben Sie die zwei Angriffsmöglichkeiten auf diese Komponente.

MySQL ist eine Datenbank und stellt diese für andere Anwendungen zur Verfügung. Diese Datenbank enthält dann alle Daten dieser Anwendung. [2 Punkte]

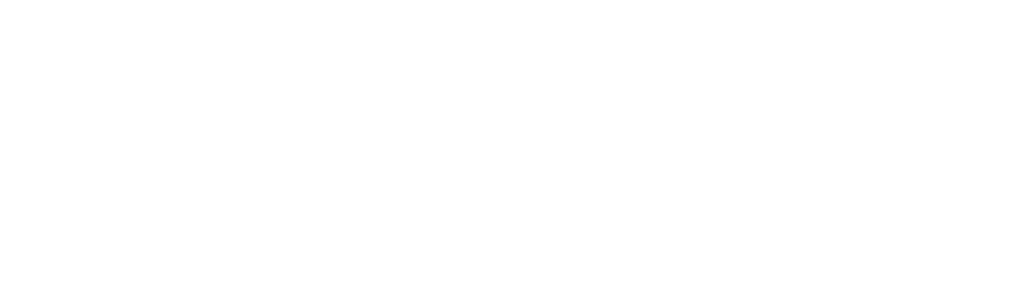
Eine Angriffsmöglichkeit, welche Schadsoftware zum Aufbau von Botnetzen oft nutzt, ist das Ausnutzen von Standardpasswörtern von Datenbanken. Dann kann der Angreifer alle Daten der Datenbank auslesen. [2 Punkte]

Eine andere Möglichkeit ist eine SQL-Injection. Hier wird Code in die Datenbank über Nutzereingaben auf einer Webseite eingeschleust, um Benutzernamen und Passwörter oder andere Daten auszulesen. [2 Punkte]



**FRAGE 40 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 04**



Der Hersteller eines Smartphones berichtet, dass die Firmware einer Vielzahl von Geräten mit einer Schwachstelle versehen ist, welche dem Angreifer erlaubt, alle Funktionen der Firmware zu kontrollieren.

Beschreiben Sie kurz, was eine Firmware ist und nennen Sie zwei Beispiele für Komponenten, welche mit Firmware ausgestattet sind.

Welchen Angriff kann ein Angreifer mit dieser Schwachstelle bezogen auf das Beispiel starten? Beschreiben Sie einen Angriff.

Firmware kommt in vielen Varianten vor und die Grenzen sind fließend. Generell ist Firmware Software, welche auf einer sehr niedrigen Ebene Funktionen von verschiedenen Hardware- Elementen zur Verfügung stellen. Auf Firmware baut dann komplexere Software, wie Betriebssysteme oder andere Anwendungssoftware, auf und nutzt die entsprechenden Funktionen der Hardware. [2 Punkte]

Konsumentenprodukte

* Hausgeräteo Multimediageräte
* Automobile
* Smartphones Computerkomponenten
* Festplatten
* Grafikkarten
* Mainboard

[1 Punkt je Beispiel; max. 2 Punkte]

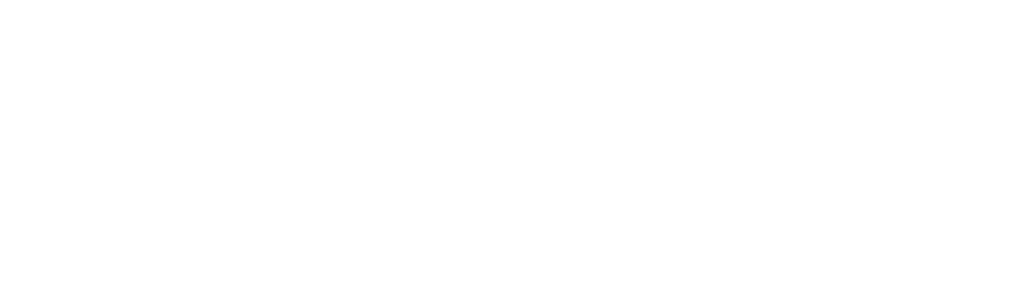
Ein beispielhafter Angriff wäre das Einschleusen von Schadcode in das Betriebssystem, da die Firmware meist das Betriebssystem erst lädt und der Angreifer dieses dann auch unter Kontrolle hat. Damit können dann Daten belauscht werden oder die Geräte inoperabel geschädigt werden. [2 Punkte]

Viele andere Beispiele sind möglich!



**FRAGE 41 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 04**



Ihre Organisation betreibt einen E-Mailserver, welcher zum öffentlichen Internet freigegeben ist. Bei einem Penetrationstest werden die TCP-Ports 22, 110 und 25 als offen angezeigt.

Erläutern Sie zuerst, welche Angriffsmöglichkeiten bei einem E-Mail-Server mit den beschriebenen Ports beachtet werden müssen.

Welcher Port wird für die E-Mail-Funktionalität **nicht** benötigt und welche Gefahr birgt dieser?

Da die Ports 110 und 25 offen sind, sind SMTP und POP3 in Verwendung. Hier kann ein Angreifer durch Fehlkonfigurationen E-Mail-Adressen abfragen. Diese Informationen können dann für Spear Phishing oder normale Phishing Attacken genutzt werden. Zusätzlich können natürlich auch E- Mail-Server Schwachstellen wie Pufferüberläufe aufweisen, sodass ein Schadcode ausgeführt werden kann. [3 Punkte]

Der Port 22 gehört zum SSH-Protokoll und wird für die Funktionalität eines E-Mail-Servers nicht benötigt. Dieses Protokoll sollte deaktiviert werden, da ein Angreifer so einen weitere Zugangsmöglichkeit hat. Hat ein Angreifer Zugang zu einem System, können SSH-Passwörter oder SSH-Keys gestohlen oder manipuliert werden. [3 Punkte]



**FRAGE 44 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 04**



Ihre Organisation betreibt einen eigenen Serverraum. Dieser wird regelmäßig nachts durch einen Dienstleister gereinigt. Der Ehepartner einer der Mitarbeiter des Dienstleister wurde letzte Woche von Ihrer Organisation entlassen und der Mitarbeiter übt Rache, indem beim Putzen ein Kabel des Coreswitches gelöst wird. Bis die Ursache gefunden ist, vergeht ein Tag. Ihr Informationssicherheitsbeauftragter ordnet dies als Angriff in der Organisationsebene ein.

Beschreiben Sie kurz, wann ein Angriff zu dieser Ebene zugeordnet wird und in welche Kategorie dieser Angriff eingeordnet wird.

Beschreiben Sie eine Maßnahme, welche diesen Vorfall verhindert hätte.

Mit Angriffen auf der Organisationsebene sind alle Angriffe gemeint, welche Regelungen einer Organisation ausnutzen oder nur durch Schwachstellen in diesen Regelungen funktionieren. Zu diesen Regelungen zählen Informationsflüsse, Rollenverteilungen, Prozesse und Aufbau- und Ablauforganisation.

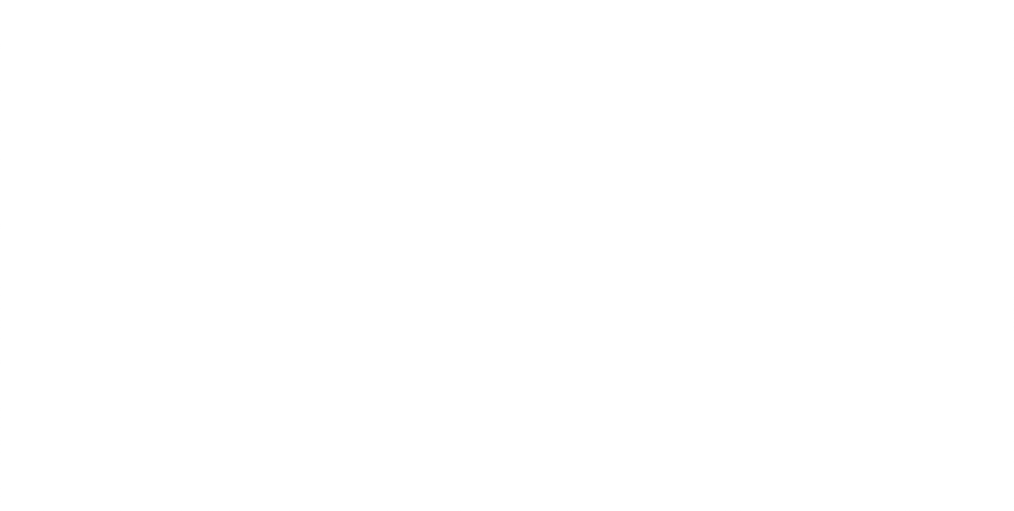
Dieser Angriff ist unter Gefährdung durch Institutionsfremde einzuordnen. [3 Punkte]

Eine Maßnahme gegen diesen Angriff wäre der ausschließliche Einsatz von eigenem Personal in den Serverräumen oder die ständige Überwachung von Institutionsfremden während des Einsatzes in Serverräumen. [3 Punkte]



**FRAGE 45 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 04**



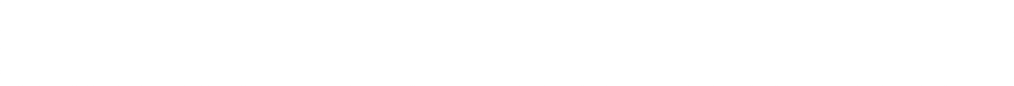
Ein Angreifer hat es über eine Schwachstelle in einer Programmierschnittstelle einer CRM-Anwendung geschafft, den internen Kommunikationsserver zu infizieren. Dieser wird für die Chatanwendung der internen Mitarbeiter verwendet. Der Angreifer hat **keine** erhöhten Rechte und kann so lediglich einige Funktionen des Systems beeinflussen. So kann der Angreifer Nachrichten zwischen Mitarbeitern mitlesen und diese auch bearbeiten.

Welche zwei Angriffsarten kann der Angreifer damit bereits ausführen? Beschreiben Sie diese kurz zusammen mit einem beispielhaften Angriffsszenario.

Das Ziel des Angreifers ist es, bezogen auf die Chatanwendung, die Position eines Man-in-the-Middle einzunehmen. Erläutern Sie zuerst, was eine Man-in-the-Middle-Attacke ist.

Welche schadhafte Funktion fehlt dem Angreifer noch auf dem infizierten System, um eine Man-in-the-Middle-Attacke auszuführen?

Wie kann der Angreifer diese Angriffsart im obigen Beispiel ausnutzen?



Beschreiben Sie zwei Beispiele.

Lauschangriffe stellen dabei die erste Art Angriff dar. In einem Netzwerk werden immer Daten zwischen den Systemen im Netzwerk ausgetauscht. Diese Daten können auf vielen verschiedenen Wegen belauscht werden. Belauschen bedeutet in diesem Fall, dass ein Angreifer diese lesen kann. Im Falle einer CRM-Anwendung könnte ein Angreier Daten über Kunden und Lieferanten. Eine kritischeres Beispiel wären Ausschreibungsunterlagen. [3 Punkte]

Einen Schritt weiter geht dann die Modifikation von Daten. Sofern ein Angreifer Zugriff auf Daten hat, kann er diese beliebig für seine Zwecke verändern. Dabei können Daten bei der Übertragung oder in gespeichertem Zustand in Datenbanken oder Dateien geändert werden. Der Angreifer hat damit die volle Kontrolle über die Daten. In einem CRM-System könnte es beispielsweise kritisch sein, wenn ein Angreifer Vertragslaufzeiten oder Konditionen verändert. [3 Punkte]

Bei einer MitM-Attacke hat der Angreifer die Möglichkeit erlangt, die Kommunikation zwischen zwei Netzwerkteilnehmern abzufangen, zu modifizieren und wieder zu versenden, sodass keiner der beiden ursprünglichen Teilnehmer diesen Angriff bemerkt. Diese Art Angriff setzt voraus, dass der Angreifer in der Lage ist, Nachrichten, welche von einem Teilnehmer abgesendet werden, an sich umzuleiten, diese zu modifizieren und dann an den anderen Teilnehmer weiterzuleiten.

Gleichzeitig muss der Angreifer in der Lage sein, beiden Teilnehmern die Identität des anderen glaubhaft zu machen, sofern eine Authentifizierung zwischen den Teilnehmern stattfindet. [3 Punkte]

Um eine MitM-Attacke durchzuführen, fehlt dem Angreifer die Möglichkeit, dem Empfänger seiner modifizierten Nachricht die Identität des originalen Absenders vorzutäuschen, also eine Spoofing- Attacke. Ohne diese Funktion wird der Empfänger die Manipulation bemerken. [3 Punkte]

Der Angreifer kann gezielt Nachrichten manipulieren, welche zum Beispiel Bankverbindungen enthalten, sodass Transaktionen auf sein Konto überwiesen werden. Dadurch entsteht ihm ein direkter finanzieller Vorteil. [3 Punkte]

Der Angreifer kann aber auch im Namen eines administrativen Benutzers den User Help Desk nach einem Link zum Zurücksetzen des Passworts fragen und so den Zugriff auf einen Account mit erhöhten Rechten erlangen. Dies erlaubt es dem Angreifer, auf weitere Systeme zuzugreifen. [3 Punkte]



**FRAGE 47 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F1/Lektion 04**



Als Informationssicherheitsbeauftragter informiert Sie der Projektleiter für die Webseite Ihrer Organisation darüber, dass auf der Webseite eine Schwachstelle existiert, welche es einem Angreifer erlaubt, eine Reverse Shell zu erzeugen, um so beliebige Befehle auszuführen. Er beruhigt Sie aber direkt, dass diese Shell nur mit den niedrigen Rechten des Webseiten- Benutzers (www-data) aufgebaut wird und somit keinerlei Gefahr besteht.

Erläutern Sie in diesem Zusammenhang, was Rechtetrennung in Bezug auf moderne Betriebssysteme ist und was eine privilege escalation ist.

Beschreiben Sie den Zusammenhang zwischen diesen beiden Begriffen in Bezug auf Computerkriminalität.

Erläutern Sie an dem gegebenen Beispiel zwei Gründe, warum die Aussage des Projektleiters bezogen auf die Gefahrensituation **nicht** richtig ist und skizzieren Sie das Vorgehen eines Angreifers, welcher diese Lücke ausnutzt.

Moderne Betriebssysteme haben zusätzlich eine strikte Rechtetrennung. Dies bedeutet, die Prozesse des Betriebssystems laufen mit höheren Rechten als die Prozesse der Benutzer. Daraus folgt, dass Benutzer bestimmte Bereiche des Speichers nicht lesen oder verändern können, bestimmte Netzwerkschnittstellen nicht nutzen können oder einige Befehle nicht

ausführen können. Dabei ist es durchaus möglich, dass ein Prozess während seiner Ausführung zwischen verschieden hohen Rechten springt. [3 Punkte]

Das Ziel eines Angreifers ist es allerdings meist, aus der anfangs infizierten Anwendung auszubrechen. Dies wird unter dem Begriff privilege escalation zusammengefasst. Dies bedeutet, dass ein Angreifer die Möglichkeit hat, Prozesse mit erhöhten Rechten zu kontrollieren oder zu starten, sodass dieser alle Funktionen des Betriebssystems nutzen kann, um zum Beispiel alle Netzwerkschnittstellen für seine Zwecke nutzen zu können. [3 Punkte]

Erlangt ein Angreifer also die Kontrolle über einen normalen Benutzeraccount ohne erhöhte Rechte liegt das Ziel meist darin, eine privilege escalation durchzuführen. Dies liegt in der Rechtetrennung von Betriebssystemen begründet, denn mit eingeschränkten Rechten kann ein Angreifer nicht auf alle Dateien zugreifen und alle Funktionen des Systems nutzen. [3 Punkte]

Der Projektleiter hat aus mehreren Gründen Unrecht. Es ist zwar korrekt, dass der Benutzer www- data nur eingeschränkte Rechte eingeräumt bekommen hat, aber selbst eine Reverse Shell mit eingeschränkten Rechten kann großen Schaden verursachen. So kann ein Angreifer den Quellcode der Webseite auslesen oder u. U. Datenbanken auslesen. [3 Punkte]

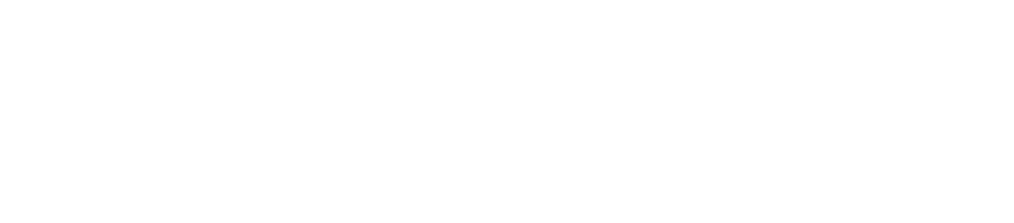
Weiterhin dient die Reverse Shell als www-data aber auch als Mittel, um eine privilege escalation durchführen zu können. Sofern auf dem Webserver eine Schwachstelle oder Fehlkonfiguration vorliegt, welche es dem Angreifer erlaubt, erhöhte Rechte zu erlangen, kann er dieses über die Shell als www-data ausnutzen. Damit ist die Schwachstelle auf der Webseite nur das erste Glied in der Kette und damit wesentlich gefährlicher als dargestellt. [3 Punkte]

Ein Angreifer würde die Schwachstelle ausnutzen und um Befehle als www-data ausführen zu können. Nachdem er eine Möglichkeit gefunden hat, seine Rechte auf dem System zu erweitern, könnte er den Code der Webseite verändern und der Organisation so erheblichen finanziellen und reputationsbezogen Schaden verursachen. [3 Punkte]



**FRAGE 49 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 05**



Nach einem schweren Sicherheitsvorfall in einer Organisation wird ein IT- forensischer Dienstleister beauftragt, welcher ein Meeting einberufen hat. Hier wird nebenbei erwähnt, dass auf eine Live-Forensik verzichtet wird. Beschreiben Sie den Begriff Live-Forensik in Bezug auf IT-Forensik und erläutern Sie zwei Vorteile dieser Vorgehensweise.

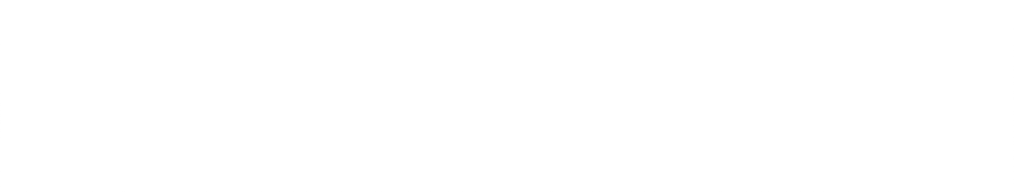
Eine Online- oder Live-Forensik wird am laufenden System durchgeführt. Das System kann also in diesem Moment noch unter dem Einfluss eines Angriffs stehen. Damit sind also flüchtige Daten, wie Prozesslisten oder der Arbeitsspeicher, auslesbar. [3 Punkte]

Dann könnten Daten und Beweise am infizierten System gesammelt werden. Dies hat den Vorteil, dass flüchtige Daten, wie der Inhalt des Arbeitsspeichers oder die aktuell aktiven Netzwerkverbindungen, analysiert werden können. Diese Informationen können sehr wertvoll sein und bei der offline-Analyse bereits verloren sein. [3 Punkte]



**FRAGE 52 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 05**



Beschreiben Sie, was Bifragmented file carving ist und worin der Unterschied zum normalen file carving liegt.

Gibt es Daten, welche mit dem Bifragmented file carving **nicht**

wiederhergestellt werden können?

Da 97 % aller Dateien entweder nicht-fragmentiert oder bi-fragmentiert, also in zwei Teile zerlegt, sind, wird beim Bifragment file carving die Lücke zwischen dem Teil einer Datei mit dem Marker für den header und dem Teil mit dem footer gesucht. Mit diesen Mitteln können Dateien nur anhand der Binärstruktur wiederhergestellt werden. [3 Punkte]

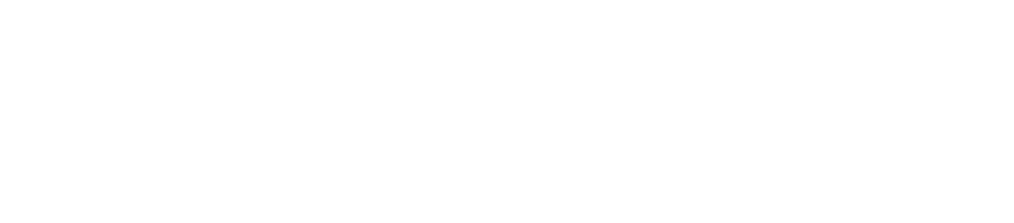
Beim normalen file carving werden nur Daten gefunden, welche zusammenhängend auf dem Datenträger gespeichert sind. [2 Punkte]

Ja, Daten welche über drei oder mehr Teile verteilt sind. [1 Punkt]



**FRAGE 45 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 05**



Sie analysieren eine mittelgroße IT-Landschaft nach einem Angriff inkl. Cloud-Anbindungen der angegriffenen Organisation. Es existieren zusätzlich strenge Vorgaben des Betriebsrats zur Verarbeitung von Mitarbeiterdaten.

Welche Anforderungen bzgl. der rechtlichen Grenzen müssen Sie bei dieser IT-forensischen Untersuchung beachten?

Bei der Analyse der Cloud-Infrastrukturen muss darauf geachtet werden, dass nur auf Systemen der beauftragenden Organisation gearbeitet wird. Es dürfen keine Daten gesammelt oder analysiert werden, welche anderen Organisationen gehören. [3 Punkte]

Außerdem müssen bei den internen Daten Aspekte des Datenschutzes beachtet werden. So müssen gesammelte Daten anonymisiert werden, wenn Daten der internen Mitarbeiter gesammelt werden. Generell gelten die Grundsätze der Datensparsamkeit und Datenvermeidung. [3 Punkte]



**FRAGE 46 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 05**



Sie arbeiten bei einem Spezialisten für Schadsoftwareanalyse und haben gerade ein neuartiges Root-Kit zur Analyse bekommen. Die Signatur in Form einer Prüfsumme ist bisher unbekannt in den Datenbanken, aber die Prozessaufrufe erinnern stark an eine andere Schadsoftware.

Was ist eine Signatur bezogen auf Schadsoftware? Beschreiben Sie dies und erläutern Sie die Probleme mit Signaturen zur Schadsoftwareerkennung.

Beschreiben Sie anhand des Beispiels, wie die Schadsoftware sonst noch eingruppiert werden kann.

Wenn eine neue Schadsoftware gefunden wurde, wird die Zeichenkette aus Bytes, welche die ausführbare Datei repräsentiert, in eine Datenbank aufgenommen. Dies ist in diesem Fall die Signatur. Signaturen können auch über Prüfsummen erzeugt werden. [2 Punkte] Schadprogramme können die Fähigkeit besitzen, ihre Signatur zu verändern. Dies wird Polymorphismus genannt. Der Abgleich mit bekannten Schadsoftwareproben über die Signatur wird damit stark erschwert. [2 Punkte]

Über andere Merkmale, wie beispielsweise die Prozessaufrufe, welche eine Schadsoftware erzeugt, kann diese in Familien eingruppiert werden. Da eine Schadsoftware diese Merkmale nur durch substantielle Änderungen am Code verändern kann, kann dies durch Polymorphismus nicht durchgeführt werden. Dadurch sind diese Merkmale weniger anfällig gegen Polymorphismen als eine Signatur. [2 Punkte]



**FRAGE 57 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 05**



Sie sind der einzige IT-Administrator eines Organisationsnetzwerks, welches den Mitarbeitern und Maschinen hauptsächlich Produktionsdaten zur Verfügung stellt und aktuell wird die Nutzung eines neuen Virenschutzkonzepts diskutiert. Dabei werden keine personenbezogenen Daten und keine vertraulichen Informationen verarbeitet.

Erläutern Sie zuerst die drei Arten der Detektion von Schadsoftware. Erläutern Sie anhand des Beispiels je einen Vor- und Nachteil für jede der verschiedenen Arten.

Beschreiben Sie einen Angriff, welcher von **keiner** dieser drei Methoden erfasst werden würde.

Eines der ersten Verfahren zu Detektion von Schadsoftware war die Signatur-basierte Detektion. Wenn eine neue Schadsoftware gefunden wurde, wird die Zeichenkette aus Bytes, welche die ausführbare Datei repräsentiert, in eine Datenbank aufgenommen. Dies ist in diesem Fall die Signatur. Wird zukünftig eine ausführbare Datei mit der gleichen Zeichenkette gefunden, wird dies als Schadsoftware erkannt und entsprechende Gegenmaßnahmen eingeleitet. [3 Punkte]

Die Heuristik-basierte Detektion bietet eine Detektionsmöglichkeit, bevor die Signaturen neuer Schadsoftware verteilt sind. Mithilfe von Heuristiken wird versucht, anhand des Systemverhaltens ein schadhaftes Programm zu identifizieren. Dabei ist kein Wissen über die Schadsoftware an sich nötig, aber Wissen über Schwachstellen und Angriffsmöglichkeiten. [3 Punkte]

Die Verhaltens-basierte Detektion von Schadsoftware ähnelt der vorherigen Variante, wobei hier nicht das System betrachtet wird auf dem das Anti-Virenprogramm läuft, sondern direkt das Verhalten der Schadsoftware untersucht wird. Sobald ein schadhaftes Verhalten erkannt wird, wird die Ausführung gestoppt. [3 Punkte]

Die Signatur-basierte Variante erkennt zuverlässig bekannte Schadprogramme. Da bekannte Schadprogramme meist bei massenhaften Kampagnen genutzt werden, bieten diese hier einen guten Schutz solange die eigene Organisation nicht das erste Opfer ist. Da die verarbeiteten Daten unkritisch sind, werden die meisten Angriffe massenhafte Kampagnen sein. [3 Punkte] Die Heuristik- und Verhaltens-basierten Detektionen erkennen auch unbekannte Schadsoftware anhand ihres Verhaltens oder anderer Merkmale. Diese sind also für neue und komplexere Bedrohungen geeignet. Der Nachteil liegt im hohen Anteil falsch-positiver Meldungen, die viel Arbeit verursachen. In einer kleinen IT mit nicht sehr kritischen Daten ist diese Art der Detektion weniger sinnvoll. Idealerweise sollten alle Varianten sinnvoll kombiniert werden. [3 Punkte]

Ein Angriff, welcher nicht von diesen drei Arten entdeckt werden würde, wäre ein Social Engineering-Angriff auf ein Administratorkonto, sodass dies von einem Angreifer kontrolliert wird. Hier kommt keine Schadsoftware zum Einsatz, sodass Signatur-basierte Detektionen nicht anschlagen können. Aus diesem Grund kann nur das Verhalten, welches der Angreifer mit dem administrativen Account an den Tag legt, detektiert werden. Sofern der Angreifer keine auffälligen Aktivitäten erzeugt, wird der Angriff nicht von Verhaltens- oder Heuristik-basierten Detektionen erfasst werden. [3 Punkte]

Sie sind Spezialist für Datenrettung und haben täglich Aufträge von verschiedensten Firmen und Privatpersonen.

Erläutern Sie zu den unteren Beispielen, wo die Daten auf dem Datenträger vorliegen inkl. eventueller Metadaten und beschreiben und begründen Sie, wie Sie vorgehen würden, um die Daten zu retten.

1. Eine verzweifelte, ältere Dame ruft an und sagt, Sie hätte auf die falschen Tasten gedrückt und die Bildersammlung ihres Enkels sei nicht mehr dort, wo sie vorher war.
2. Ein Student meldet sich bei Ihnen, weil er versehentlich anstatt einer veralteten die neueste Version seiner Masterarbeit gelöscht hat und auch den Papierkorb versehentlich geleert hat.
3. Eine Organisation wendet sich nach einem Cyberangriff an Sie, bei dem der Angreifer seine Spuren verwischen wollte, indem er die gesamte NTFS-Dateistruktur eines Servers gelöscht hat. Die Organisation will Hinweise auf den Kriminellen auf der Festplatte des Servers ausfindig machen.
4. Eine Organisation wendet sich an Sie, weil ein Batchskript des Storage-Area-Network-Administrators versehentlich zwei Serverfestplatten komplett mit 0 überschrieben hat.
5. Die Daten liegen vermutlich noch im Papierkorb, da bei modernen Betriebssystemen Dateien immer beim Löschen in den Papierkorb gelangen, um dem Benutzer die Möglichkeit zu geben, diese wiederherzustellen. [3 Punkte]

Die Daten sind hier noch auf dem Datenträger vorhanden und in der Dateisystemstruktur vorhanden. Nur der Verweis zu den Daten ist nicht mehr im ursprünglichen Verzeichnis, sondern im Papierkorb. Die Daten können über die Funktion des Papierkorb wiederhergestellt werden. [3 Punkte]

1. Die Daten sind gelöscht und aus dem Papierkorb gelöscht, sodass einige Daten in der Dateistruktur gelöscht sind, aber einige andere noch vorhanden sind. [2 Punkte]

Hier kann eine Wiederherstellung über die Dateisystemstruktur erfolgen, da noch Hinweise zur Datei vorhanden sind. Dadurch kann die Datei wiederhergestellt werden. Dafür existieren spezielle Tools. [2 Punkte]

1. Die Dateisystemstruktur ist demnach komplett zerstört, d. h. dort liegen keine Daten mehr. Aber die Daten sind trotzdem noch irgendwo auf dem Datenträger vorhanden. [2 Punkte] Um diese Daten zu finden, müssen Techniken des file carving eingesetzt werden. Diese suchen nach bestimmten headern und footern, um die Dateien im Byte-Code auf dem Datenträger zu finden. [2 Punkte]
2. Da die gesamte Festplatte mit 0 überschrieben wurde, sind die gesuchten Daten weder in der Dateisystemstruktur, noch auf dem Datenträger irgendwo zu finden. [2 Punkte]

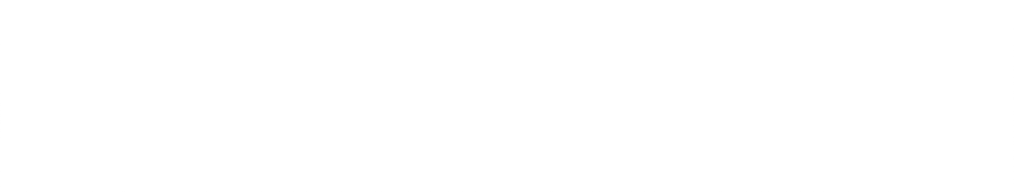
Hier hilft nur die Suche nach einem Backup, denn die Daten sind unwiderruflich verloren (wipe-out). [2 Punkte]

[Die Aufteilung, welche Teil 3 Punkte und welcher 2 Punkte bringt kann variieren, je nachdem wo der Student generelle Erläuterung zur Dateisystemstruktur unterbringt. Diese sind notwendig für das Lösen der Aufgabe, aber werden nur in einem Teil benötigt.]



**FRAGE 61 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 06**



Ihre Organisation rüstet die Serverschränke nach Anforderungen aus dem ISMS mit brand- und einbruchsicheren Türen aus.

Erläutern Sie mithilfe des oberen Beispiels, was eine präventive Maßnahme ist. Nennen Sie außerdem beispielhaft drei weitere präventive Maßnahmen.

Präventive Maßnahmen sind Maßnahmen, welche vor Eintreten eines Sicherheitsvorfalls ergriffen werden. Das Ziel liegt darin, den Sicherheitsvorfall zu verhindern, die Eintrittswahrscheinlichkeit zu senken oder die Konsequenzen des Vorfalls zu verringern. Der Serverraum wird in diesem Fall vor einem Einbruch oder einem Brand präventiv abgesichert. [3 Punkte]

Beispiele [1 Punkte pro Bsp.; max. 3 Pkt.] Passwortschutz

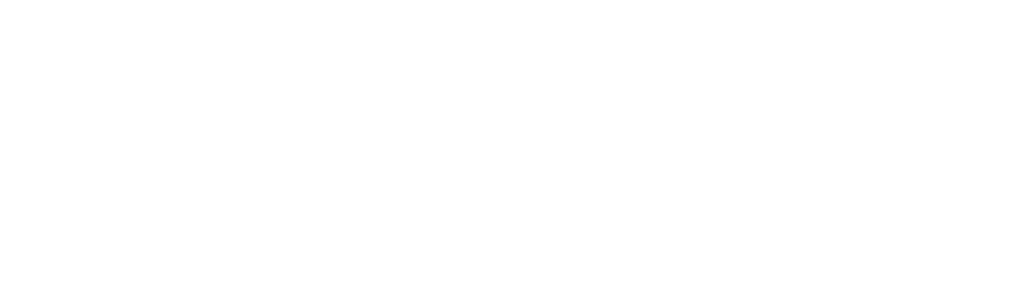
Wachschutz

Perimeterschutz (Zaun) ums Gebäude



**FRAGE 63 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 06**



In Ihrer Organisation werden eine Vielzahl verschiedener Anwendungen genutzt und Mitarbeiter beschweren sich mehrfach, dass das Merken einer so großen Anzahl von Passwörtern unmöglich ist. Ihre Idee, um die Zahl der Passwörter zu reduzieren, ist SSO.

Was bedeutet SSO und welchen Vorteil hat es für die Passwortvielfalt? Beschreiben Sie ein Beispiel, bei dem SSO helfen kann, die Passwortvielfalt zu reduzieren.

SSO steht für Single-Sign-On und beschreibt die Möglichkeit, sich an weiteren Diensten anzumelden, sobald ein Benutzer einmal authentifiziert ist. Die Authentifizierung muss also nicht für jeden Dienst einzeln durchgeführt werden. [2 Punkte]

Der Vorteil ist, dass ein Benutzer sich einmal anmeldet und bei weiteren Diensten keine Anmeldung notwendig ist, da die Authentifizierung weitergenutzt wird und so das Passwort nicht erneut eingegeben werden muss. Ein Benutzer muss sich so nicht mehrere Zugangsdaten merken. So können komplexere Passwortregeln erzwungen werden oder biometrische Authentifizierungen genutzt werden. Außerdem ist der Passwortwechsel erleichtert. [2 Punkte] Beispielsweise kann der Login in das Windowsbetriebssystem für weitere Dienste genutzt werden, sodass ein Benutzer nur am Morgen sein Windows-Passwort eingibt und dann alle weiteren Dienste, wie Webanwendungen oder Warenwirtschaftssysteme, auf diese Authentifizierung zurückgreifen. [2 Punkte]



**FRAGE 65 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 06**



In Ihrer Organisation wird gerade Microsoft 365 eingeführt und es wird damit erstmals ein Zugriff auf Unternehmensdaten außerhalb des Organisationsnetzwerks ermöglicht. Aktuell werden hauptsächlich der Benutzername und ein Passwort zum Zugriff auf Anwendungen genutzt. Ihr Informationssicherheitsbeauftragter schlägt für den Zugang zu Microsoft 365 MFA vor.

Erläutern Sie zuerst, was MFA bedeutet.

Beschreiben Sie, ob im oberen Beispiel MFA angewendet werden soll. Begründen Sie Ihre Antwort.

MFA: Multi-Faktor-Authentifizierung bezieht sich dem Namen nach nur auf Authentifizierung. Mit MFA wird die Authentifizierung mit mehreren Faktoren durchgeführt, d.h. statt nur ein Passwort zu nutzen, um einen Benutzer zu authentifizieren, werden weitere Merkmale benötigt. Dabei kann zum Beispiel der Besitz eines persönlichen Gegenstandes, wie des eigenen Smartphones oder eines Security-Tokens als weiteres Merkmal hinzukommen. [3 Punkte]

In diesem Beispiel sollte für den Zugang zu Microsoft 365 MFA genutzt werden, aber nur, wenn der Zugriff außerhalb des Organisationsnetzwerkes erfolgt, da ein Angreifer eine Authentifizierung außerhalb des Netzwerks leicht selber anstoßen kann und ohne MFA – also nur mit Benutzername/Passwort – eine wesentlich größere Chance hat, Daten der Organisation abzugreifen. [3 Punkte]



**FRAGE 59 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 06**



In Ihrer Organisation wird gerade ein Collaboration-Tool zum gemeinsamen Arbeiten eingeführt und es wird damit erstmals ein Zugriff auf Unternehmensdaten von außerhalb des Organisationsnetzwerks möglich.

Aktuell werden hauptsächlich Benutzername und Passwort zum Zugriff auf Anwendungen genutzt. Ihr Informationssicherheitsbeauftragter schlägt für den Zugang zum Collaboration-Tool MFA vor.

Erläutern Sie zuerst, was MFA bedeutet.

Beschreiben Sie, ob im oberen Beispiel MFA angewendet werden soll. Begründen Sie Ihre Antwort.

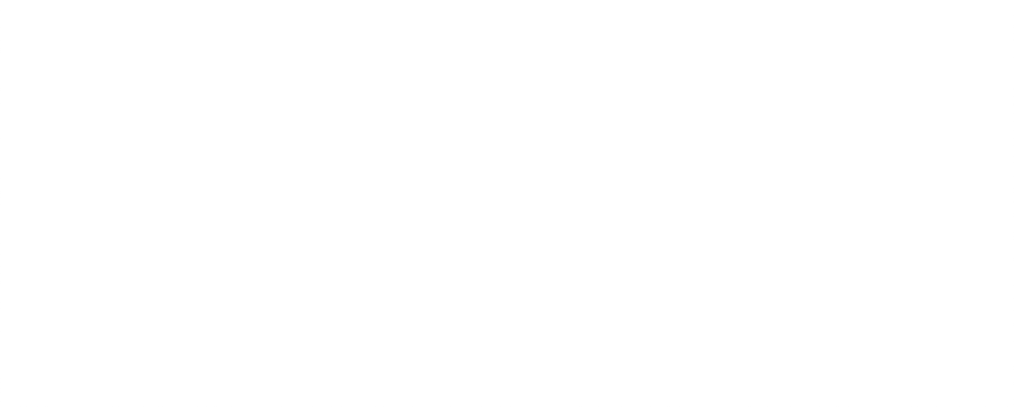
MFA: Multi-Faktor-Authentifizierung bezieht sich dem Namen nach nur auf Authentifizierung. Mit MFA wird die Authentifizierung mit mehreren Faktoren durchgeführt, d.h. statt nur ein Passwort zu nutzen, um einen Benutzer zu authentifizieren, werden weitere Merkmale benötigt. Dabei kann zum Beispiel der Besitz eines persönlichen Gegenstandes, wie des eigenen Smartphones oder eines Security-Tokens als weiteres Merkmal hinzukommen. [3 Punkte]

In diesem Beispiel sollte für den Zugang zum Collaboration-Tool MFA genutzt werden, aber nur wenn der Zugriff außerhalb des Organisationsnetzwerkes erfolgt, da ein Angreifer eine Authentifizierung außerhalb des Netzwerks leicht selber anstoßen kann und ohne MFA - also nur mit Benutzername/Passwort - eine wesentlich größere Chance hat Daten der Organisation abzugreifen. [3 Punkte]



**FRAGE 70 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 06**



Ihre Organisation besteht aus mehreren Standorten und Mitarbeiter haben die Möglichkeit, im Homeoffice zu arbeiten. Diese Anbindungen werden per VPN umgesetzt. Dieser VPN wird über eine Smartcard, welche in die Laptops der Mitarbeiter eingelegt wird, aktiviert. Nach einem Vorfall, bei dem ein Angreifer – unter der Vorgabe, ein Supportmitarbeiter zu sein – einen Mitarbeiter zur Herausgabe der Smartcard verleitet hat, werden nun großflächig Schulungs- und Sensibilisierungsmaßnahmen für alle Mitarbeiter angesetzt.

Beschreiben Sie anhand des Beispiels, welche acht Ziele ein solches Schulungs- und Sensibilisierungsprogramm verfolgt.

Welche weiteren Benutzergruppen sollten speziell geschult werden?

[2 Punkte je Aspekt + Anwendung des Beispiels] Erzeugen von Sicherheitsbewusstsein

Das Bewusstsein, dass die Smartcard extrem wichtig ist, muss geschaffen werden. Kenntnisse zu Regelungen der Informationssicherheit vermitteln

Die Regelung, dass betriebliche Gegenstände (Smartcard) niemals rausgegeben werden dürfen, muss beachtet werden.

Sensibilisierung zu Maßnahmen der Informationssicherheit erzeugen

Notwendigkeit des VPN begründen, um Mitarbeitern klar zu machen, dass dies notwendig ist. Schulung zu Sicherheitsfunktionalitäten

Schulung zur groben Funktionsweise des VPN und der Smartcard. Was passiert, wenn ein Angreifer Zugang erhält? Erkennen und Melden von Sicherheitsvorfällen

Wie hätte der Mitarbeiter den Vorfall korrekt melden können? Beachtung von Sicherungsmaßnahmen und sorgsamer Umgang mit Informationen

Smartcards enthalten kritische Informationen und mit diesen muss sorgsam umgegangen werden.

Sensibilisierung zu Social Engineering

Sensibilisierung dazu, dass Supportmitarbeiter niemals Passwörter oder Smartcards verlangen werden.

Wandel der Sicherheitskultur

Generell muss die Sicherheitskultur verändert werden. Sicherheitsmaßnahmen sollen nicht als störend empfunden werden, sondern aktiv von den Mitarbeitern mitgestaltet werden.

Neben den Mitarbeitern müssen außerdem die Administratoren spezielle Schulungen erhalten, damit diese Anwendungen, wie einen VPN, korrekt und sicher konfigurieren. [2 Punkte]





**FRAGE 72 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 06**



Sie sind Informationssicherheitsbeauftragter eines mittelgroßen Maschinenbauers und sollen ein Berechtigungskonzept erstellen. Dabei sind folgende Usergruppen und Zugriffe auf Freigaben im Netzwerk interessant: Alle Benutzer – beinhaltet alle Mitarbeiter – Freigabe: Dienstreiseplan Konstrukteure – beinhaltet alle Mitarbeiter der Konstruktion – Freigabe: Konstruktionspläne

Buchhaltung – beinhaltet alle Mitarbeiter der Lohn- und Finanzbuchhaltung

– Freigabe: Mitarbeiterbezüge

Erläutern Sie im ersten Schritt die Begriffe Authentifizierung, Autorisierung und Zugangsberechtigung.

Beschreiben Sie, mit welchen Methoden Sie die Authentifizierung, Autorisierung und Zugangsberechtigung für die oben genannten Benutzergruppen und Freigaben realisieren würden. Gehen Sie dabei auf den Schutzbedarf der jeweiligen Freigaben ein und erläutern Sie je zwei Maßnahmen, um diesen Schutzbedarf zu erfüllen.

Die Authentifizierung oder Authentisierung beschreibt die Überprüfung der Authentizität, also ob der Kommunikationspartner der ist, der dieser vorgibt zu sein. Authentische Informationen sind dabei von der angegebenen Quelle erstellt oder versandt worden. Authentifizierung wird meist über Passworteingaben, Chipkarten oder biometrische Merkmale sichergestellt. [3 Punkte] Autorisierung beschreibt die Überprüfung, ob eine Person, Hardwarekomponente oder Anwendung berechtigt ist, eine bestimmte Aktion durchzuführen. Dies betrifft also explizit nicht nur Personen, sondern auch die Kommunikation zwischen Anwendungen oder IT-Komponenten. [3 Punkte]

Eine Zugangsberechtigung erlaubt einer Person, einer Komponente oder einem Dienst, eine bestimmte Ressource zu nutzen. Damit kombiniert die Zugangsberechtigung die Vorgänge Authentifizierung und Autorisierung. [3 Punkte]

Alle Benutzer – beinhaltet alle Mitarbeiter – Freigabe: Dienstreiseplan

Da diese Benutzergruppe alle Benutzer betrifft und der Dienstreiseplan für alle Nutzer öffentlich ist, liegt hier ein normaler Schutzbedarf vor. Die Authentifizierung kann also über Benutzername und Passwort erfolgen, welche jedem Mitarbeiter zu Beginn seiner Tätigkeit zugeteilt wird. Die Autorisierung erfolgt dann über die autorisierte Benutzerkennung und es sollte die SSO mit dem Login des Betriebssystems genutzt werden. Es sollte ein Passwortablauf definiert sein. [3 Punkte] Konstrukteure – beinhaltet alle Mitarbeiter der Konstruktion – Freigabe:

Konstruktionspläne:

Die Konstruktionspläne sind kritische Daten für das Unternehmen, da eine Industriespionage hier verheerend wäre. Aus diesem Grund sollte hier ein zweiter Faktor zum Einsatz kommen.

Entweder die IP-Adresse des PCs des Mitarbeiters, One-Time-Passwörter über SMS oder andere Token werden als zweiter Faktor genutzt. Erst auf dieser Grundlage sollte die Autorisierung zur Freigabe erfolgen. [3 Punkte]

Buchhaltung – beinhaltet alle Mitarbeiter der Lohn- und Finanzbuchhaltung – Freigabe:

Mitarbeiterbezüge:

Auch diese Freigabe ist mit einem hohen Schutzbedarf zu versehen. Hier kann ein MFA- Verfahren zum Einsatz kommen oder eine Verschlüsselung der Freigabe, sodass nur mit einem vorher verteilten Schlüssel oder Benutzerzertifikat der Inhalt der Freigabe entschlüsselt werden kann. [3 Punkte]

Die Maßnahmen zur Absicherung der Shares sind dem Studenten überlassen. Die Begründung ist wichtig!



**FRAGE 74 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 07**



Sie arbeiten in einem Handwerksbetrieb mit 20 Mitarbeitern und einer kleinen IT-Infrastruktur als IT-Admin. Sie entdecken den Befall einer der Arbeitsplatzrechner mit einer Ransomware und fangen direkt an, Informationen im Netzwerk zu sammeln.

Welche Schritte haben Sie, angelehnt an die organisatorischen Empfehlungen der Allianz für Cybersicherheit, ausgelassen und welche Konsequenzen ergeben sich daraus? Beschreiben Sie diese zwei Schritte kurz.

Nennen und erläutern Sie einen Schritt, welcher nach der erwähnten Sammlung von Informationen folgt.

Ausgelassen:

Einrichtung eines Krisenstabes: Aktuell trifft der IT-Admin alle relevanten Entscheidungen. Diese Kompetenz sollte auf den Krisenstab umgelegt werden. [2 Punkte]

Interne Kommunikation: Die internen Entscheidungsträger wissen nichts von der Infektion und weitreichende Folgen könnten übersehen werden [2 Punkte]

weiterer Schritt:

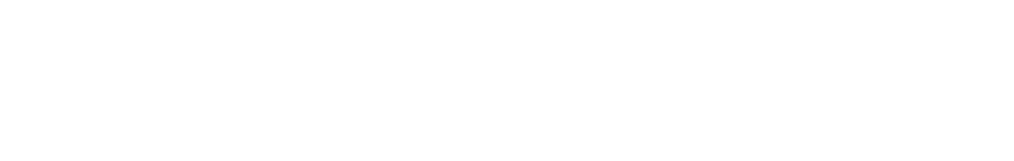
externe Unterstützung:

externe IT-Berater oder IT-Forensiker können dazu gezogen werden, um den Vorfall zu bereinigen und den Schaden zu beheben. [2 Punkte]



**FRAGE 76 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 07**



Wie wird ein Angriffsgraph, bezogen auf Netzwerkangriffe und Computerkriminalität, aufgebaut? Beschreiben Sie den Nutzen eines solchen Angriffsgraphen.

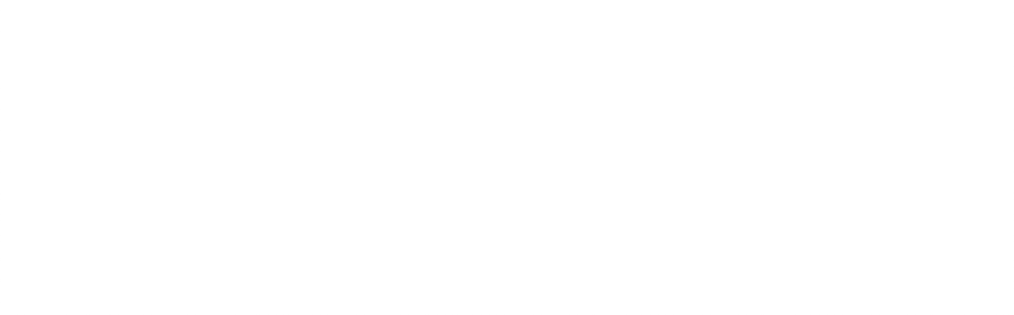
Dafür werden, basierend auf der eigenen Netzwerkstruktur, Angriffsmöglichkeiten in Form eines baumartigen Graphen erstellt und ein Simulationsmodell auf diese Struktur angewendet. Dieser Graph stellt alle Möglichkeiten dar, wie ein Angreifer in das Netzwerk einbrechen, sich verbreiten und kompletten Zugriff erhalten kann. [3 Punkte]

Damit kann dann beispielsweise simuliert werden, welche Auswirkungen eine Infektion des Servers X für die Clientgruppe A und den Netzwerkabschnitt B hätte. Neben der Simulation können solche Systeme auch mit (nahezu) Echtzeitdaten gefüttert werden, sodass bei einem Angriff direkt auch das Schadensausmaß berechnet werden kann. [3 Punkte]



**FRAGE 77 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 07**



Was ist KRITIS und welche Organisationen werden unter diesem Begriff zusammengefasst?

Nennen Sie ein Beispiel für eine KRITIS-Organisation aus einem der folgenden Bereiche und erläutern Sie, warum dieses zu dieser Kategorie zählt:

Medien und Kultur; Wasser;

Finanz- und Versicherungswesen.

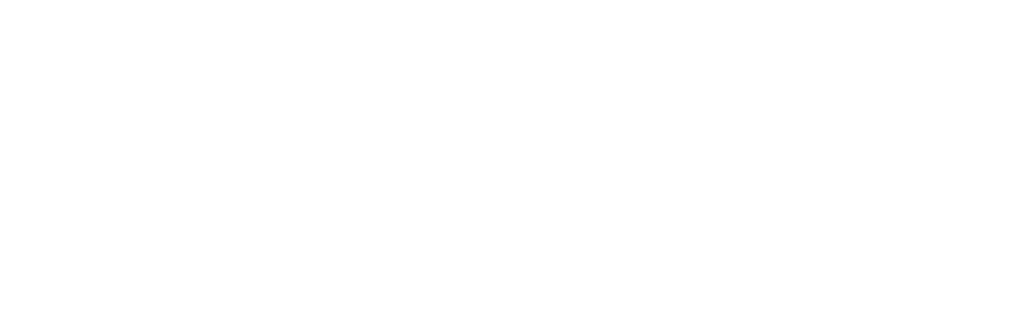
Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (auch IT- Sicherheitsgesetz oder IT-SiG) verpflichtet der Gesetzgeber Betreiber sogenannter kritischer Infrastruktur dazu, Mindeststandards in Bezug auf IT-Sicherheit umzusetzen. Bestimmte Sektoren, wie Ernährung, Wasser oder Finanzwesen gehören zu KRITIS. Für jeden Sektor gibt es Schwellwerte, wann ein Unternehmen zur kritischen Infrastruktur gehört. [3 Punkte]

Eine Bank, wie die Commerzbank, gehört zu KRITIS, da hier großen Mengen Geld täglich elektronisch bearbeitet werden und die Versorgung mit Girokonten und dem Geld vieler Bürger gewährleistet werden muss. [3 Punkte] Andere Beispiele wären öffentlicher Rundfunk (Medien) oder lokaler Wasserversorger (Wasser).



**FRAGE 80 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 07**



Was ist KRITIS und welche Organisationen werden unter diesem Begriff zusammengefasst?

Nennen Sie ein Beispiel für eine KRITIS-Organisation aus einem der folgenden Bereiche und erläutern Sie, warum dieses zu dieser Kategorie zählt:

Gesundheit; IT und ITK;

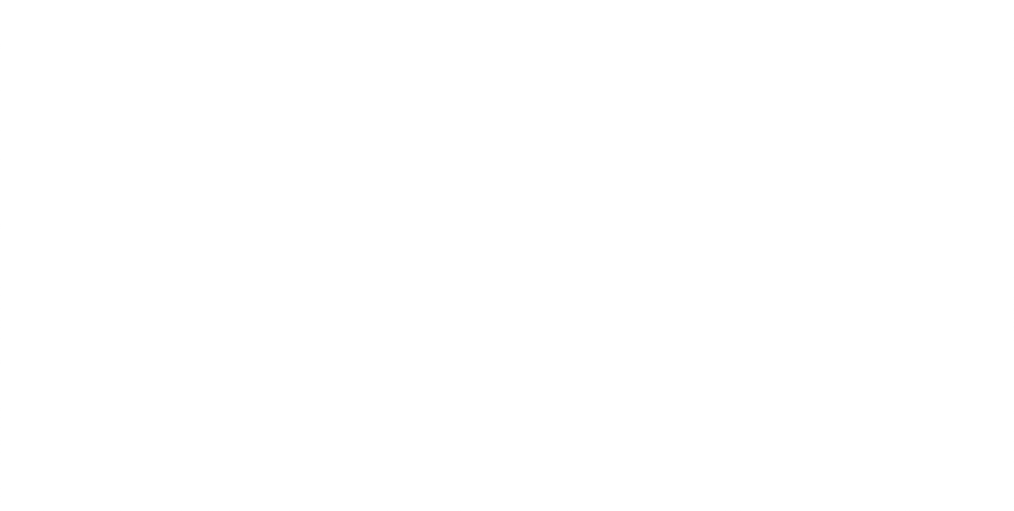
Transport und Verkehr.

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (auch IT- Sicherheitsgesetz oder IT-SiG) verpflichtet der Gesetzgeber Betreiber sogenannter kritischer Infrastruktur dazu, Mindeststandards in Bezug auf IT-Sicherheit umzusetzen. Bestimmte Sektoren, wie Ernährung, Wasser oder Finanzwesen gehören zu KRITIS. Für jeden Sektor gibt es Schwellwerte, wann ein Unternehmen zur kritischen Infrastruktur gehört. [3 Punkte] Krankenhäuser, welche eine bestimmte Anzahl Betten besitzen, gehören zu KRITIS, denn wenn die Infrastruktur dieses Krankenhauses erfolgreich angegriffen wird und die medizinische Versorgung von tausenden Menschen gefährdet ist, hätte dies katastrophale Folgen. [3 Punkte] Andere Beispiele wären Bundesnetz - Netz des Bundestages (IT) oder Schenker (Transport).



**FRAGE 82 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 07**



Erläutern Sie, was Threat Intelligence im Zusammenhang mit Computerkriminalität bedeutet.

Welche Arten von Threat Intelligence gibt es?

Nennen Sie vier Arten und erläutern Sie in einem Satz, welche Informationen in diese Art eingruppiert werden.

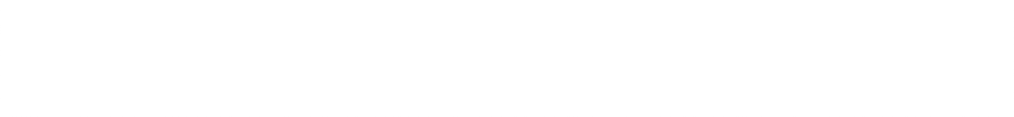
Ordnen Sie die folgenden Beispiele in die Arten von Threat Intelligence ein: Organisierte Cyberkriminelle planen zukünftig mehr Angriffe auf Linux. Emotet nutzt seit gestern verschlüsselte Anhänge, um Virenscanner zu umgehen.

Die IP-Adresse des C&C-Servers einer neuen Schadsoftware ist 10.127.541.99.

Um aktuelle Befehle abzurufen, nutzt der Schädling NotCredya die URL badguy675.evil.com.

Ein anonymer Tipp gibt Ihnen die Information, dass es einen Innentäter in Ihrer Organisation gibt.

Angreifer nutzen seit gestern die Schwachstelle CVE-2021-1234 aus.



g. Informationen in sozialen Netzwerken werden immer stärker gegen Organisationen genutzt.

Informationen über Bedrohungen oder Angreifer in Bezug auf Computerkriminalität werden Threat Intelligence genannt. Dabei existieren mehrere Definitionen für diesen Begriff. Wichtig ist, dass Threat Intelligence relevante Informationen sein müssen, auf deren Basis passende Aktionen (reaktive und präventive Maßnahmen) ausgeführt werden können. [3 Punkte]

[1 Punkt je Nennung; 1 Punkt je Erläuterung]

Strategic Threat Intelligence: Informationen über die generelle Gefahrenlage durch Computerkriminalität für strategische Entscheidungen über zukünftige Risiken.

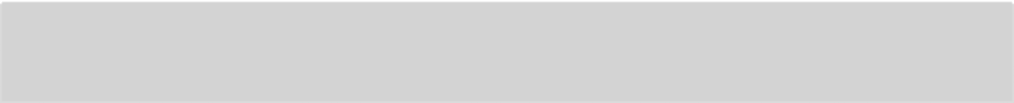
Operational Threat Intelligence: Informationen über die spezielle Gefahrenlage für die eigene Organisation.

Tactical Threat Intelligence: Informationen über das generelle Vorgehen von Computerkriminellen. Wird auch als Taktiken, Techniken und Vorgehensweisen (engl. TTP – Tactics, Techniques and Procedures) bezeichnet.

Technical Threat Intelligence: Informationen, welche von technischen Komponenten, wie Servern, Clients, Firewalls oder Switches erzeugt werden.

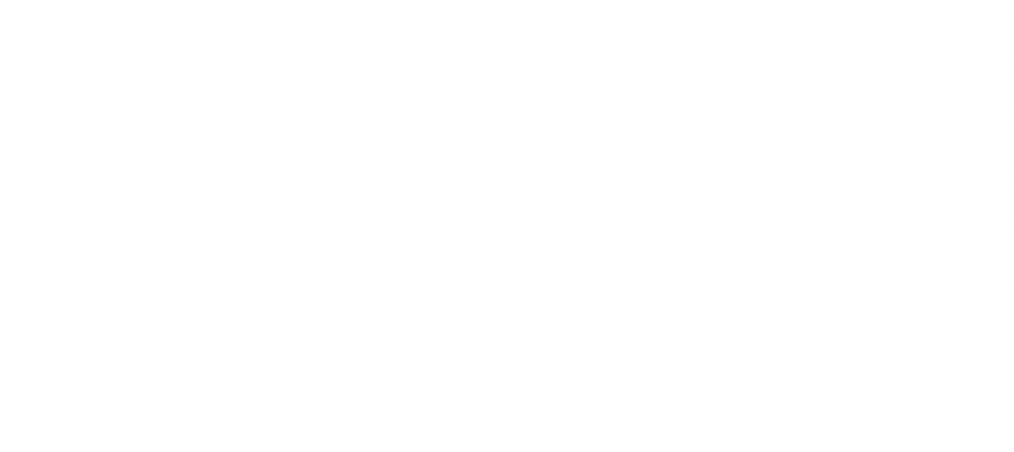
[1 Punkt je richtige Zuordnung]

* 1. strategic
  2. tactical
  3. technical
  4. technical
  5. operational
  6. tactical
  7. strategic



**FRAGE 83 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 07**



Sie sind IT-Leiter eines mittelständischen Dienstleisters, spezialisiert auf Softwareentwicklung. Sie sind außerdem zuständig für die Sichtung aller Sicherheitsmeldungen der IT-Infrastrukturen und versuchen, Angriffe frühzeitig zu erkennen. Nachdem Sie letzte Woche nur knapp schwere Konsequenzen eines Schadsoftwarebefalls verhindern konnten, erfahren Sie von einem Fachkollegen bei einem Kunden, dass die gleiche Schadsoftware auch in seiner Firma vor acht Wochen zugeschlagen hat. Hätten Sie die Merkmale der Schadsoftware gekannt, hätte Sie die Bedrohung direkt erkennen und eingreifen können.

Sie erinnern sich an Ihr Studium und an ein Werkzeug zum Teilen von Informationen über Bedrohungen: TISPs.

Was ist eine TISP und wie funktioniert sie?

Nach Rückfragen bei älteren Kollegen stellen Sie fest, dass es schon einmal Bestrebungen gab, eine TISP einzuführen. Dies wurde allerdings einstimmig



abgelehnt.

Nennen und erläutern Sie kurz fünf Gründe, welche Organisationen davon abhalten, eine TISP zu nutzen.

Eine TISP ist eine Threat Intelligence Sharing Platform, also eine Plattform zum Teilen von Threat Intelligence. Threat Intelligence ist Wissen über Bedrohungen, also Merkmale, welche Bedrohungen, wie Schadsoftware oder schadhaftes Verhalten, eindeutig identifizieren. Dieses Wissen kann über TISPs geteilt werden, sodass das Wissen über einen einmal erfolgten Angriff mit vielen Organisationen geteilt wird, sodass der Angriff dort unter Umständen verhindert werden kann. [3 Punkte]

[1 Punkt je Nennung und 2 Punkte je Erläuterung; max. 15 Punkte; es existieren neun Gründe in der Pflichtliteratur]

Negative Publicity:

Viele Organisationen versuchen, jedes Anzeichen für Schwäche unter Verschluss zu halten und ein Anzeichen für einen Angriff, auch wenn dieser nicht erfolgreich war, wird als schlechte Publicity gewertet. Aus diesem Grund dürfen diese Informationen das Unternehmen nicht verlassen und werden nicht geteilt. Dieser Aspekt trifft ein Softwarehaus besonders stark, da ein einmal infiziertes Softwarehaus schwer weiter Software verkaufen wird.

Gesetze & Datenschutz:

Jede Information, welche mit anderen Organisationen geteilt wird, müsste nach gesetzlichen und datenschutzrechtlichen Aspekten bewertet werden, ob diese geteilt werden darf oder nicht. Viele Organisationen schrecken aufgrund der Komplexität dieses Themas davor zurück.

Qualitätsbedenken:

Da die Qualität der zuliefernden Systeme für die TISP in anderen Organisationen unklar ist, ist auch die Qualität der gelieferten Daten unklar. Ein IOC sollte so sein, dass daraus eine direkte Handlungsempfehlung abzuleiten ist, aber dafür müssen die Monitoring-Systeme, welche die TISP beliefern, auch entsprechend arbeiten. Vertrauenswürdge Software ist hier auch ein Qualitätsmerkmal.

Kostenfaktor:

TISPs sind teuer und gerade für kleinere Unternehmen kaum erschwinglich. Geringschätzung des Risikos eines Angriffs:

Das Bewusstsein für die Folgen eines Cyberangriffs ist bei vielen Geschäftsleitungen noch nicht angekommen, sodass die Einführung einer TISP keine Priorität hat.



**FRAGE 86 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 08**



Was bedeutet es, dass eine Software kryptoagil ist?

Beschreiben Sie einen Grund, warum Kryptoagilität notwendig ist.

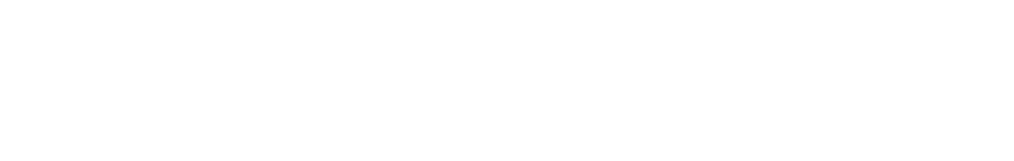
Kryptoagil:

Unter Kryptoagilität versteht man die Fähigkeit eines Systems, die verwendeten kryptografischen Algorithmen auszutauschen. Bei einer Software könnten kryptografische Verfahren über externe Bibliotheken eingebunden werden, welche man austauschen kann, oder es gibt Konfigurationsschnittstellen, um die kryptografischen Algorithmen zu definieren. [3 Punkte] Angenommen, ein Softwareprodukt, welches im Jahr 1980 veröffentlicht wurde, unterstützt ausschließlich das zu diesem Zeitpunkt aktuelle Verschlüsselungsverfahren DES. Aufgrund der geringen Schlüssellänge von 56 Bits ist dieses Verfahren seit 1997 obsolet. Sofern die Software nicht kryptoagil ist und das Verschlüsselungsverfahren gegen den Nachfolger AES ausgetauscht werden kann, kann die Software nicht mehr sicher verwendet werden. [3 Punkte]



**FRAGE 88 VON 319**

**DLMIMWCK01\_Offen\_leicht/Lektion 08**



Welche Quelle für präventive Maßnahmen zur Cybersicherheit ist für ein kleines oder mittleres Unternehmen empfehlenswert?

Nennen Sie fünf dieser empfohlenen präventiven Maßnahmen.

BSI [1 Punkt]

[1 Punkt je Maßnahme]

Verwendung von HTTPS statt HTTP Multi-Faktor-Authentifizierung Anti-Spoofing-Maßnahmen (bspw. DMARC oder SPF) Verwendung ständig aktueller Sicherheitsupdates

Offline-Backups Monitoring

Entsprechende Backupstrategie

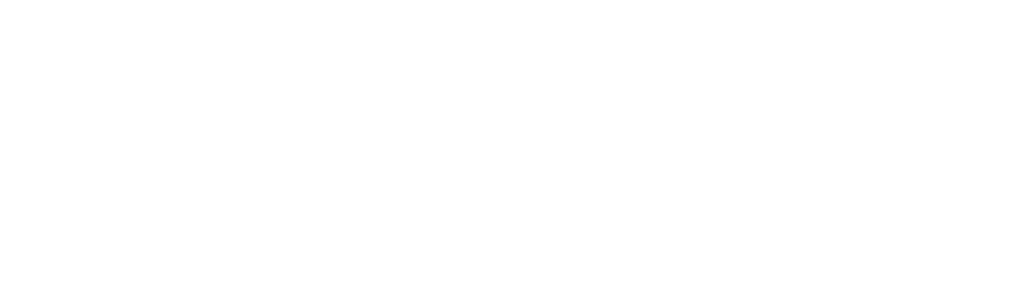
restriktive Nutzung von RDP- und anderen Freigaben nach außen spezialisierte Dienstleister

Patchmanagement Awareness



**FRAGE 90 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 08**



Ihre Organisation programmiert ein Collaboration-Tool für videobasiertes Lernen. Im Release-Prozess hat Sicherheit bisher **keine** große Rolle gespielt. Allerdings sind auch immer wieder Schwachstellen zu Tage getreten. Aus diesem Grund wird aktuell ein Vulnerability Disclosure Program (VDP) diskutiert.

Erläutern Sie, was ein VDP ist. Nennen und beschreiben Sie zwei Vorteile eines VDP.

Ein VDP ermöglicht es, Sicherheitsforschern ohne die Androhung von Strafen Sicherheitslücken in der Software oder auf Webseiten an die Betreiber zu melden, sodass diese geschlossen werden können. Die gemeldeten Sicherheitslücken können dann vom Hersteller der Software behoben werden. [3 Punkte]

Die Vorteile liegen darin, dass kontinuierlich Schwachstellen gesucht werden, also auch nach jedem Nebenrelease oder Patch. Außerdem werden diese Schwachstellen von Profis gesucht, welche die Techniken der Angreifer kennen. Diese Kenntnisse gehen meist über die der Entwickler hinaus. [3 Punkte]



**FRAGE 92 VON 319**

**DLMIMWCK01\_Offen\_mittel/Lektion 08**



Beschreiben Sie, was der Begriff Cyberscam bedeutet. Erläutern Sie ein Beispiel dazu.

Cyberscam: Unter Cyberscam versteht man alle Betrugsarten, welche mithilfe des Internets ausgeübt werden. Es gibt verschiedene Arten von Cyberscam, wie beispielsweise die Chef- Masche, Phishing, Romance Scam, Anlagebetrug oder Online Shopping-Betrug. [3 Punkte] Chef-Masche: Für Organisationen ist dabei vor allem die Chef-Masche relevant, da hierbei Zahlungsanforderungen von Geschäftskonten erwirkt werden sollen. Der Angreifer gibt sich als Chef aus und drängt die Mitarbeiter mit Aggression und Zeitdruck dazu, Handlungen zu vollziehen, welche dem Angreifer nutzen. [3 Punkte]



**FRAGE 93 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 08**



Sie sind Administrator eines kleinen Fassadenherstellers und sollen für ihren Chef eine Liste mit effektiven Sicherungsmaßnahmen vorlegen. Ihre IT-Infrastruktur besteht grob aus:

einem Webserver für die Firmenhomepage, einem E-Mail-Server und einem Festplattencluster für die zentrale Datenablage.

Nach kurzem googeln finden Sie den Lagebericht des BSI aus dem Jahr 2019 und schreiben einige der Maßnahmen auf.

Nennen und beschreiben Sie sechs Maßnahmen des BSI-Lageberichts 2019.

[1 Punkt pro Nennung, 2 Punkte pro Beispielanwendung] HTTPS statt HTTP:

Der Webserver sollte mit HTTPS laufen, damit keine MitM-Attacken durchgeführt werden können. Dies schützt die Kunden und die Vertraulichkeit.

Mehr-Faktor-Authentifizierung:

Die Mitarbeiter bzw. exponierten Mitarbeiter (wie Admins oder die Geschäftsführung) sollten sich mit mehreren Faktoren anmelden, also zusätzlich mit einem OTP auf dem Handy oder einem Hardwaretoken.

Offline-Backups:

Die Backups des Festplattenclusters müssen regelmäßig erstellt werden. Zusätzlich muss das aktuelle Backup offline aufbewahrt werden, also getrennt vom Firmennetzwerk. Der zentrale Datenspeicher muss hier dringend gebackupt werden, da dies der einzige Datenspeicher ist. Monitoring:

Das Netzwerk, die Aktivitäten auf der Homepage, die Benutzerauthentifizierung und die E-Mail- Aktivitäten sollten mit einem Monitoring-System gescannt werden, um auffälliges Verhalten direkt zu erkennen und Maßnahmen ergreifen zu können.

Patchmanagement:

Alle Systeme müssen regelmäßig gepatcht werden. Dazu gehört allen voran der Webserver, da dieser für das Internet freigegeben und somit ständigen automatisierten Scans und Angriffen ausgeliefert ist. Anschließend sollten der E-Mail-Server und die restlichen internen Server gepatcht werden.

Awareness:

Die Mitarbeiter sollten mit Schulungen und Sensibilisierungen bedacht werden. Administratoren sollten in den sicherheitskritischen Anwendungen (bspw. Monitoring) geschult werden und alle Mitarbeiter müssten bspw. zum Thema Spam sensibilisiert werden.



**FRAGE 95 VON 319**

**DLMIMWCK01\_Offen\_schwer\_F2/Lektion 08**



Sie sind Geschäftsführer eines Maschinenbauers mit einem Fokus auf digitalen Vertriebsmodellen. Nachdem mehrere Vertriebsmitarbeiter ihr eigenes Telefon für berufliche Zwecke nutzen dürfen, wollen auch viele andere Mitarbeiter diese Möglichkeit nutzen. Um bei der Nutzung privater Geräte die Gefahren für das Unternehmen zu minimieren, sollen Sie den Umgang mit "Bring your own Device" steuern.

Welche Hinweise sollen laut dem "European Cybercrime Centre" im Zuge von BYOD beachtet werden?

Nennen und beschrieben Sie die neun Hinweise mit einem Satz.

[1 Punkt für Nennung; 1 Punkt für Beschreibung]

Mitarbeiterinformationen: Die Mitarbeiter müssen über die Risiken im Umgang mit mobilen Endgeräten geschult werden.

Richtlinien für BYOD (Bring your own device): Sofern Mitarbeiter eigene Geräte nutzen dürfen, müssen dafür Regeln festgelegt werden.

Richtlinien für mobile Geräte: Es müssen Richtlinien festgelegt und überprüft werden. Erfüllt ein Gerät diese Richtlinien nicht, darf keine Verbindung zum Netzwerk hergestellt werden. Vorsicht bei öffentlichen Netzwerken: Öffentliche Netzwerke stellen ein großes Risiko für Unternehmensdaten dar.

Softwareupdates: Softwareupdates müssen immer zeitnah eingespielt werden.

Apps nur aus vertrauenswürdigen Quellen: Apps und Software für mobile Endgeräte dürfen nur aus vertrauenswürdigen Quellen bezogen werden.

Jailbreak/Rooting verhindern: Jailbreaking und Rooting muss verhindert oder verboten werden. Erwägung von Cloud-Speichern: Die Nutzung von Cloud-Speichern sollte gegen die Speicherung der Daten auf dem mobilen Gerät abgewogen werden.

Mobile Security App: Um die Software des mobilen Endgerätes zusätzlich zu überprüfen, können Mobile Security Apps installiert werden.



**FRAGE 121 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 01**



Welche der folgenden Taten zählt zu Cybercrime im weiteren Sinne?

**Wählen Sie eine Antwort:**

Fälschen einer Webseite Man-in-the-Middle-Angriff *Verkauf illegaler Waren*

Diebstahl von Login-Daten (Phishing)



**FRAGE 122 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 01**



Welche Ebene stellt **keine** grundsätzliche Kategorisierung von Schwachstellen dar?

**Wählen Sie eine Antwort:**

Schwachstellen auf Organisationsebene Schwachstellen auf Netzwerk- und Serverebene Schwachstellen auf Anwendungsebene *Schwachstellen auf Client-Ebene*



**FRAGE 123 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 01**



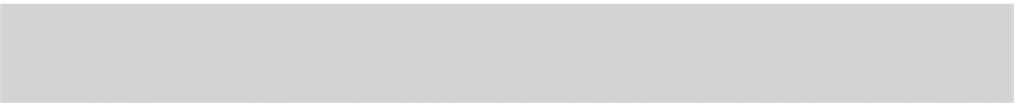
Angenommen, eine Schwachstelle erlaubt es, über die Messung der Schwingungen des Prozessors die kryptografische Sicherheit einer Verschlüsselung auszuhebeln.

Auf welche Ebene würden Sie diese Schwachstelle einordnen?

**Wählen Sie eine Antwort:**

*Schwachstelle auf Firmware- und Chipebene* Schwachstelle auf Netzwerk- und Serverebene Schwachstelle auf Organisationsebene

Schwachstelle auf Anwendungsebene



**FRAGE 124 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 01**



Welche Entwicklung wird der fünften Generation Schadsoftware zugeschrieben?

**Wählen Sie eine Antwort:**

Kommerzialisierung von Schadsoftware Selbst-Replizierung

*Schadsoftware-as-a-Service*

Nutzung des Internets



**FRAGE 125 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 01**



Welche zwei grundsätzlichen Arten der Schadsoftware-Analyse werden unterschieden?

**Wählen Sie eine Antwort:**

Immersiv und stetig Reversiv und progressiv Post- und Prä-Analyse *Statisch und dynamisch*



**FRAGE 126 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 01**



Was ist die grundsätzliche Eigenschaft eines trojanischen Pferdes?

**Wählen Sie eine Antwort:**

Es nutzt Updatefunktionen anderer Anwendungen. Es verbreitet sich selbständig.

Es richtet keinen Schaden an.

*Es wird in legitimer Software versteckt.*



**FRAGE 128 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 01**



Was ist **kein** grundlegender Bestandteil eines Botnetzes?

**Wählen Sie eine Antwort:**

Botmaster Bots *Botware*

Command & Control-Server



**FRAGE 136 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 02**



Auf welchen Tatbestand stellt der § 42 BDSG ab?

**Wählen Sie eine Antwort:**

Gewerbsmäßige Speicherung und unberechtigtes Einbehalten personenbezogener Daten *Gewerbsmäßige Weitergabe und unberechtigte Veröffentlichung personenbezogener Daten* Gewerbsmäßige Weitergabe und unberechtigte Veröffentlichung jeglicher Daten

Gewerbsmäßige Weitergabe und unberechtigte Veröffentlichung von Identitätsmerkmalen



**DLMIMWCK01\_MC\_schwer/Lektion 02**



Welcher der folgenden Paragrafen trifft auf die Tat eines Angreifers zu, welcher sich ein öffentlich-bestätigtes SSL-Zertifikat beschafft, um damit in Zukunft Man-In-the-Middle-Angriffe zu starten?

**Wählen Sie eine Antwort:**

§ 42 BDSG: Strafvorschrift

§ 202a StGB: Ausspähen von Daten

§ 253 StGB: Erpressung

*§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten*



**DLMIMWCK01\_MC\_leicht/Lektion 02**



Welchen Tatbestand enthält § 202b?

**Wählen Sie eine Antwort:**

*Abfangen von Daten* Ausspähen von Daten Identitätsmissbrauch

Betrug



**FRAGE 142 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 02**



Wie werden Plattformen genannt, welche Nutzern die Möglichkeit bieten, Daten hochzuladen, um diese dann anderen Nutzern zum Download von dieser Plattform anzubieten?

**Wählen Sie eine Antwort:**

*Filehoster* E-Hoster Hostfiler Filelister



**FRAGE 143 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 02**



Welchen Tatbestand enthält § 269 StGB?

**Wählen Sie eine Antwort:**

*Fälschung beweiserheblicher Daten* Identitätsmissbrauch Beweismissbrauch

Missbrauch personenbezogener Daten



**FRAGE 146 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 02**



Wann fällt eine Phishing-E-Mail unter den § 269 StGB?

**Wählen Sie eine Antwort:**

Wenn gefälschte Produkte verkauft werden

*Wenn ein Vertragsverhältnis zum Empfänger vorgetäuscht wird* Wenn Dienstleitungen beworben werden, welche nie erbracht werden Wenn der Absender gefälscht ist



**FRAGE 147 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 02**



Welche der folgenden Handlungen ist **nicht** im Paragraf für Computerbetrug enthalten?

**Wählen Sie eine Antwort:**

*Unrichtige Verwendung von Programmen* Unbefugte Einwirkung auf den Ablauf Unrichtige Gestaltung eines Programms

Verwendung unrichtiger oder unvollständiger Daten



**FRAGE 149 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 03**



Welches der folgenden Geräte gibt es bereits als Teil des IoT zu kaufen?

**Wählen Sie eine Antwort:**

Einwegflasche Kaugummipackung *Lampe* Dachbalken



**FRAGE 151 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 03**



Mit welcher Bezeichnung wird eine Person betitelt, die Schwachstellen in einer Software entgegen der Lizenzrichtlinien des Herstellers ausnutzt, um den Benutzern der Software mehr Möglichkeiten zur Nutzung dieser zu eröffnen?

**Wählen Sie eine Antwort:**

Black-hat White-hat Red-hat *Grey-hat*



**FRAGE 154 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 03**



In welche Kategorien werden Motive für Cyberangriffe eingeteilt?

**Wählen Sie eine Antwort:**

Extern & intern Exponiert & interniert

Externalisiert & internalisiert

*Extrinsisch & intrinsisch*



**FRAGE 156 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 03**



Welches Mittel sollte, sofern möglich, **nicht** eingesetzt werden, um die Daten nach dem Angriff eines Verschlüsselungstrojaners wiederzuerlangen?

**Wählen Sie eine Antwort:**

*Zahlung des Lösegelds* Wiederherstellung der Backups Einsatz eines Decryptors

Einsatz von IT-forensischem Personal



**DLMIMWCK01\_MC\_schwer/Lektion 03**



Als Sicherheitsbeauftragter eines national tätigen Konzerns werden Sie alarmiert, dass verdächtige Software auf einem Ihrer Server gefunden wurde. Im Zuge der forensischen Untersuchung stellen Sie fest, dass diese Software Emotet ist und bereits einige Systeme befallen hat, aber kein Schaden angerichtet wurde. Es wurden lediglich einige Verbindungen über einen Fernwartungsport in ihr Netzwerk aufgebaut.

Welche Vorgehensweise wird hier von Seiten der Angreifer ausgeführt?

**Wählen Sie eine Antwort:**

*Die Betreiber eines Verschlüsselungstrojaners schätzen den Wert Ihres Ziels ab.*

Die Betreiber von Emotet testen die Funktionalitäten der Schadsoftware. Die Betreiber eines DoS-as-a-Service-Portals bereiten einen Angriff vor.

Geheimdienste erkunden ihr Netzwerk, um Daten zu stehlen.



**FRAGE 160 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 03**



Was unterscheidet einen DoS- und einen DDoS-Angriff?

**Wählen Sie eine Antwort:**

*Die Anzahl der angegriffenen Ziele*

Die Art der eingesetzten Schadsoftware Die Anzahl der angreifenden Geräte

Die Art der verwendeten Internetleitung des Angreifers



**FRAGE 162 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 03**



Was ist **kein** Synonym für Industriespionage?

**Wählen Sie eine Antwort:**

Betriebsspionage Konkurrenzausspähung *Wirtschaftsspionage*

Werksspionage



**FRAGE 163 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 04**



Welcher der folgenden Angriffe ist ein Angriff auf Chip-Ebene?

**Wählen Sie eine Antwort:**

DirtyZombie HorrorLoad *ZombieLoad* ZombieLine



**FRAGE 166 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 04**



Eine neue Angriffsart erlaubt es, über einen erweiterten Temperatursensor in Festplatten mit motorischem Lesekopf die Daten der Festplatte auszulesen.

Zu welchem funktionalen und physischen Typ Attacke gehört diese neue Angriffsart?

**Wählen Sie eine Antwort:**

Stromverbrauch & akustisch Kryptografisch & elektromagnetisch Prozessorlast & Interferenzen

*Speichernutzung & thermisch*



**FRAGE 168 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 04**



Eine neue Angriffsart erlaubt es, anhand der Stromzufuhr eines Trusted Platform Modules Rückschlüsse auf die verwendeten asymmetrischen Schlüsselpaare zu ziehen.

Zu welchem funktionalen und physischen Typ Attacke gehört diese neue Angriffsart?

**Wählen Sie eine Antwort:**

Mikro-architektonisch & akustisch Prozessorlast & Zeitmessung Thermisch & Nutzerinteraktion

*Kryptografisch & Stromverbrauch*



**FRAGE 169 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 04**



Welcher der folgenden Begriffe stellt eine Angriffsart auf Netzwerke dar?

**Wählen Sie eine Antwort:**

Loofing-Attacke Groofing-Angriff Splinter-Attacke *Spoofing-Angriff*



**FRAGE 171 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 04**



Für was stehen die Buchstaben DNS im Zusammenhang mit Netzwerkprotokollen?

**Wählen Sie eine Antwort:**

Domain Name Switch Domain Numeration System Data Name System

*Domain Name System*



**FRAGE 173 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 04**



Auf welchem Port wird eine DNS-Verbindung nach dem RFC 1340 aufgebaut?

**Wählen Sie eine Antwort:**

443

*53*

22

110



**FRAGE 176 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 04**



Als Administrator einer Webseite sehen Sie auf ihrem Dashboard die Eingaben, welche die Besucher in die Upload-Funktion eingeben. Ihnen fallen unnormale Eingabewerte auf, welche nach Dateipfadmanipulationen aussehen, wie "/../../../../etc/passwd" oder "/../../../../../var/log/auth.log".

Welche Angriffsform versucht ein Angreifer hier gerade auszuführen?

**Wählen Sie eine Antwort:**

XXS

*Path Traversal*

XXE

Spoofing



**FRAGE 177 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 05**



Was ist das übergeordnete Ziel der IT-Forensik?

**Wählen Sie eine Antwort:**

*Aufklärung von Vorfällen der Computerkriminalität*

Sicherung der Spuren eines ATP-Angriffs

Analyse von Log-Dateien und Monitoringsystemen Präsentation von Angriffsvektoren auf der Führungsebene



**FRAGE 180 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 05**



Wie kann ein Polymorphismus **nicht** entstehen?

**Wählen Sie eine Antwort:**

Nutzung einer anderen Verschlüsselung Veränderung des Dateinamens Einfügen von ungenutztem Code *Aktionen des Opfers*



**FRAGE 182 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 05**



Sie arbeiten für ein großes Pharmaunternehmen und der Schutz der internen Informationen hat höchste Priorität. Ihr Unternehmen ist bereits Ziel mehrerer Angriffe mit bisher völlig unbekannter Schadsoftware geworden.

Welche Detektionsmethode muss im Unternehmen dringend eingesetzt werden?

**Wählen Sie eine Antwort:**

Signatur-basierte Detektion Fraktal-basierte Detektion *Verhaltens-basierte Detektion*

Morphismus-basierte Detektion





**FRAGE 184 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 05**



Zwischen welchen zwei Arten der Detektion wird in Bezug auf Schadsoftware unterschieden?

**Wählen Sie eine Antwort:**

Off-demand & time-windowed VOD & delayed

*On-demand & real-time*

By-order & instant



**FRAGE 186 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 05**



Welche Aktivität muss hauptsächlich in der Vorbereitungsphase der forensischen Untersuchung durchgeführt werden?

**Wählen Sie eine Antwort:**

Sicherung von Daten Begutachtung von Daten

*Bereitlegen aller notwendigen Werkzeuge*

Multimediaanalyse



**FRAGE 188 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 05**



Sie arbeiten für einen IT-forensischen Dienstleister und haben die Daten aller Netzwerkverbindungen, die Prozessliste eines Servers und den Inhalt des Dateisystems vor sich. Aktuell versuchen Sie herauszufinden, welcher Prozess, welche Netzwerkschnittstellen mit welchen ausführbaren Dateien ausgerufen hat.

In welcher Phase der IT-forensischen Untersuchung befinden Sie sich?

**Wählen Sie eine Antwort:**

Begutachtung von Daten *Rekonstruktion der Ereignisse* Sammeln von Daten

Vorbereitung



**FRAGE 189 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 05**



Welche der folgenden Techniken ist nach dem wipe out eines Datenträgers anzuwenden?

**Wählen Sie eine Antwort:**

*Keine der Genannten*

File carving

Signatur-basierte Wiederherstellung Bi-fragmented file carving



**FRAGE 191 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 06**



Wann werden präventive Maßnahmen ergriffen?

**Wählen Sie eine Antwort:**

Nach der Infektion durch ein Virus, aber vor der IT-forensischen Untersuchung Nach einem Sicherheitsvorfall

Während eines Sicherheitsvorfalls

*Vor einem Sicherheitsvorfall*



**FRAGE 194 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 06**



Welche der folgenden Maßnahmen ist eine präventive Maßnahme?

**Wählen Sie eine Antwort:**

Abschalten eines Netzwerksegments, um die Ausbreitung eines Wurms einzudämmen Benachrichtigung öffentlicher Stellen aufgrund eines Virenbefalls

*Erstellen einer Richtlinie zum Einsatz von kryptografischen Schlüsseln*

Wiederherstellung aller Server aus den Backups im Zuge des Disaster Recovery



**FRAGE 195 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 06**



Was bedeutet SSO?

**Wählen Sie eine Antwort:**

Single-Signature-Over Save-Sign-on

Save-Signature-On

*Single-Sign-On*



**FRAGE 198 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 06**



Bei der Anwendungsentwicklung in der eigenen Organisation stellt ein Webentwickler das neue Administrationswerkzeug für Webseiten vor. Einführend erwähnt der Webentwickler, dass der Zugang zu diesem Werkzeug über die URL "[www.beispielfirma.de/app/administration](http://www.beispielfirma.de/app/administration)" erfolgt.

Ist dieser Zugang sicher vor Unbefugten?

**Wählen Sie eine Antwort:**

Ja, wenn die URL mit Sonderzeichen gemischt wird, bspw. "/app/adm!n!5trat!0n".

*Ja, wenn ein Login für den Aufruf von "/app/administration" notwendig ist.*

Ja, wenn nur sehr wenige Mitarbeiter Kenntnis von der Existenz der URL haben. Ja, wenn keine Verlinkungen zu "/app/administration" existieren.



**FRAGE 199 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 06**



Was ist ein Active Directory?

**Wählen Sie eine Antwort:**

Betriebssystem

Threat Intelligence Sharing Platform Netzwerk-Management-Tool *Verzeichnisdienst*



**FRAGE 202 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 06**



Für welchen Schutzbedarf sieht der IT-Grundschutz eine automatische Reaktion auf sicherheitsrelevante Ereignisse vor?

**Wählen Sie eine Antwort:**

Geringer Schutzbedarf Standard-Schutzbedarf Normaler Schutzbedarf

*Erhöhten Schutzbedarf*



**FRAGE 203 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 06**



Wofür steht die Abkürzung IDS?

**Wählen Sie eine Antwort:**

Incident Determination System Incident Detection System *Intrusion Detection System* Intrusion Determination System



**FRAGE 205 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 07**



Welche der folgenden Begriffe stellt eine physische Konsequenz dar?

**Wählen Sie eine Antwort:**

Schlechte Berichterstattung in der Presse

Serviceleistung an einen Kunden kann nicht erbracht werden.

*Defekt einer Festplatte*

Ein Auftrag kann nicht erfüllt werden.



**FRAGE 208 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 07**



Zu welcher Art Threat Intelligence wird folgende Information zugeordnet? "Emotet-Mails werden aktuell mit realen Konversationen versendet, um vertrauenswürdig beim Empfänger zu wirken!"

**Wählen Sie eine Antwort:**

*Tactical* Longterm Strategic Technical



**FRAGE 209 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 07**



Wer sollte alle Entscheidungen im Falle eines Cyberangriffs treffen?

**Wählen Sie eine Antwort:**

Der Mitarbeiter, der den Angriff entdeckt Der forensische Dienstleister

*Der Krisenstab*

Der Systemadministrator des infizierten Systems



**FRAGE 212 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 07**



Auf welchem Programmierfehler basiert ein Pufferüberlauf?

**Wählen Sie eine Antwort:**

Es wird ".NET 3.4.1" anstatt ".NET 4.1" genutzt.

Dem Benutzer wird keine aussagekräftige Fehlermeldung angezeigt.

*Die Länge eines Eingabewertes wird nicht überprüft.*

Es wird implizite Typeconversion zugelassen.



**FRAGE 214 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 07**



Welche Arten von Threat Intelligence existieren?

**Wählen Sie eine Antwort:**

Medium, longterm, acustic, political Shortterm, network, delayed, critical Historical, instant, proactive, organizational

*Strategic, operational, tactical, technical*



**DLMIMWCK01\_MC\_schwer/Lektion 07**



Welche Art von IOC hinterlässt ein Angreifer, welcher per Social Engineering in sozialen Netzwerken Zugangsdaten eines Administrators herausfindet und diese ausnutzt, um über eine schlecht programmierte Administrationsoberfläche Daten von Kunden zu ändern?

**Wählen Sie eine Antwort:**

Host-based E-Mail Network

*Keine der genannten*



**FRAGE 218 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 07**



Welche Branche gehört **nicht** zu den Betreibern kritischer Infrastruktur?

**Wählen Sie eine Antwort:**

Öffentlicher Rundfunk

*Hochschulen*

Banken Geheimdienst



**FRAGE 220 VON 319**

**DLMIMWCK01\_MC\_mittel/Lektion 08**



Welche Quelle können Sie nutzen, wenn es um konkrete Zahlen zu Straftatbeständen in Deutschland geht?

**Wählen Sie eine Antwort:**

PSK

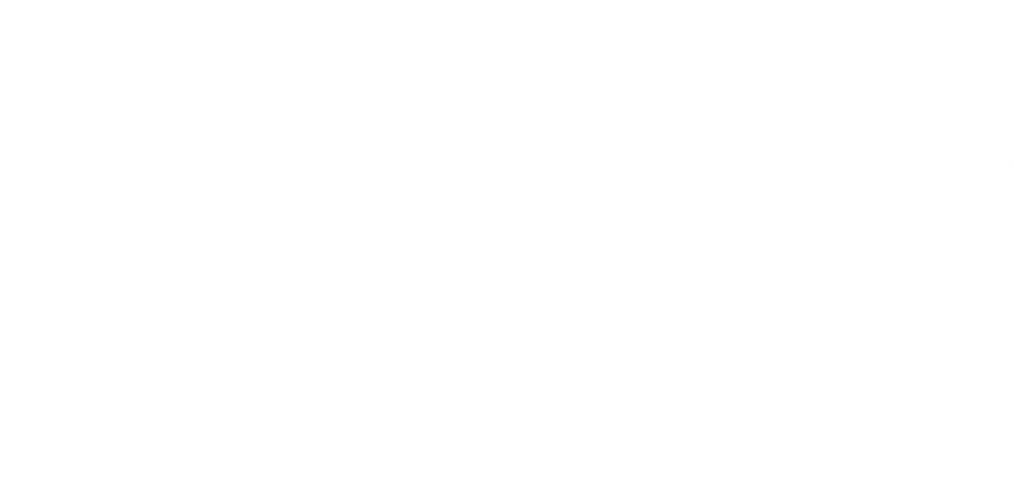
*PKS*

Polizeilicher Statistikkanal Polizeilicher Kriminalstand



**FRAGE 221 VON 319**

**DLMIMWCK01\_MC\_schwer/Lektion 08**



Sie sind Teamleiter der Entwicklung in einem Unternehmen für Softwareentwicklung. Eines ihrer Produkte unterstützt aktuell nur die Eingabe von Passwörtern mit einer Länge von sechs Zeichen. Da solche kurzen Passwörter ein Sicherheitsrisiko darstellen, wird diskutiert, wie eine Authentifizierung zukünftig durchgeführt werden soll.

Was sollte nach den Empfehlungen des Weisenrats für Cyber-Sicherheit 2020 getan werden?

**Wählen Sie eine Antwort:**

*Einführung einer Authentifizierung mittels biometrischer Verfahren*

Einführung einer Mindestlänge von 14 Zeichen Erhöhung der Passwortlänge auf 20 Zeichen

Entfernen der Authentifizierung



**DLMIMWCK01\_MC\_mittel/Lektion 08**



Welche Maßnahme empfiehlt das BSI im Lagebericht 2019 gegen DDoS- Angriffe?

**Wählen Sie eine Antwort:**

*Spezialisierte Dienstleister* Awareness-Kampagnen Einsetzen von DMARC

Neue Serverhardware



**DLMIMWCK01\_MC\_schwer/Lektion 08**



Sie besitzen ein Unternehmen, welches Dokumente aus öffentlich zugänglichen Quellen sammelt, aggregiert und durchsuchbar zur Verfügung stellt.

Welche der folgenden Maßnahmen ist für Sie am wichtigsten?

**Wählen Sie eine Antwort:**

Mehr-Faktor-Authentifizierung Awareness-Schulungen

Beauftragung eines Scrubbing Center

*Offline-Backups*



**FRAGE 227 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 08**



Welche Auswirkung der COVID-19-Pandemie wirkt laut ENISA am stärksten auf die Cybersicherheit?

**Wählen Sie eine Antwort:**

Erhöhter Informationsbedarf

*Starke Verbreitung von Homeoffice*

Erhöhte Anzahl von Intensivpatienten Entwicklung des Impfstoffs



**FRAGE 229 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 08**



Wecher Trend fordert laut ENISA neue Formen von Schutzmaßnahmen?

**Wählen Sie eine Antwort:**

*Digitalisierung von Prozessen*

Fachkräftemangel

Verbreitung erneuerbarer Energien Trend zu On-Premise-Diensten



**FRAGE 231 VON 319**

**DLMIMWCK01\_MC\_leicht/Lektion 08**



Wofür steht die Abkürzung VDP im Zusammenhang mit Cybersicherheit?

**Wählen Sie eine Antwort:**

Vulnerabilitiy Defacement Program Vulnerability Dont Patch *Vulnerability Disclosure Program* Vulnerability Disclosure Path