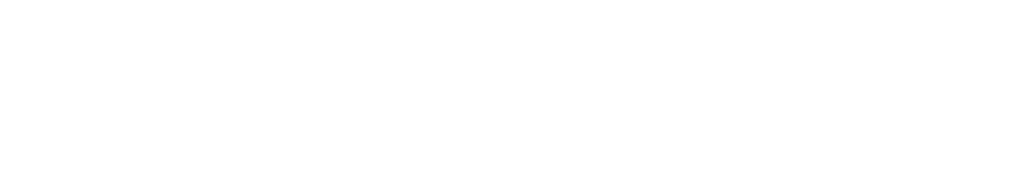


**FRAGE 1 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 01**

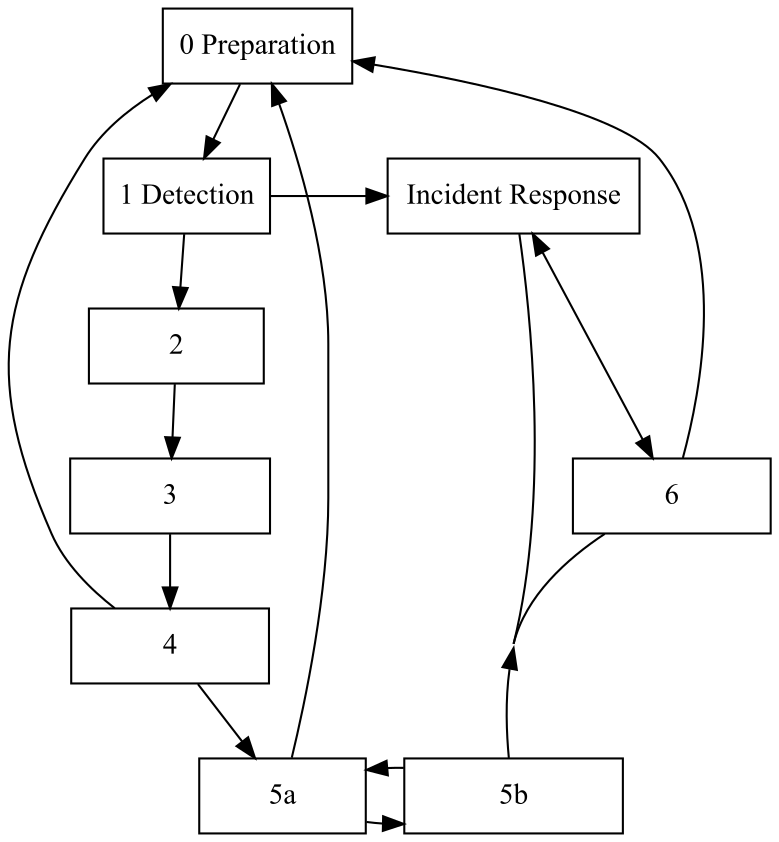


1. Was ist das Ziel eines Distributed-Denial-of-Service-Angriffs (DDoS-Angriffs)?
2. Welche Eigenschaften haben derartige Attacken mit regulären Denial-of-Service-Angriffen (DoS-Angriffen) gemein?
3. Worin besteht der wichtigste Unterschied zwischen DDoS- und DoS-Angriffen?
4. Das Ziel eines Distributed-Denial-of-Service-Angriffs/DDoS-Angriffs besteht darin, die Verfügbarkeit eines bereitgestellten Service zu beeinträchtigen (1 P).
5. Diese Zielsetzung stimmt mit der eines regulären Denial-of-Service-Angriffs (DoS-Angriffs) überein (1 P).
6. DoS-Angriffe gehen von einzelnen Systemen aus (2 P), während DDoS-Attacken auf einer möglichst großen Zahl angreifender Systeme basieren (2 P).



**FRAGE 2 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 01**



Benennen Sie die Schritte, die in dem abgebildeten allgemeinen Prozessmodell der Netzwerkforensik fehlen.

2 Datensammlung, 3 Beweissicherung, 4 Prüfung, 5a Analyse, 5b Untersuchung, 6 Ergebnispräsentation (je 1 P)



**FRAGE 3 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 01**



Definieren Sie den Begriff „Netzwerkforensik“.

Netzwerkforensik beinhaltet die Erfassung, Aufzeichnung (2 P für diesen Aspekt) und Analyse (2 P) von Netzwerk- und Ereignisdaten (2 P) – mit dem Ziel, die Ursachen von Angriffen (1 P) und anderen Vorfällen (1 P) ausfindig zu machen.



**FRAGE 4 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 01**



Im Rahmen der IT-Leistungsüberwachung wird festgestellt, dass die Auslastung eines bestimmten Webservers weit über dem normalen Maß liegt.

1. Welche Art von Angriff kommt als mögliche Ursache für dieses Phänomen infrage?
2. Nennen und beschreiben Sie eine Gegenmaßnahme, mit der sich sicherstellen lässt, dass der betroffene Webservice für legitime Benutzer:innen verfügbar bleibt.
3. Unter welchen Voraussetzungen ist die von Ihnen genannte Gegenmaßnahme effektiv?
4. (Distributed-)Denial-of-Service-Angriff (2 P)
5. Eine mögliche Gegenmaßnahme ist Scrubbing (2 P), d. h. der Einsatz eines Filtermechanismus, der dafür sorgt, dass illegitime Anfragen vor Erreichen des Servers identifiziert und ignoriert/abgelehnt werden (2 P).
6. Eine notwendige Voraussetzung ist in diesem Fall die trennscharfe Identifizierung illegitimer Anfragen (2 P).

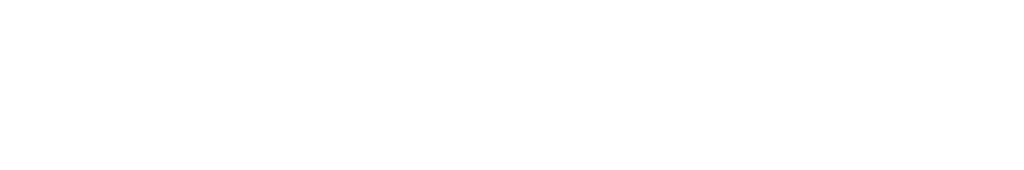
Alternative Antwort zu b): Abwehr des Angriffs durch dynamische Skalierung (2 P), d. h. durch die rasche Bereitstellung zusätzlicher Ressourcen zur Beantwortung aller Anfragen (2 P).

Alternative Antwort zu c): Voraussetzung für die (D)DoS-Abwehr durch dynamische Skalierung ist die Skalierbarkeit (2 P) der Serversysteme sowie der IT-Umgebungen, in denen sie gehostet werden.



**FRAGE 5 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 01**



1. Skizzieren Sie ein Szenario, bei dem sich die schädlichen Aktivitäten einer Angreifergruppe gegen ein konkretes Ziel richten.
2. Nennen Sie eine dazu passende Gegenmaßnahme und erläutern Sie, warum diese in dem von Ihnen beschriebenen Szenario effektiv ist.
3. Ein Spear-Phishing-Angriff (3 P) auf ein bestimmtes Mitglied der Belegschaft (1 P). (Andere Antworten möglich)
4. Eine mögliche (langfristige) Gegenmaßnahme sind Mitarbeiterschulungen (3 P), die das Sicherheitsbewusstsein besonders gefährdeter Personen steigern (3 P). (Andere Antworten möglich. In diesem Fall gilt folgender Punkteschlüssel: 3 P für das Szenario, 1 P für die Angabe des Angriffsziels, 3 P für die Gegenmaßnahme, 3 P für die Begründung ihrer Effektivität)



**FRAGE 6 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 01**



Erläutern Sie den Unterschied zwischen einer IDS-Warnmeldung, einem Sicherheitsereignis und einem Sicherheitsvorfall und illustrieren Sie dies anhand eines Beispiels.

Eine Warnmeldung ist eine unbearbeitete Ausgabe eines IDS oder eines anderen Sensors (2 P).

Sie wird zum Sicherheitsereignis, wenn ein Fehlalarm ausgeschlossen werden kann (2 P).

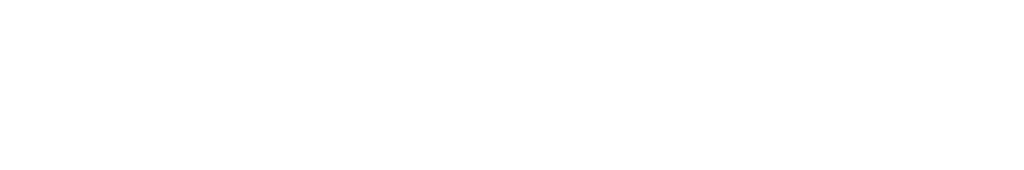
Ein Sicherheitsereignis gilt nur dann als Sicherheitsvorfall, wenn eine Sicherheitsrichtlinie verletzt wurde (2 P).

Ein Beispiel hierfür ist der Systemzugriff eines Users, dessen Anmeldedaten eigentlich bereits abgelaufen sein sollten (2 P für das Beispiel). Hier liegt ein Sicherheitsvorfall vor, wenn der Vorgang eine bestehende Sicherheitsrichtlinie des betreffenden Unternehmens verletzt (2 P für die korrekte Klassifizierung). (Andere Antworten sind möglich.)



**FRAGE 7 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 02**



Eine netzwerkbasierte Anwendung möchte Daten an eine andere Anwendung senden.

1. In welchen Einheiten werden die fraglichen Daten auf den verschiedenen Ebenen des TCP/IP-Schichtenmodells gekapselt, bevor sie als Bits über eine physische Verbindung übermittelt werden?
2. Welche Informationen werden bei den einzelnen Schritten hinzugefügt?
3. Die Daten werden zunächst in Segmente zerlegt (1 P). Anschließend werden die einzelnen Segmente in Paketen gekapselt (1 P). Diese Pakete werden dann wiederum in Frames eingeschlossen (1 P).
4. Segmente enthalten Portnummern und andere für die Datenverarbeitung wichtige Informationen (1 P). Paket-Header enthalten die Adressen der jeweiligen Sender- und Empfängersysteme. Frames enthalten Informationen, die für die Fehlererkennung und -korrektur von Bedeutung sind (1 P).



**FRAGE 8 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 02**



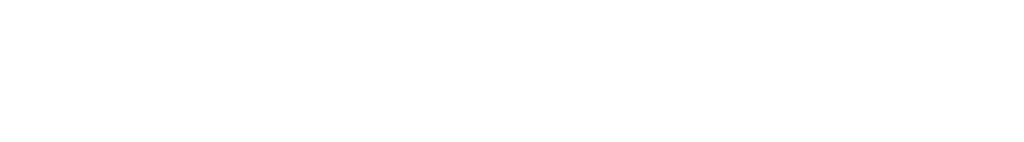
Erläutern Sie den Unterschied zwischen verbindungsorientierten und verbindungslosen Kommunikationsprotokollen in den beiden folgenden Punkten:

1. Wie erfolgt der Datenaustausch?
2. Wer kommuniziert mit wem?
3. Verbindungsorientierte Protokolle stellen datenstromorientierte Kommunikationskanäle bereit (2 P), während verbindungslose Protokolle einzelne Nachrichten/Datagramme übermitteln (2 P).
4. Bei verbindungsorientierten Protokollen erfolgt der Datenaustausch zwischen zwei Peers (1 P). Im Unterschied dazu versetzen verbindungslose Protokolle einen Peer in die Lage, Nachrichten an einen oder mehrere Empfänger zu senden (1 P).



**FRAGE 9 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 02**



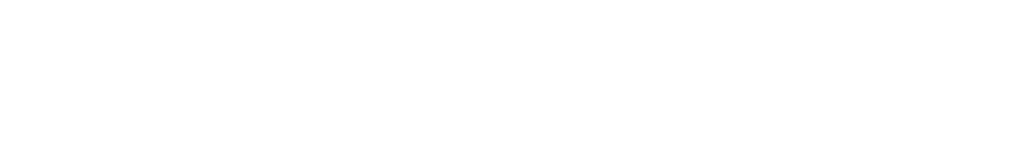
Erläutern Sie den Unterschied zwischen der Internet-/Netzwerkschicht und der Verbindungsschicht.

1. Was sind jeweils die Hauptfunktionen?
2. Welche Dateneinheiten werden auf den betreffenden Schichten ausgetauscht?
3. Hauptfunktion der Internet-/Netzwerkschicht ist die Datenübertragung zwischen Systemen, die nicht notwendigerweise benachbart bzw. direkt miteinander verbunden sind (2 P). Die Verbindungsschicht stellt eine zuverlässige (2 P) Datenverbindung zwischen zwei benachbarten Systemen (2 P) bereit.
4. Auf der Internet-/Netzwerkschicht werden Pakete (1 P), auf der Verbindungsschicht dagegen Frames (1 P) übermittelt.



**FRAGE 10 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 02**



Die Netzwerkstandards des IEEE-802-Projekts spezifizieren die Datenübertragung über verschiedenste Medien – von Funkverbindungen bis hin zu Kupferkabeln. Welche zwei Features einer geschichteten Netzwerkarchitektur sind der Grund dafür, dass diese Vielfalt bei der Erstellung und Implementierung von Netzwerkanwendungen nicht berücksichtigt werden muss? Erläutern Sie Ihre Antwort.

1. Transparenz (1 P): Es sind keine Anpassungen erforderlich, wenn Protokolle der höheren Schichten die Dienste der darunterliegenden Schichten in Anspruch nehmen (3 P). 2. Unabhängigkeit von bestimmten physischen Infrastrukturen (1 P): Die Protokolle der höheren Schichten sind für alle einschlägigen physischen Datenübertragungsmechanismen tauglich (3 P).



**FRAGE 11 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 02**



Moderne Netzwerke werden in verschiedenen, aufeinander aufbauenden Schichten implementiert.

1. Nennen und erläutern Sie eines der Designziele dieser Architektur.
2. Schildern Sie für ein spezifisches Netzwerkprotokoll, wie dieses das von Ihnen genannte Designziel erfüllt.
3. Trennung der Belange (2P – Korrekte Nennung des Namens eines Designziels): Jedes für eine spezifische Schicht genutzte Protokoll soll unabhängig von den anderen Protokollen weiterentwickelt werden können (3P – Beschreibung).
4. Das IPv6-Protokoll (2P – Nennung eines Beispiels) ist eine Weiterentwicklung von IPv4, die einige spezifische Defizite von IPv4 behebt, ohne dass dies Auswirkungen auf die Protokolle der darüberliegenden Schichten (z. B. TCP) oder die darunterliegenden Schichten (z. B. Ethernet) hat (3P – korrekte Begründung).



**FRAGE 12 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 02**



Der Standardisierungsentwurf RFC 1772 löst den vorgeschlagenen Standard RFC 1655 ab.

1. Welches RFC-Dokument ist neueren Datums? Begründen Sie Ihre Antwort.
2. Welches RFC-Dokument wird mit höherer Wahrscheinlichkeit in der Praxis herangezogen? Begründen Sie Ihre Antwort.
3. Welches RFC-Dokument sollte als Grundlage für die Implementierung neuer Anwendungen genutzt werden? Begründen Sie Ihre Antwort.
4. RFC 1772 ist neuer als RFC 1655 (1 P), was an der höheren RFC-Nummer ersichtlich wird (1 P).
5. RFC 1655 kommt mit höherer Wahrscheinlichkeit in der Praxis zum Einsatz (1 P), da die Einstufung als „vorgeschlagenen Standard“ auf einen hohen Verbreitungsgrad hindeutet (3 P).
6. Neue Anwendungen sollten auf Basis von RFC 1772 implementiert werden, weil der neuere Standard wahrscheinlich einige Defizite der älteren Version aus RFC 1655 behebt (3P – schlüssige Begründung).

ODER: Bei der Implementierung neuer Anwendungen sollte RFC 1655 herangezogen werden, weil dieser vorgeschlagene Standard (zumindest aktuell) weiter verbreitet ist (3P – schlüssige Begründung).



**FRAGE 13 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 03**



Nennen Sie die drei Phasen eines typischen TCP-Dialogs.

Verbindungsaufbau (2 P), Datenaustausch zwischen den beiden Peers (2 P), Trennung der Verbindung durch einen oder beide Peers (2 P)



**FRAGE 14 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 03**



1. Welchem Zweck dient ein SOCKS-Proxy?
2. Beschreiben Sie, wie diese Funktion praktisch realisiert wird.
3. Ein SOCKS-Proxy ermöglicht die Übertragung von Daten unter Umgehung der Firewall bzw. über die Grenze eines Netzwerksegments hinweg (3 P für den einen oder den anderen Aspekt).
4. Das SOCKS-Protokoll weist den Server an, Daten im Auftrag des Clients zu übermitteln und die empfangenen Antworten an den Client weiterzuleiten (3 P).



**FRAGE 15 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 03**



Nennen Sie zwei Anwendungen des UDP und begründen Sie jeweils, warum sich der Einsatz dieses Protokolls hier anbietet.

Punkteschlüssel: je 1 P für die Nennung einer Anwendung, je 3 P für die Begründung

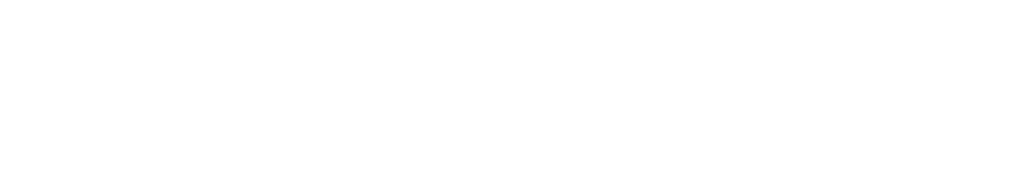
Beispiel: Eine mögliche Anwendung ist die Synchronisierung diverser Systemuhren mithilfe des Network Time Protocol (1 P). Hier bietet sich die Nutzung des UDP an, weil es dank seiner geringen Latenzen übertragungsbedingte Verzerrungen der Zeitwerte minimiert (3 P).

Eine weitere Anwendung ist der Versand von Nachrichten, die mehrere Empfänger gleichzeitig oder dem Sender unbekannte Adressaten erreichen sollen (1 P). Hier erweist es sich als Vorteil, dass das UDP Broadcastfunktionen bereitstellt (3 P).



**FRAGE 16 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 03**



Das TCP nutzt Empfangs- und Sendepuffer auf beiden Peers.

1. Welche wichtige Funktion erfüllen diese Puffer?
2. Welche Methode bzw. welches Verfahren kommt bei der Realisierung dieser Funktion zur Anwendung?
3. Welche zusätzlichen Informationen liefert der Pufferzustand?

a) Die wichtigste Funktion der Puffer besteht in der Wiederherstellung der von den Peers ausgetauschten Daten in der richtigen Reihenfolge (3 P) mithilfe des b) Sliding-Window-Verfahrens. (2 P).

1. Der Zustand der Empfangs- und Sendepuffer kann auf Probleme auf den unteren Netzwerkschichten hinweisen (3 P).



**FRAGE 17 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 03**



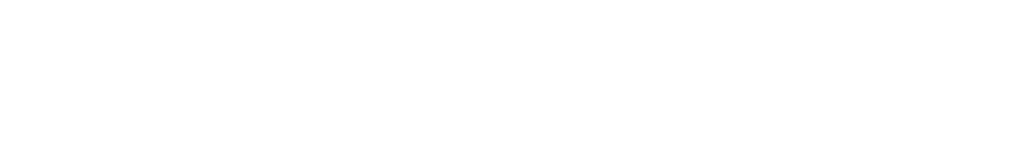
Ein TCP-SYN-Flood-Angriff ist eine effektive Methode zur Durchführung einer Denial-of-Service-Attacke. Erläutern Sie, wie ein TCP-SYN-Flood-Angriff abläuft.

1. Welcher Mechanismus des TCP wird dabei missbraucht?
2. Wie kann damit eine Überlastung der Serverressourcen herbeigeführt werden?
3. Ist es möglich, einen TCP-SYN-Flood-Angriff auf der Anwendungsschicht abzuwehren? Erläutern Sie Ihre Antwort.
4. TCP-SYN-Flood-Angriffe nehmen den Drei-Wege-Handshake beim Aufbau einer TCP-Verbindung ins Visier (2 P).
5. Wenn ein Server ein SYN-Segment empfängt (2 P), richtet er in Erwartung einer neuen Verbindung Sende- und Empfangspuffer ein und weist diesen Puffern einen Teil seiner Ressourcen zu (2 P), was bei einer großen Zahl von SYN-Anfragen zur völligen Überlastung führen kann.
6. Es ist nicht möglich, einen SYN-Flood-Angriff auf der Anwendungsschicht abzuwehren (2 P), da für diese Attacke grundlegende Funktionen der TCP-Transportschicht missbraucht werden (2 P).



**FRAGE 18 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 03**



Einige Remotedesktop-Tools versetzen die Benutzer:innen in die Lage, ein Remotesystem so zu steuern, als ob sie direkten, physischen Zugriff darauf hätten. Welches Transportprotokoll ist für ein solches Anwendungsszenario am sinnvollsten? Erläutern Sie Ihre Antwort.

TCP (2 P), weil TCP einen datenstromorientierten (3 P), bidirektionalen (2 P) Kommunikationskanal implementiert und die ursprüngliche Reihenfolge der empfangenen Pakete wiederherstellt (3 P). All diese Eigenschaften sind für Remotedesktop-Anwendungen unerlässlich.



**FRAGE 19 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 04**



Worin besteht der Hauptunterschied zwischen IPv4- und IPv6-Adressen?

IPv4-Adressen weisen eine Länge von 32 Bit auf (3 P), IPv6-Adressen sind dagegen 128 Bit lang (3 P).



**FRAGE 20 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 04**



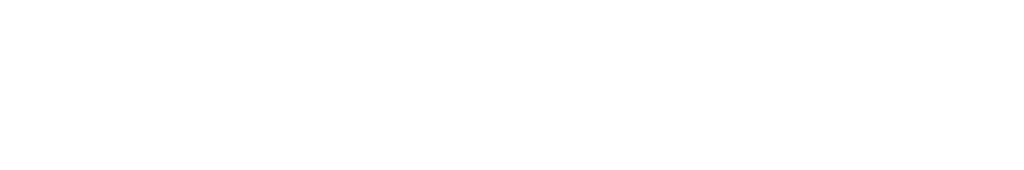
Nennen Sie drei Bereiche, die von der Internet Assigned Numbers Authority verwaltet werden.

(Je 2 P) Reservierte/spezielle IP-Adressbereiche, Protokollnummern, Portnummern, AS-Nummern, Bereitstellung von whois-Daten durch regionale Registrierungsstellen



**FRAGE 21 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 04**



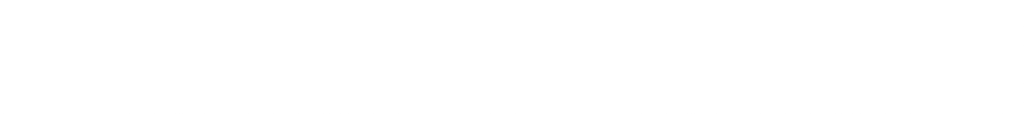
Eine Netzwerkadministratorin möchte überprüfen, dass ihre Router korrekt konfiguriert sind und jedes IP-Paket über den jeweils vorgesehenen Pfad übertragen wird.

1. Welches Tool kann sie zu diesem Zweck nutzen?
2. Wie funktioniert das in a) genannte Tool?
3. Für diesen Zweck steht das Tool „traceroute“ zur Verfügung (2 P).
4. Dieses Tool versendet eine Reihe von ICMP-Nachrichten an die gewünschte Zieladresse (2 P). Dabei erhält jedes Paket eine andere Gültigkeitsdauer bzw. einen anderen TTL-Wert (2 P), sodass jedes Mal ein anderer Router eine Zeitüberschreitung meldet (2 P). Auf diese Weise lassen sich nach und nach sämtliche Übertragungsstationen rekonstruieren.



**FRAGE 22 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 04**



1. Welchem Zweck dient das Dynamic Host Configuration Protocol (DHCP)?
2. Wie funktioniert es?
3. Über DHCP erhalten neue Netzwerkclients Konfigurationsdaten (2 P), die unter anderem eine verfügbare IP-Adresse enthalten (1 P).
4. Der Client kann diese Informationen mit einer Broadcastnachricht anfordern (3 P), die dann vom DHCP-Server beantwortet wird (2 P).



**FRAGE 23 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 04**

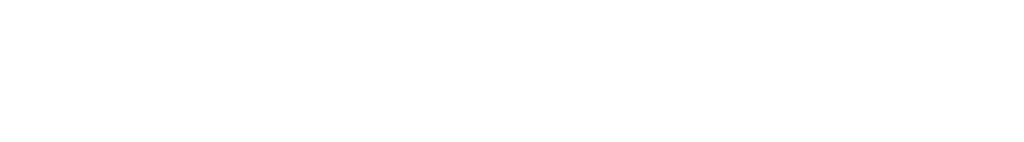


1. Welchen Zweck erfüllt die Netzwerkadressübersetzung (NAT)?
2. Warum ist NAT unverzichtbar?
3. Wie funktioniert NAT? Illustrieren Sie dies an einem Beispiel mit willkürlich gewählten Adressen und Ports.
4. Dank Netzwerkadressübersetzung können sich mehrere Systeme eine reguläre IP-Adresse teilen.
5. NAT ist eine Notwendigkeit, seit die Zahl der mit dem Internet verbundenen Systeme die Zahl der verfügbaren IPv4-Adressen übersteigt (2 P).
6. NAT bietet sich für interne Netzwerke mit einem privaten IP-Adressblock wie etwa 192.168.177.\* an (2 P für den privaten IP-Block). Versendet ein Gerät aus diesem Netzwerk Pakete an eine externe Adresse, werden diese vom NAT-Router mit einer neuen Quelladresse und einem neuen Quellport versehen und dann an ihr vorgesehenes Ziel weitergeleitet (2 P). Eingehende Antworten werden in umgekehrter Weise bearbeitet und erhalten dabei vom NAT-Router die verbindungslokale Ziel-Adresse und den Zielport des Absenders der ursprünglichen Anfrage (2 P).



**FRAGE 24 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 04**



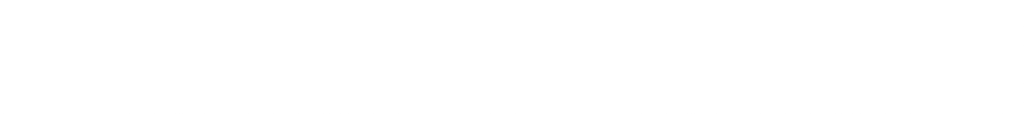
Ein Gast nutzt die automatische IPv4-Konfiguration, um eine Verbindung mit dem Netzwerk seines Hotels herzustellen.

1. Kann er danach direkt auf das Internet zugreifen? Wenn ja, warum? Wenn nein, warum nicht?
2. Nennen Sie drei Maßnahmen, die das IT-Team des Hotels ergreifen kann, um eine funktionierende Verbindung einzurichten.
3. Nein (2 P), weil Pakete aus dem für die automatische Konfiguration genutzten IP-Block nicht routingfähig sind (2 P).
4. Das IT-Team des Hotels könnte einen Proxy-Server (2 P) oder einen NAT-fähigen Router (2 P) einrichten oder einen DHCP-Server implementieren (2 P).



**FRAGE 25 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 05**



1. Welchem Zweck dient das Address Resolution Protocol (ARP)?
2. Wie funktioniert es?
3. Das ARP bietet vernetzten Systemen die Möglichkeit, die einer IP-Adresse zugeordnete MAC-Adresse zu ermitteln (2 P).
4. Entsprechende Anfragen werden als Broadcastnachrichten versendet (2 P). Das betreffende System antwortet dann mit seiner MAC- und IP-Adresse (2 P).



**FRAGE 26 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 05**

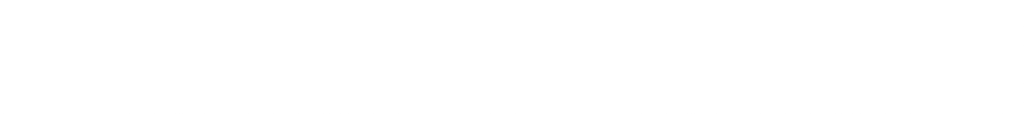


1. Was ist die primäre Funktion des Border Gateway Protocol (BGP)?
2. Wie werden hier Routen konfiguriert?
3. Auf welcher Basis?
4. Der Hauptzweck des BGP besteht in der Bereitstellung von Verbindungen, die autonome Systeme verknüpfen (2 P).
5. BGP-Routen werden manuell konfiguriert (2 P).
6. Als Basis dienen Richtlinien (2 P), die von den jeweiligen Inhaberorganisation der autonomen Systeme festgelegt oder zwischen den verschiedenen Inhabern vereinbart wurden.



**FRAGE 27 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 05**



Erläutern Sie, wie ein für das Routing Information Protocol (RIP) konfigurierter Router feststellt, dass eine Verbindung zu einem benachbarten Router nicht verfügbar ist.

Benachbarte RIP-Router tauschen regelmäßig Informationen aus (2 P). Außerdem richten sie einen Timer (1 P) für jede einzelne Route ein (2 P). Läuft ein solcher Timer ab, ohne dass eine Nachricht des betreffenden Peers eingegangen ist, wird die Route zu diesem Router als nicht verfügbar markiert (3 P).



**FRAGE 28 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 05**



1. Nennen Sie einen Angriff, der sich gegen die Routinginfrastruktur richtet.
2. Beschreiben Sie dessen Folgen.
3. Wie wird dieser Angriff durchgeführt?

Punkteschlüssel: 2 P für die Nennung des Angriffs;   
3 P für die Folgen; 3 P für den Ablauf.

Beispiel:

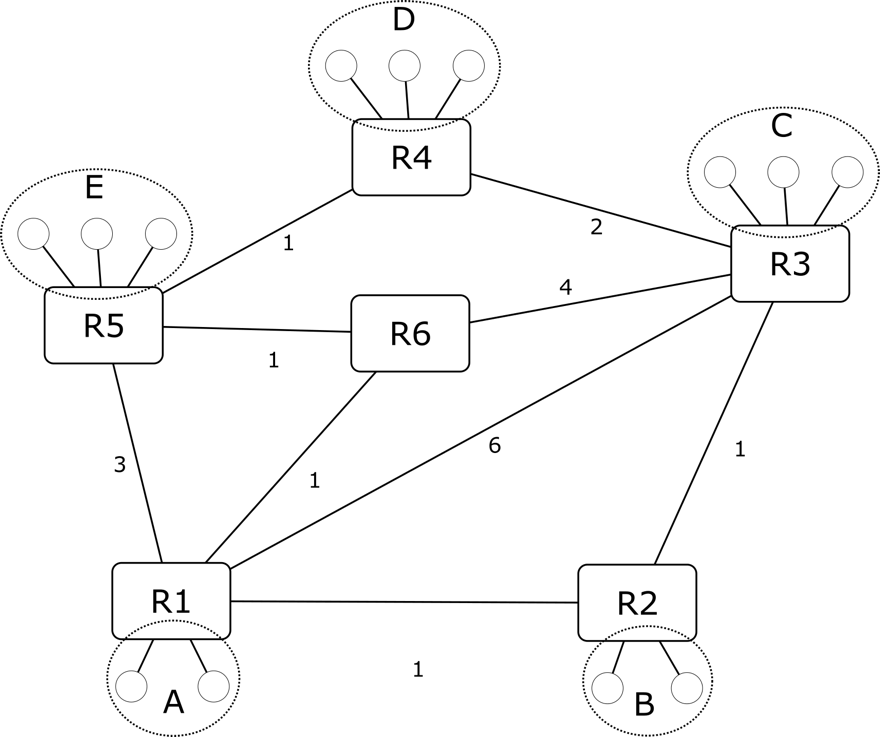
a) ARP-Poisoning (2 P);

1. Alle an ein bestimmtes Zielsystem adressierten Datenpakete werden auf ein von den Angreifer:innen kontrolliertes System im selben Netzwerksegment umgeleitet (3 P);
2. Ausgangspunkt ist hier der Versand gefälschter ARP-Nachrichten (3 P) an lokale Systeme.



**FRAGE 29 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 05**



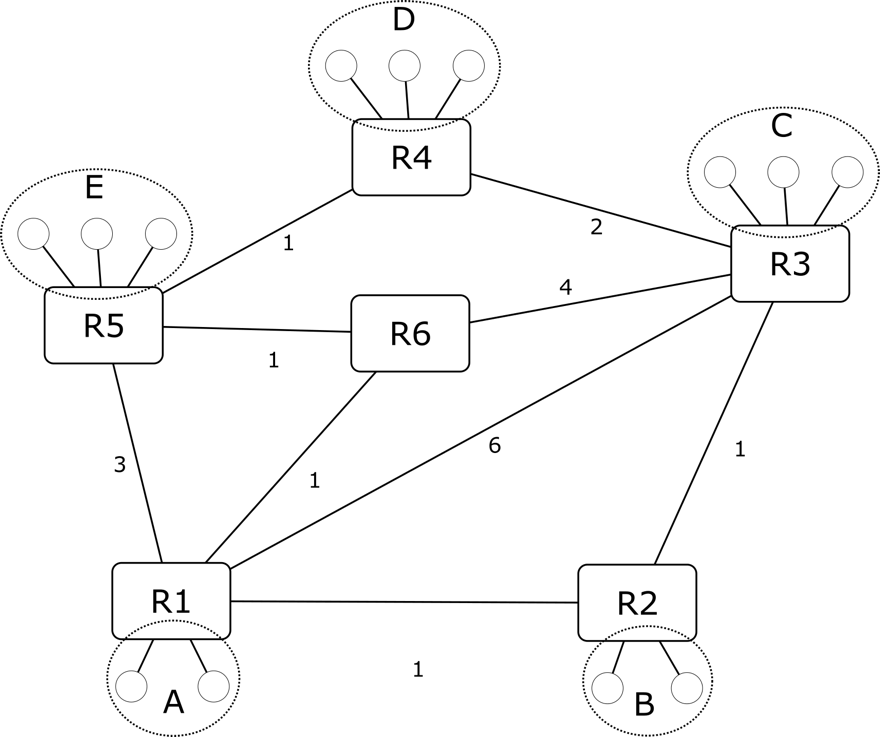
Sehen Sie sich die nachstehende Abbildung genau an und beantworten Sie dann die folgenden Fragen:

1. Welchem Zweck dient das Routing Information Protocol (RIP)?
2. Wie wird die Unterbrechung der Verbindung zwischen R6 und R3 durch das   
   auf R6 und den anderen Routern laufende RIP behandelt?
3. Hauptzweck des RIP ist die Optimierung der Routen bzw. Übertragungspfade (2 P) zu anderen Netzwerksegmenten.
4. R6 stellt zunächst eine Zeitüberschreitung fest, stuft die Verbindung zu R3 daraufhin als nicht verfügbar ein und ändert die eigene Routingtabelle entsprechend (2 P). Anschließend informiert R6 die benachbarten Router R1 und R5 über die vorgenommene Änderung (3 P), was diese ihrerseits zur Anpassung ihrer Routingtabellen veranlasst. Dadurch wird die Änderung letztlich auch von R4, R3 und R2 übernommen (3 P).



**FRAGE 30 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 05**



Sehen Sie sich die abgebildete Netzwerkinfrastruktur genau an und beantworten Sie dann die folgenden Fragen:

1. Wie stellt sich die Routingtabelle des Routers R2 für Netzwerk D dar? Welche Werte sind in dem entsprechenden Distanzvektor enthalten?
2. Wie ändert sich die Routingtabelle von R2, wenn die Verbindung zwischen R1 und R6 unterbrochen wird?
3. Wie aus der Abbildung ersichtlich wird, ist das Ziel D über die Gateways R1 und R3 erreichbar. Somit enthält der Distanzvektor zwei Einträge bzw. Kostenwerte für D: einen Wert von 4 für die Route über R1 (3 P) und einen Wert von 3 für die Route über R3 (3 P).
4. Wenn die Verbindung zwischen R1 und R6 abreißt, steigt der Kostenwert für die Datenübertragung über R1 auf 5 (3 P), während der Kostenwert für R3 unverändert bleibt (1 P).



**FRAGE 31 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 06**



Nennen Sie drei Arten von Einträgen in einer DNS-Datenbank.

Je 2 P Punkte, z. B.: A, AAAA, CNAME, NS, MX, SOA, TXT, SRV



**FRAGE 32 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 06**



1. Was bezeichnet der Begriff „Reverse-Lookup“ im Kontext des DNS?
2. Worin besteht der Unterschied zwischen einem Reverse-Lookup und einer regulären DNS-Abfrage?
3. Bei einem Reverse-Lookup wird ein DNS-Server nach dem FQDN der angegebenen IP-Adresse gefragt (3 P).
4. Im Unterschied dazu geht es bei einer regulären DNS-Abfrage um die Ermittlung der IP-Adresse, die dem angegebenen Klarnamen zugeordnet ist (3 P).



**FRAGE 33 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 06**



1. Geben Sie einen vollqualifizierten Domainnamen (FQDN) mit mindestens vier Komponenten an.
2. Illustrieren Sie die hierarchische Struktur des DNS-Namensraums, indem Sie die verschiedenen Komponenten aus ihrem Beispiel benennen.
3. Beispiel: server21.mail.google.com (2 P) – andere Antworten sind möglich.
4. Dieser FQDN setzt sich aus den folgenden Komponenten zusammen: Top-Level-Domain: com (2 P); Domain: google (2 P); Unterdomäne: mail (1 P); Hostname: server21 (1 P). (Alle Antworten müssen in Bezug auf das gewählte Beispiel zutreffend sein. Die Punkte werden dann zu 50 % für die Nennung des Namens der Komponente und zu 50 % für die korrekte Zuordnung zum gewählten Beispiel vergeben.)



**FRAGE 34 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 06**



Das Sender Policy Framework (SPF) und „Domain-based Message Authentication, Reporting and Conformance“ (DMARC) sind zwei verschiedene Lösungen für ein bestimmtes Problem.

1. Beschreiben Sie das Problem, das mithilfe dieser Ansätze gelöst werden soll.
2. Welche Rolle spielt dabei das Domain Name System?
3. Worin unterscheiden sich die beiden Ansätze?
4. Beide Ansätze dienen der Bekämpfung schädlicher E-Mails, die scheinbar von legitimen Absendern stammen (2 P).
5. SPF und DMARC nutzen das DNS zur Aufbewahrung und Bereitstellung öffentlich zugänglicher Informationen (2 P).
6. Während das SPF die Authentifizierung der Absender verdächtiger E-Mails ermöglicht (2 P), lässt sich mithilfe von DMARC festlegen, was in Reaktion auf verdächtige E-Mails geschehen sollte (2 P).



**FRAGE 35 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 06**



Wie kann ein Client eine autoritative Antwort für den DNS-Namen „[www.amazon.de](http://www.amazon.de/)“ erhalten? Beschreiben Sie die einzelnen Schritte des Vorgangs und benennen Sie dabei die jeweiligen Kommunikationspartner.

Da eine autoritative Antwort verlangt wird, kontaktiert der Client zunächst einen Root-Server (2 P), um die Adresse des DNS-Servers zu erfragen, der für die Top-Level-Domain „de“ zuständig ist (3 P). Anschließend erkundigt sich der Client bei diesem TLD-Server nach dem Nameserver für die Domain „amazon“ (3 P). Dieser dritte Server wird dann im letzten Schritt um die Auflösung des Hostnamens „www“ gebeten (3 P). Seine Antwort auf diese Anfrage ist autoritativ.



**FRAGE 36 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 06**



1. Nennen Sie einen Sicherheitsmechanismus, mit dem sich die Authentizität von DNS-Einträgen sicherstellen lässt.
2. Illustrieren Sie den entsprechenden Verifizierungsprozess anhand eines geeigneten Beispiels.

a) Die Authentizität von DNS-Einträgen lässt sich mit DNSSEC bzw. den DNS-Sicherheitserweiterungen prüfen (2 P für den Namen). b) In der DNSSEC-Infrastruktur werden Signaturen (2 P) der Einträge einer Zone (1 P) aufbewahrt. Das ermöglicht Authentizitätsprüfungen, da jede dieser Signaturen mithilfe des in derselben Zone gespeicherten öffentlichen Schlüssels (2 P) verifiziert werden kann. Zudem lässt sich die Echtheit eines des jeweiligen öffentlichen Schlüssels anhand des entsprechenden Eintrags auf dem übergeordneten DNS-Server prüfen (3 P).



**FRAGE 37 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 07**



Nennen Sie zwei Features von HTTP/2, mit denen Schwächen von HTTP/1.1 behoben werden sollen.

Mehrere Anfrage/Antwort-Interaktionen können synchron bearbeitet werden.

Header werden effizienter codiert.

Anfragen lassen sich priorisieren, damit die wichtigsten Daten zuerst abgerufen werden können.

(Zwei der drei hier aufgeführten Antworten sind ausreichend; je 3 P)



**FRAGE 38 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 07**



Nennen Sie zwei Erweiterungen des SMTP und deren jeweiligen Verwendungszweck.

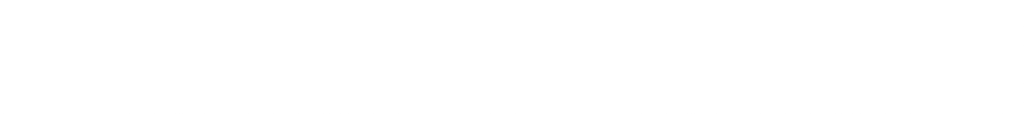
3 P für jede Erweiterung (1 P für den Namen, 2 P für die Beschreibung):

8BITMIME (ermöglicht die Übertragung von Daten in nicht textbasierten Formaten), AUTH (unterstützt die Authentifizierung), STARTTLS (erlaubt die Verschlüsselung einer bestehenden Verbindung)



**FRAGE 39 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 07**



1. Beschreiben Sie ein typisches Einsatzszenario für HTTP.
2. Welche Informationen sind in den hierfür nötigen Anfragen und Antworten jeweils enthalten?
3. Eine Userin nutzt einen Webbrowser, um Informationen (1 P) von einem Webserver (1 P) abzurufen.
4. Der Webbrowser fordert die angegebene URI an (1 P). Zu diesem Zweck nutzt er eine einschlägige Methode (1 P) wie GET/POST/PUSH/DELETE/HEAD, worauf der Server mit einem Statuscode (2 P) und den angeforderten Inhalten (2 P) antwortet.

(Anschließend fordert der Webbrowser weitere Inhalte an, die mit dem ersten Dokument verknüpft sind.)



**FRAGE 40 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 07**



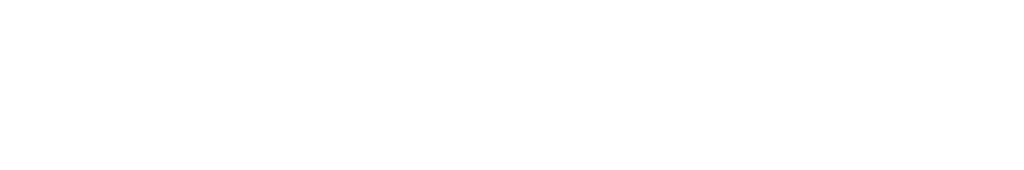
Beschreiben Sie ein typisches Einsatzszenario für SMTP.

Ein E-Mail-Client nutzt SMTP zum Versand einer E-Mail (1 P). Zu diesem Zweck stellt er eine Verbindung zu einem SMTP-Server her und identifiziert sich diesem gegenüber (2 P). Anschließend übermittelt der Client Informationen zu Sender und Empfänger der E-Mail (2 P), gefolgt vom eigentlichen Inhalt der Nachricht (2 P). Daraufhin bestätigt der Server den Erhalt der E-Mail (1 P).



**FRAGE 41 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 07**



1. Warum ist HTTP als zustandsloses Protokoll zu klassifizieren?
2. Was bedeutet das für die Beziehung zwischen den einzelnen Anfragen?
3. Welche Technologie wurde eingeführt, um diese grundlegende Eigenschaft des Protokolls aufzuheben? Erläutern Sie die Gründe dafür.
4. HTTP-Kommunikation basiert auf einem einfachen Anforderung/Antwort-Schema (3 P).
5. Das bedeutet, dass jede eingehende Anfrage vom Server unabhängig von allen vorherigen Anfragen beantwortet werden kann (3 P).
6. Um den aktuellen Stand eines HTTP-basierten Dialogs abzubilden, werden Cookies verwendet (3 P). Sie ermöglichen die Speicherung von Statusinformationen und fungieren unter anderem als Basis der digitalen Einkaufswagen von Onlinehändlern (1 P).



**FRAGE 42 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 07**



Warum lässt sich die Interaktion eines HTTP-Clients mit einem HTTP-Server relativ leicht verfolgen, wenn dafür das unverschlüsselte HTTP/1.1 verwendet wird? (**Hinweis**:Stellen Sie heraus, wie Anfragen und Antworten in diesem Szenario übertragen werden, und beleuchten Sie die Rolle des untergeordneten Protokolls.)

HTTP/1.1 ist ein textbasiertes (2 P) Protokoll, das die Wiederverwendung (2 P) einer TCP-Verbindung für mehrere aufeinanderfolgende Anfragen an denselben Server gestattet. Das bedeutet, dass die aufeinanderfolgenden Anfragen eines Clients alle derselben TCP-Verbindung zugeordnet und nacheinander bearbeitet werden (3 P). Somit kann jeder Beobachter die einzelnen Schritte der Interaktion des Clients mit dem Server anhand der TCP-Sequenznummern nachvollziehen (3 P).



**FRAGE 43 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 08**



Nennen Sie drei Designziele von IPsec (Security Architecture for IP).

Je 2 P für: Zugangskontrolle, Integrität, Ursprungsauthentifizierung, Erkennung/Abwehr von Replay-Angriffen, Vertraulichkeit



**FRAGE 44 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 08**



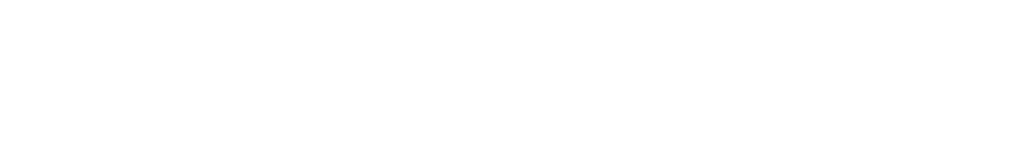
Nennen Sie die drei Designziele von Transport Layer Security (TLS).

Authentifizierung (2 P), Vertraulichkeit (2 P), Integrität (2 P)



**FRAGE 45 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 08**



Bei der Implementierung von IPsec können die Sicherheitsverantwortlichen zwischen zwei Betriebsmodi wählen.

1. Nennen Sie die beiden Betriebsmodi.
2. Erläutern Sie, worin der Hauptunterschied zwischen ihnen besteht.
3. Transportmodus (2 P) und Tunnelmodus (2 P).
4. Im Transportmodus werden nur die IP-Nutzdaten verschlüsselt (2 P). Im Tunnelmodus werden hingegen komplette Pakete verschlüsselt und in neuen IP-Paketen gekapselt (2 P).



**FRAGE 46 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 08**



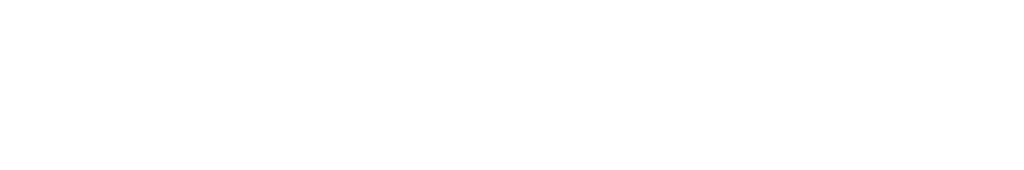
Ein von zu Hause arbeitender Netzwerkadministrator möchte über ein Remotedesktop-Tool auf einen Anwendungsserver zugreifen. Allerdings ist der Zugang zu dem fraglichen System nur aus der unternehmensinternen Umgebung gestattet.

1. Wie kann der Administrator sein Ziel dennoch erreichen, wenn er das aufwendige Genehmigungsverfahren für neue Firewallregeln vermeiden möchte und bereits Zugriff auf einen SSH-Server in der Infrastruktur des Unternehmens hat?
2. Wie wahrscheinlich löst dieser Vorgang einen Sicherheitsalarm des Intrusion-Detection-Systems aus?
3. Der Administrator kann eine lokale Portweiterleitung einrichten (2 P), um den SSH-Server als Proxyserver (2 P) für den Zugriff auf den Anwendungsserver zu nutzen.
4. Ob der Vorgang einen Sicherheitsalarm auslöst, hängt im Wesentlichen von der Konfiguration des IDS ab: Einerseits handelt es sich hier nicht um ein Angriffsmuster (2 P), andererseits ist es möglich, dass in diesem Szenario eine ungewöhnlich hohe Auslastung des betreffenden SSH-Dienstes registriert wird (2 P).



**FRAGE 47 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 08**



Ein Unternehmen benötigt ein gültiges Zertifikat für einen Webserver. Beschreiben Sie den Prozess der Beantragung und Ausstellung eines solchen Zertifikats im Detail.

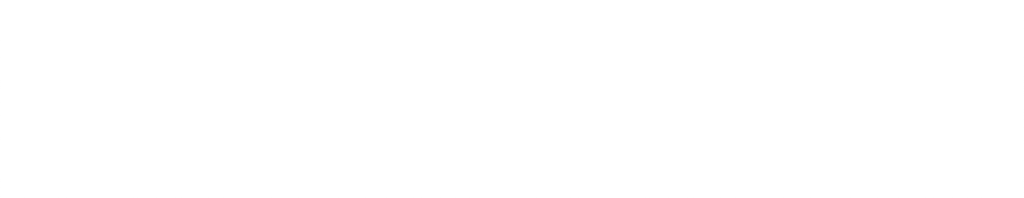
(**Hinweis**:Geben Sie dabei genau an, wer der Inhaber des Zertifikats ist, und welche Partei welche Informationen an wen schickt.)

Der Webserver ist der spätere Inhaber („subject“) des Zertifikats (1 P). Seine Beantragung beginnt damit, dass das Unternehmen ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, erzeugt (1 P). Anschließend erstellt das Unternehmen eine Signaturanforderung (CSR), die alle relevanten Informationen über den Webserver (1 P) und den neuen öffentlichen Schlüssel (1 P) enthält. Diese Signaturanforderung geht dann an eine Zertifizierungsstelle (1 P), die die darin enthaltenen Angaben prüft (1 P) und sie (d. h. die CSR) in ein Zertifikat umwandelt (1 P), indem sie sie mit ihrem privaten Schlüssel signiert (2 P). Anschließend wird das Zertifikat an das Unternehmen übermittelt und kann von diesem dann auf dem Webserver installiert werden (1 P).



**FRAGE 48 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 08**



Eine Hackergruppe führt während eines Diffie-Hellman-Schlüsselaustauschs einen Man-in-the-Middle-Angriff durch.

1. Welche Voraussetzung muss hierfür gegeben sein?
2. In welchen Schritten läuft der Angriff ab?
3. Was ist das Endergebnis der Attacke?
4. Man-in-the-Middle-Angriffe auf höhere Ebenen setzen einen erfolgreichen Man-in-the-Middle-Angriff auf eine der unteren Schichten bzw. auf die Routinginfrastruktur voraus: Die Angreifer:innen müssen zunächst dafür sorgen, dass die an ein Zielsystem adressierten IP-Pakete auf ein von ihnen kontrolliertes System umgeleitet werden (2 P).
5. Die Angreifer:innen schlüpfen in die Rolle des Severs (2 P) und nehmen die Verbindungsanfrage eines Clients an (1 P). Dann stellen sie ihrerseits eine Verbindung zwischen ihrem System und dem Server her (1 P), wofür sie ihren eigenen öffentlichen Schlüssel nutzen (2 P).
6. Am Ende haben die Angreifer:innen zwei voneinander unabhängige sichere Kommunikationskanäle eingerichtet – einen zwischen dem Client und ihrem System, einen anderen zwischen ihrem System und dem Server (2 P).



**FRAGE 49 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 09**



Nennen Sie zwei sicherheitsrelevante Eigenschaften signaturbasierter Intrusion-Detection-Systeme.

Je 3 P für: signaturbasierte Systeme sind effizient; signaturbasierte Systeme sind nicht in der Lage, unbekannte Angriffe aufzudecken; signaturbasierte Systeme geben nur wenige Fehlalarme aus.



**FRAGE 50 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 09**



Nennen Sie zwei zentrale Funktionen eines SIEM-Systems.

Je 3 P für: die Integration und Konsolidierung von Sicherheitsdaten; die datengestützte Erstellung eines Überblicks über die Sicherheitslage; die Zusammenführung der Protokolldaten diverser Systeme; die Bereitstellung einer zentralen Datenbank für die Erfassung und Aufbewahrung von Beweismitteln



**FRAGE 51 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 09**



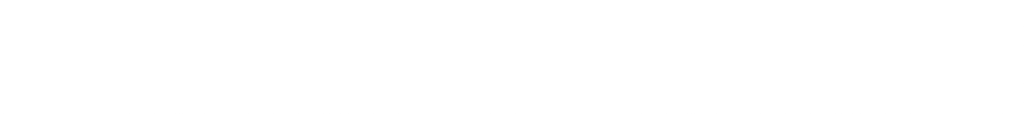
Ein geschäftskritisches Anwendungssystem soll streng überwacht werden. Welche Art von Intrusion-Detection-System ist für diesen Zweck am besten geeignet? Erläutern Sie Ihre Antwort.

Die Verantwortlichen sollten ein hostbasiertes IDS nutzen (2 P), weil es detaillierte Einblicke in die Aktivitäten auf dem betreffenden System ermöglicht (3 P) und außerdem die Aufdeckung von Insider-Angriffen unterstützt (3 P).



**FRAGE 52 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 09**



Nennen und beschreiben Sie zwei verdächtige Ereignisse, die sich durch eine Analyse des Datenflusses im Netzwerk aufdecken lassen. Geben Sie für jedes genannte Beispiel an, welche schädlichen Aktivitäten sich dahinter verbergen könnten.

2 P für die Nennung/Beschreibung jedes Ereignisses, 2 P für die Angabe der dazu passenden schädlichen Aktivitäten:

Plötzlicher Anstieg des Netzwerktraffics – mögliches Indiz für die Ausschleusung von Daten;

Ungewöhnlich starke Nutzung eines gängigen Protokolls – mögliches Indiz für getarnte Kommunikation;

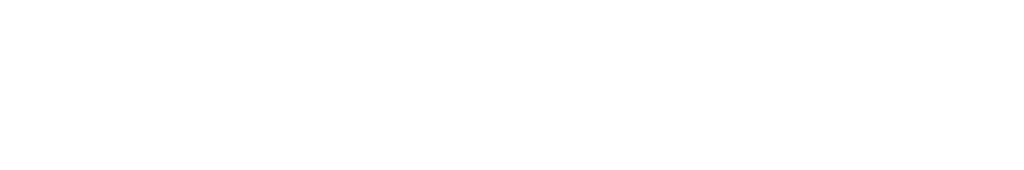
Ungültige TCP-Sequenznummern – mögliches Indiz für einen RST-Angriff oder Session-Hijacking:

Nutzung ungewöhnlicher Ports (statt der Standardports des fraglichen Protokolls) – mögliches Indiz für verborgene Kommunikationskanäle



**FRAGE 53 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 09**

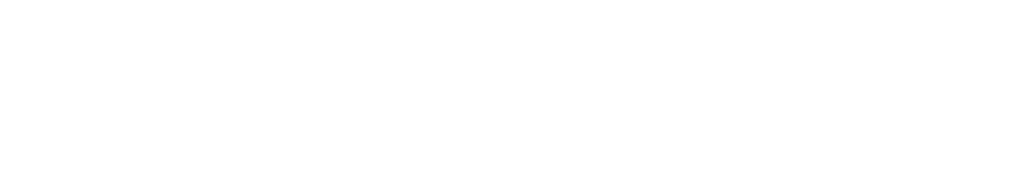


1. Was wird im Kontext von Cybersicherheitsereignissen als Fehlalarm bezeichnet?
2. Wie lassen sich Fehlalarme zur Verbesserung der Cybersicherheit nutzen?
3. Illustrieren Sie anhand eines geeigneten Beispielsszenarios, wie ein solcher Fehler aufgedeckt wird und anschließend behoben werden kann.
4. Ein Fehlalarm liegt vor, wenn eine Warnmeldung irrtümlich als Sicherheitsereignis eingestuft wurde (2 P).
5. Eine Analyse der ausgegebenen Fehlalarme ermöglicht die Optimierung der implementierten Regeln/Richtlinien/Sensoren (2 P).
6. 3 P für ein passendes Szenario (z. B. IDS-Meldungen über ungewöhnliche Systemzugriffe, die letztlich auf die kürzlich erfolgte Implementierung neuer Unternehmensprozesse zurückzuführen sind), 3 P für geeignete Behebungsmaßnahmen (z. B. eine Anpassung der IDS-Regeln an die neuen Unternehmensprozesse, begleitet von einer genauen Untersuchung der Auswirkungen auf die Sicherheit).



**FRAGE 54 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 09**



1. Was wird im Kontext von Cybersicherheitsereignissen als Falsch-negativ-Fehler bezeichnet?
2. Wie lassen sich solche Fehler aufspüren?
3. Illustrieren Sie anhand eines geeigneten Beispielsszenarios, wie ein solcher Fehler aufgedeckt wird und anschließend behoben werden kann.
4. Ein Falsch-negativ-Fehler liegt dann vor, wenn ein verdächtiger Vorgang fälschlicherweise nicht als Sicherheitsereignis erkannt bzw. eingestuft wurde (2 P).
5. Falsch-negativ-Fehler können aufgespürt werden, indem die Sicherheitsverantwortlichen verdächtige Aktivitäten simulieren, die eigentlich ein Sicherheitsereignis auslösen sollten (3 P).
6. Beispielsweise kann sich während einer Sicherheitsübung zeigen, dass die Umgehung einer Firewall durch das zuständige IDS nicht erkannt wird (2 P für ein geeignetes Beispiel). Mögliche Maßnahmen zur Behebung dieser Sicherheitslücke sind die Anpassung der IDS-Regeln sowie die Aktualisierung oder Ersetzung der anfälligen Firewall (3 P für effektive Behebungsmaßnahmen).



**FRAGE 55 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 10**



Nennen Sie drei relevante Dimensionen von Cybersicherheitsdaten.

Je 2 P für: Schweregrad der gemeldeten Ereignisse; betroffene Netzwerksegmente; Stellenwert der betroffenen Systeme; geltende gesetzliche Datenschutzvorgaben; geografischer Standort; Betriebssystem und Version; Zugänglichkeit der betroffenen Software und Dienste; Gerätetyp; Art des Traffics; Zeitdaten



**FRAGE 56 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 10**



Nennen Sie drei Verfahren zur Datenklassifizierung, die auf Cybersicherheitsdaten angewendet werden können.

(Je 2 P für) Naiver Bayes-Klassifikator; Bayessche Netze; Markov-Ketten; Entscheidungsbaumalgorithmen; Stützvektormaschinen; künstliche neuronale Netze



**FRAGE 57 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 10**



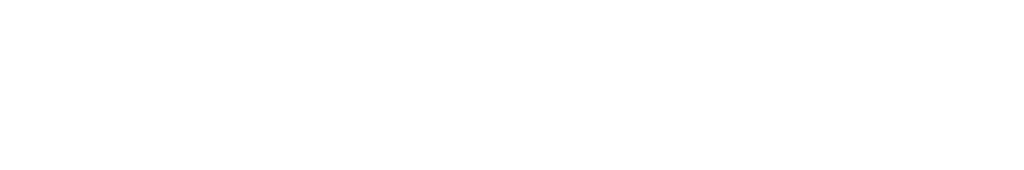
Ein verhaltensbasiertes Intrusion-Detection-System gibt eine Warnmeldung über verdächtige Netzwerkaktivitäten aus. Die nähere Untersuchung der Ursachen der Anomalie führt zu einer Workstation, die Verbindungen zu einer IP-Adresse aus einer DNS-Sperrliste aufzubauen sucht.

1. Was sind DNS-Sperrlisten (DNSBLs)?
2. Was sagt ein entsprechender Eintrag über die fragliche IP-Adresse aus?
3. Welche zwei Maßnahmen sollten in der Folge eingeleitet werden?
4. DNS-Sperrlisten enthalten Adressen, die in der Vergangenheit in den Versand von Spam-E-Mails involviert waren (2 P).
5. Dementsprechend sind die gelisteten Adressen als nicht vertrauenswürdig einzustufen.
6. Die Verantwortlichen sollten die Kommunikation blockieren (2 P) und die betreffende Workstation auf Malware untersuchen (2 P).



**FRAGE 58 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 10**



DNS-Daten ändern sich ständig.

1. Was ist der Grund dafür?
2. Wie wirkt sich das auf forensische Untersuchungen aus?
3. Welche zwei Datenquellen können in der Netzwerkforensik zur Behebung dieses Problems genutzt werden?
4. Das Domain Name System ist im Grunde eine verteilte Datenbank (2 P). In den verschiedenen DNS-Zonen werden im Rahmen des Normalbetriebs ständig Einträge hinzugefügt, verändert und entfernt (2 P).
5. Daher können sich die DNS-Daten, die für die forensische Untersuchung eines Vorfalls relevant sind, schon vor Beginn der Untersuchung geändert haben (2 P).
6. Die zum Zeitpunkt des Vorfalls aktuellen DNS-Daten können aus Speichern für passive DNS-Daten oder DNS-Repositories abgerufen werden (2 P).



**FRAGE 59 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 10**



Ein netzwerkbasiertes Intrusion-Detection-System meldet schädlichen Traffic, dessen Ursprung außerhalb des Unternehmens liegt. Da die betreffenden Datenströme mutmaßlich von einem aus kompromittierten Systemen bestehenden Botnetz ausgehen, werden die vorhandenen Firewalls so konfiguriert, dass sie den Traffic blockieren.

1. Welche weiteren Maßnahmen sollten ergriffen werden, um diesen Angriff zu unterbinden?
2. Welche anderen Stakeholder sind in den Vorfall involviert?
3. Wie lassen sich ihre Identitäten und Kontaktdaten ermitteln?
4. Das Sicherheitsteam sollte versuchen, die Quelle des Angriffs trockenzulegen (2 P).
5. Zu diesem Zweck sollte es die Organisationen, von deren Infrastruktur der Angriff ausgeht (3 P), über den Vorfall informieren.
6. Eine Identifizierung ist über die AS-Nummern möglich (3 P), die als Bindeglied zwischen den kompromittierten IP-Adressblöcken und den verantwortlichen Organisationen fungieren (2 P).



**FRAGE 60 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 10**



Gewiefte Hackergruppen bringen bei jedem Angriff maßgeschneiderte Malwarevarianten zum Einsatz. Das erschwert eine Erkennung durch signaturbasierte Sicherheitssysteme.

1. Welche Art von Methoden ermöglicht die Aufdeckung solcher unbekannten Bedrohungen?
2. Nennen Sie ein einschlägiges Verfahren und beschreiben Sie dieses, indem Sie die folgenden Fragen beantworten:
3. Welchem Zweck dient die genannte Methode?
4. Welche Voraussetzung muss gegeben sein, damit die Methode effektiv ist?
5. Warum muss diese Voraussetzungen gegeben sein?
6. Auf maschinellem Lernen basierende Methoden (2 P) ermöglichen die Erkennung bisher unbekannter Malware.
7. In diese Kategorie fallen unter anderem Entscheidungsbaumalgorithmen (2 P für ein passendes Beispiel).
8. Diese werden zur Klassifizierung genutzt (2 P für den korrekten Einsatzzweck).
9. Voraussetzung hierfür sind geeignete Trainingsdaten (2 P).
10. Letztere sind notwendig, weil es sich um eine überwachte Lernmethode handelt (2 P).





**FRAGE 61 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 01**



Die mit forensischen Methoden gesammelten Daten müssen ...

**Wählen Sie eine Antwort:**

|  |
| --- |
| ... anonymisiert werden. |
| ... konkrete Folgemaßnahmen benennen. |
| *... vor Gericht als Beweismittel taugen.* |
| ... die mutmaßlichen Angreifer:innen identifizieren. |



**FRAGE 62 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 01**



Wireshark ist ...

**Wählen Sie eine Antwort:**

|  |
| --- |
| ... ein Intrusion-Detection-System. |
| ... Datensystem zur Archivierung forensischer Daten. |
| *... ein Tool zur Analyse des Netzwerktraffics.* |
| ... ein SIEM-System. |





**FRAGE 63 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 01**



Angreifer:innen versuchen üblicherweise, ihre Spuren auf kompromittierten Systemen zu verwischen. Dabei können von solchen Manipulationsversuchen auch Sicherheitssysteme betroffen sein.

Welcher Schritt aus dem allgemeinen Prozessmodell der Netzwerkforensik zielt auf die Verhinderung der Manipulation von Beweismitteln?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Prüfung |
| *Beweissicherung* |
| Erkennung |
| Datensammlung |



**FRAGE 64 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 01**



Das allgemeine Prozessmodell der Netzwerkforensik enthält einen Schritt, welcher der Auswahl der relevanten Daten aus den gesammelten forensischen Informationen gewidmet ist.

Wie lautet die Bezeichnung für diesen Schritt?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Datensammlung |
| Beweissicherung |
| Erkennung |
| *Prüfung* |





**FRAGE 65 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 01**



Ein Intrusion-Detection-System hat einen nicht genehmigten Zugriff auf eine interne Forschungsdatenbank festgestellt.

Eine genauere Untersuchung der Meldung zeigt, dass es sich beim Urheber des Vorgangs um einen externen Gast handelt, der die nötigen Zugangsdaten von dem verantwortlichen Team erhalten hat und sich lediglich ein Bild von dessen Ergebnissen machen wollte.

Wie ist dieser Vorgang einzustufen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| als Sicherheitswarnung |
| als Fehlalarm |
| als Sicherheitsereignis |
| *als Sicherheitsvorfall* |



**FRAGE 66 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 01**



Ein Intrusion-Detection-System hat einen nicht genehmigten Zugriff auf eine interne Forschungsdatenbank festgestellt.

Eine genauere Untersuchung der Meldung zeigt, dass die Anomalie aufgetreten ist, weil ein Mitglied des Forschungsteams einen anderen Computer benutzen musste.

Wie ist dieser Vorgang einzustufen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| als Sicherheitswarnung |
| als Sicherheitsereignis |
| *als Fehlalarm* |
| als Sicherheitsvorfall |





**FRAGE 67 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 02**



Welchen wichtigen Zweck erfüllt die Transportschicht?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Sicherstellung der Integrität der übertragenen Daten |
| *Markierung der miteinander kommunizierenden Prozesse* |
| Markierung der miteinander kommunizierenden Geräte |
| Übersetzung der ausgetauschten Informationen in eine systemunabhängige Form |



**FRAGE 68 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 02**



Verbindungsorientierte Protokolle ...

**Wählen Sie eine Antwort:**

|  |
| --- |
| ... stellen einen Kanal für die asynchrone Kommunikation bereit. |
| ... zeichnen sich im Vergleich zu verbindungslosen Protokollen durch einen geringeren Overhead aus. |
| ... überlassen der Anwendungsschicht die Wiederherstellung der ursprünglichen Paketreihenfolge. |
| *... stellen einen Kanal für die synchrone Kommunikation bereit.* |





**FRAGE 69 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 02**



Ein Anwendungsprotokoll soll kurze Nachrichten so schnell wie möglich an eine große Zahl von Empfängern senden.

Dabei sind einzelne Nachrichten verzichtbar, solange die relevanten Zeitbeschränkungen eingehalten werden. Welche Art von untergeordnetem Protokoll sollte das Anwendungsprotokoll in diesem Fall nutzen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| ein auf der Netzwerkschicht residierendes Protokoll |
| ein auf der Verbindungsschicht residierendes Protokoll |
| *ein verbindungsloses Protokoll* |
| ein verbindungsorientiertes Protokoll |



**FRAGE 70 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 02**



Internetstandards werden von der IETF in RFC-Dokumenten veröffentlicht. Was passiert, wenn ein Standard von Grund auf überarbeitet werden muss?

**Wählen Sie eine Antwort:**



|  |
| --- |
| Die neuen Mechanismen und Methoden werden in das bestehende RFC-Dokument eingepflegt. Anschließend werden alle von den Änderungen Betroffenen über die Neuerungen informiert. |
| Eine überarbeitete Version des RFC-Dokuments wird erstellt und muss dann von allen verantwortlichen IT-Teams unmittelbar umgesetzt werden. |
| *Ein Standardisierungsentwurf wird erstellt und als neues RFC-Dokument veröffentlicht.* |
| Ein neues RFC-Dokument wird erstellt und die vorherige Version wird aus dem RFC-Archiv entfernt. |





RFC 1149 beschreibt die Übermittlung von IP-Paketen durch „gefiederte Träger“.

2001 wurde der Standard erstmals genutzt, um ICMP-Ping-Nachrichten ohne Änderung des Internet Protocol (IP) mithilfe von Brieftauben zu übermitteln. Welche Schicht aus dem TCP/IP-Referenzmodell wurde auf diese Weise implementiert?

**Wählen Sie eine Antwort:**



**FRAGE 71 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 02**

|  |
| --- |
| die Transportschicht |
| die Anwendungsschicht |
| die Internet-/Netzwerkschicht |
| *die Verbindungsschicht* |



**FRAGE 72 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 02**



Das „Echo“-Protokoll ist ein Anwendungsprotokoll, das alle empfangenen Daten an den Absender zurückschickt.

Welche Schicht des TCP/IP-Modells speichert die Adresse, an welche die Antwortnachricht gesendet werden soll?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *die Internet-/Netzwerkschicht* |
| die Verbindungsschicht |
| die Anwendungsschicht |
| die Transportschicht |





**FRAGE 73 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 03**



Welche der genannten Informationen finden sich im UDP-Header?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *Quell- und Zielport* |
| Sequenznummer |
| Länge des Headers |
| Bestätigungsnummer |



**FRAGE 74 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 03**



*Ein SOCKS-Proxy ...*

**Wählen Sie eine Antwort:**

|  |
| --- |
| ... versendet Broadcastnachrichten, um andere SOCKS-Proxies zu identifizieren. |
| ... wehrt Denial-of-Service-Angriffe ab. |
| ... trennt Netzwerksegmente auf der Netzwerkschicht und setzt Zugriffsregeln durch. |
| *... überträgt Daten im Auftrag anderer Systeme.* |





**FRAGE 75 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 03**



Wie läuft ein UDP-Reflection-Angriff ab?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Die Angreifer:innen fangen den UDP-Traffic eines legitimen Servers ab und leiten ihn auf ein von ihnen kontrolliertes System um. Anschließend werden die so erbeuteten Datenpakete analysiert und nach nützlichen Informationen über die Netzwerkinfrastruktur des Opfers durchsucht. |
| Die Angreifer:innen übermitteln gespoofte Pakete an eine bekannte Adresse des Opfers. Daraufhin sendet das betreffende Empfängersystem wahllos Antworten an andere Systeme in der Umgebung. Diese antworten ihrerseits mit Fehlermeldungen, welche die Netzwerkinfrastruktur des Opfers stark auslasten. |
| Die Angreifer:innen senden gespoofte Pakete an einen legitimen Server, der darauf mit Antwortnachrichten reagiert. Letztere werden von den Kriminellen gescannt und nach Hinweise n auf veraltete Software mit bekannten Schwachstellen (in der Netzwerkinfrastruktur des Opfers) durchsucht. |
| *Die Angreifer:innen schicken gespoofte Pakete an einen legitimen Server, der darauf mit dem Versand von Antwortnachrichten an die Adresse des eigentlichen Angriffsziels reagiert. Da diese Antwortnachrichten zusätzliche Daten enthalten, wird die Netzwerkinfrastruktur des Opfers stark ausgelastet.* |



**FRAGE 76 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 03**



Wie stellt TCP fest, dass Datenpakete fehlen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *Der Sender verfügt über einen Timer für jedes Segment im Sendepuffer . Geht innerhalb der festgelegten Frist keine Empfangsbestätigung ein, wird der Übertragungsvorgang wiederholt.* |
| Der Empfänger verfügt über einen Timer für jedes Segment im Empfangspuffer. Geht das nächste Segment des Datenstroms nicht innerhalb der festgesetzten Frist ein, wird der Sender aufgefordert, dieses erneut zu übermitteln. |
| Der Sender verfügt über einen Timer für jedes Segment im Empfangspuffer. Geht innerhalb der festgelegten Frist keine Bestätigungsnachricht ein, wird der Übertragungsvorgang wiederholt. |
| Der Empfänger verfügt über einen Timer für jedes Segment im Sendepuffer. Geht das nächste Segment des Datenstroms nicht innerhalb der festgesetzten Frist ein, wird der Sender aufgefordert, dieses erneut zu übermitteln. |





**FRAGE 77 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 03**



Eine Administratorin nutzt ein Remotedesktop-Tool, das ihre Befehle in unverschlüsselter Form an ein Serversystem übermittelt.

Welche Angriffsmethode versetzt Hacker:innen unter diesen Bedingungen unmittelbar in die Lage, Code per Fernzugriff auszuführen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *TCP-Session-Hijacking* |
| TCP-RST-Angriff |
| UDP-Reflection-Angriff |
| TCP-SYN-Flood-Angriff |



**FRAGE 78 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 03**



Anwendungen für das Internet der Dinge (IoT) verknüpfen viele verschiedene Sensoren und Aktoren, die über eingebettete Hardware angesteuert werden.

Warum bietet sich hier der Einsatz des UDP an?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *Über UDP-Broadcastnachrichten können verschiedenartige Systeme miteinander kommunizieren, ohne dass dies mit einem hohen Konfigurationsaufwand verbunden ist.* |
| Da das UDP die Integrität der übertragenen Nachrichten sicherstellt, erreichen alle Sensordaten ihr Ziel ohne Verzerrungen oder Verluste. |
| Da die TCP-Nachrichtenübermittlung mit einem hohen Rechenaufwand vverbunden ist, erreichen TCP-basierte eingebettete Systeme nicht die für IoT-Anwendungen nötigen Durchsatzraten. |
| Da die UDP-Kommunikation nur mit einem relativ geringen Rechenaufwand verbunden ist, gehen UDP-Nachrichten stets in der korrekten Reihenfolge ein, was wiederum eine rasche Reaktion auf die darin enthaltenen Sensordaten ermöglicht. |



**FRAGE 79 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 04**



Wie kann ein Router feststellen, ob eine IP-Adresse dem lokalen Netzwerksegment zugehörig ist?

**Wählen Sie eine Antwort:**

|  |
| --- |
| IP-Adressen bestehen aus einer Netzwerkkennung und einer Hostkennung. Somit lässt sich anhand der für den Router konfigurierten ARP-Tabelle feststellen, ob die Netzwerkkennung der fraglichen IP-Adresse mit der Netzwerkkennung des Routers übereinstimmt. |
| Die Routingtabelle des Routers enthält einen Eintrag für den IP-Adressbereich des lokalen Netzwerksegments. |
| Der Router verfügt über eine statisch konfigurierte Liste aller I P-Adressen aus dem lokalen Netzwerksegment. |
| *IP-Adressen bestehen aus einer Netzwerkkennung und einer Hostkennung. Somit lässt sich anhand der für den Router konfigurierten Subnetzmaske feststellen, ob die Netzwerkkennung der fraglichen IP-Adresse mit der Netzwerkkennung des Routers übereinstimmt.* |



**FRAGE 80 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 04**



Das SOCKS-Protokoll ...



**Wählen Sie eine Antwort:**

|  |
| --- |
| ... ermöglicht die Implementierung einer verschlüsselten Transportschicht. |
| ... ist ein Hilfsprotokoll für die Übermittlung von Statusmeldungen. |
| ... ist ein Nachfolger von HTTP mit verbesserter Leistung. |
| *... kann für Cyberangriffe missbraucht werden.* |





**FRAGE 81 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 04**



Welchem Zweck dient das ICMP?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *ICMP ist ein Hilfsprotokoll für die Übermittlung von Statusmeldungen auf der Netzwerkschicht.* |
| ICMP ist ein Signaturprotokoll zur Authentifizierung von IP-Paketen. |
| ICMP ist ein Integritätsprotokoll zur Übermittlung von Prüfsummen für UDP-Datagramme. |
| ICMP ist ein Handshake-Protokoll zur Einrichtung von TCP-Verbindungen. |



**FRAGE 82 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 04**



Die „Dual Stack Lite“-Angebote einiger Internetprovider bieten Unternehmen die Möglichkeit, wertvolle IPv4-Adressen zu sparen.

Dabei erhalten alle Endbenutzer:innen öffentliche IPv6-Adressen, können aber trotzdem auf IPv4-Dienste zugreifen.

Welche Technologie kommt hier in spezieller Form zur Anwendung?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Routing |
| Proxy-Kommunikation |
| *Netzwerkadressübersetzung* |
| Firewallfilter |





**FRAGE 83 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 04**



Ein System hat die IPv4-Adresse 172.16.20.1. Was lässt sich aus dieser Tatsache schließen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *Das System ist Teil eines Netzwerks mit der Standardsubnetzmaske 255.255.0.0.* |
| Das System hat seine Adresse durch automatische IPv4-Konfiguration erhalten. |
| Das System kann Datenpakete direkt an Internetadressen senden. |
| Das System gehört einem Netzwerksegment mit maximal 253 weiteren Systemen an. |



**FRAGE 84 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 04**

Bei welchem der folgenden Vorschläge handelt es sich um eine tatsächlich mögliche Firewallregel?



**Wählen Sie eine Antwort:**

|  |
| --- |
| ERLAUBE alle von der IP-Adresse Y ausgehenden UDP-Verbindungen. |
| *BLOCKIERE alle auf Port 80 eingehenden TCP-Verbindungen aus dem Netzwerksegment X.* |
| BLOCKIERE alle ausgehenden TCP-Verbindungen, die die Zeichenfolge „password“ enthalten. |
| ERLAUBE alle erfolgreich authentifizierten eingehenden HTTP-Verbindungen aus dem Netzwerksegment X. |





Welche Folgen hat ein TCP-RST-Angriff auf einen BGP-Router?

**Wählen Sie eine Antwort:**



**FRAGE 85 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 05**

|  |
| --- |
| Der Router und sein Peer gehen davon aus, dass die Verbindung dauerhaft unterbrochen ist. |
| Der Router und sein Peer gehen davon aus, dass die Verbindung weiterhin besteht, was den Angreifer:innen die Möglichkeit bietet, die Kommunikation zu belauschen. |
| *Der Router und sein Peer gehen davon aus, dass die Verbindung unterbrochen ist und zu einem späteren Zeitpunkt wiederhergestellt werden kann.* |
| Der Router und sein Peer gehen davon aus, dass die Verbindung weiterhin besteht, auch wenn sie unterbrochen ist. |





**FRAGE 86 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 05**

Welche der folgenden Aussagen über AS-Nummern ist zutreffend?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Jede AS-Nummer wird einem bestimmten BGP-Router zugewiesen. |
| Jede AS-Nummer wird einer bestimmten Person zugewiesen. |
| Jede AS-Nummer wird einem zusammenhängenden I P-Adressblock zugewiesen. |
| *Jede AS-Nummer wird einer bestimmten Organisation zugewiesen.* |





**FRAGE 87 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 05**



Eine ARP-Tabelle dient als Speicher für ...

**Wählen Sie eine Antwort:**

|  |
| --- |
| ... die bekannten IP-Adressblöcke statisch konfigurierter Routingtabellen. |
| *... die bekannten MAC-Adressen, die lokalen IP-Adressen zugeordnet sind.* |
| ... BGP-Richtlinien und -Regeln. |
| ... die Distanzvektoren von Routersystemen. |



**FRAGE 88 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 05**



Zwei Organisationen möchten sich gegenseitig ihre jeweiligen Netzwerkinfrastrukturen für den Zugriff auf das Internet zur Verfügung stellen.

Unter welchen Voraussetzungen kann das Border Gateway Protocol für diesen Zweck genutzt werden?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Jede der beiden Organisationen muss über einen Domainnamen verfügen. |
| Jede der beiden Organisationen muss eine ARP-Tabelle erstellt haben. |
| Jede der beiden Organisationen muss eine Routingtabelle erstellt haben. |
| *Jede der beiden Organisationen muss über eine AS-Nummer verfügen.* |



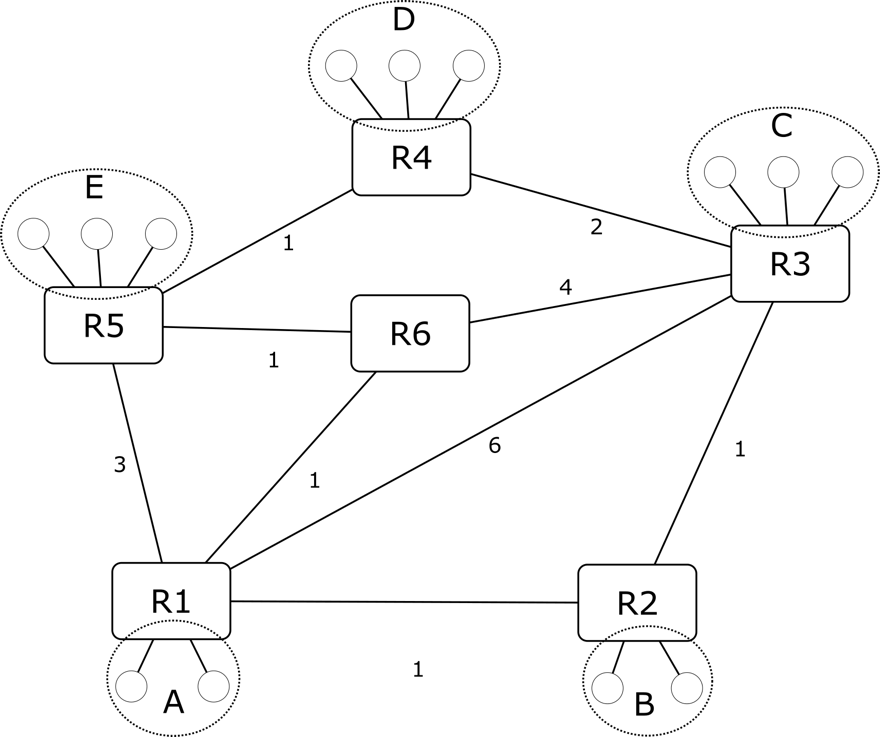


**FRAGE 89 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 05**



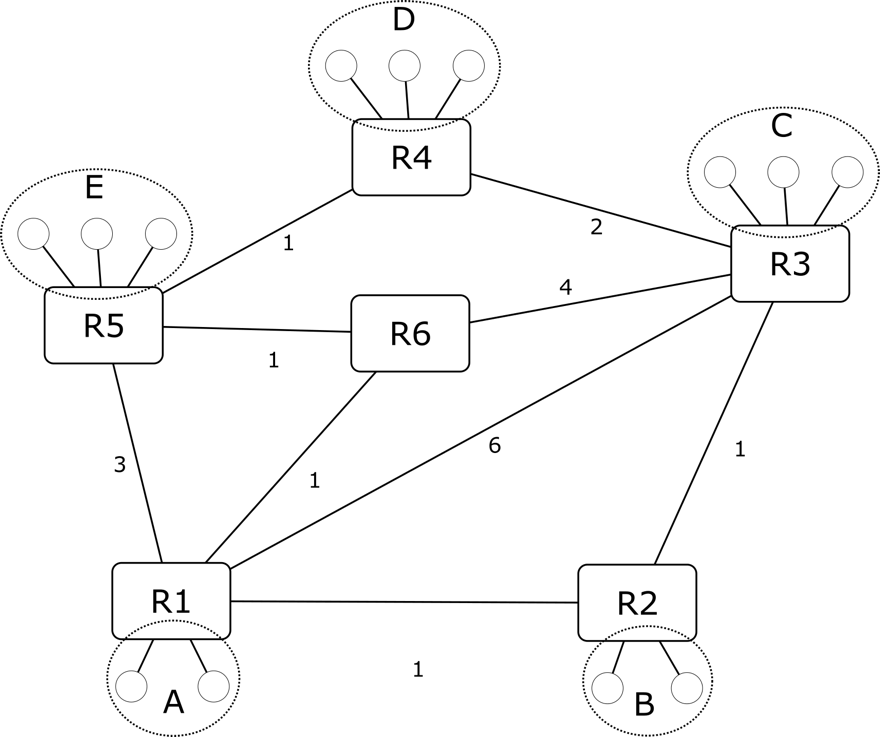
Sehen Sie sich die abgebildete Netzwerkinfrastruktur genau an: An welchen benachbarten Router würde R1 ein IP-Paket übermitteln, das an ein System aus Netzwerk D adressiert ist?



**Wählen Sie eine Antwort:**

|  |
| --- |
| Router 3 |
| Router 5 |
| *Router 6* |
| Router 2 |





Sehen Sie sich die abgebildete Netzwerkinfrastruktur genau an: An welchen benachbarten Router würde R3 ein IP-Paket übermitteln, das an ein System aus Netzwerk A adressiert ist?

**Wählen Sie eine Antwort:**



**FRAGE 90 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 05**

|  |
| --- |
| Router 4 |
| *Router 2* |
| Router 1 |
| Router 6 |





**FRAGE 91 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 06**



Was ist eine DNS-Zone?

**Wählen Sie eine Antwort:**

|  |
| --- |
| eine Datenbank mit sämtlichen Informationen einer regionalen Internet- Registrierungsstelle |
| eine Tabelle auf einem DNS-Server |
| *ein abgegrenzter Zuständigkeitsbereich* |
| eine IP-Adresse, die einem vollqualifizierten Domainnamen (FQDN) zugeordnet ist |



**FRAGE 92 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 06**



Welcher der folgenden DNS-Einträge wird im Rahmen der DNS-Sicherheitserweiterungen (DNSSEC) genutzt?

**Wählen Sie eine Antwort:**

|  |
| --- |
| CNAME |
| SOA |
| *RRSIG* |
| SRV |





DNS-Rootserver ...

**Wählen Sie eine Antwort:**



**FRAGE 93 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 06**



Ein Programm fordert eine autoritative DNS-Antwort für den FQDN „login.research.mycompany.de“ an.

Von welchem der nachfolgend aufgeführten DNS-Server (sofern vorhanden) sollte diese Antwort stammen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *von dem DNS-Server, der die Zone „research.mycompany.de“ verwaltet.* |
| von dem DNS-Server, der die Rootzone „.“ verwaltet. |
| von dem DNS-Server, der die Top-Level-Domain „de“ verwaltet. |
| von dem DNS-Server, der die Zone „mycompany.de“ verwaltet. |



**FRAGE 94 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 06**

|  |
| --- |
| *... stellen autoritative Informationen zu allen für die Verwaltung von Top-Level-Domains verantwortlichen Nameservern bereit.* |
| ... unterstehen sämtlich der direkten Kontrolle der Internet Assigned Numbers Authority. |
| ... sind allesamt unter einer statischen IP-Adresse erreichbar, damit sie stets einfach zu finden sind. |
| ... stellen autoritative Informationen zu sämtlichen von regionalen Registrierungsstellen verwalteten Domains bereit. |





**FRAGE 95 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 06**



Die IP-Adresse für den FQDN „web.mycompany.com“ wird mithilfe der DNS-Sicherheitserweiterungen (DNSSEC) geschützt.

Wie lässt sich der entsprechende Eintrag überprüfen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Die „com“-Zone enthält einen öffentlichen Schlüssel für den genannten Eintrag. Zur Verifizierung dieses öffentlichen Schlüssels lässt sich dessen Signatur heranziehen, die ihrerseits in der Zone „mycompany.com“ gespeichert ist. |
| Die „com“-Zone enthält eine Signatur für den genannten Eintrag. Diese Signatur kann mithilfe des in derselben Zone gespeicherten öffentlichen Schlüssels verifiziert werden. |
| *Die Zone „mycompany.com“ enthält eine Signatur für den genannten Eintrag. Diese Signatur kann mithilfe des in derselben Zone gespeicherten öffentlichen Schlüssels verifiziert werden.* |
| Die Zone „mycompany.com“ enthält einen öffentlichen Schlüssel für diesen Eintrag. Dieser öffentliche Schlüssel kann mithilfe des in derselben Zone gespeicherten privaten Schlüssels verifiziert werden. |



**FRAGE 96 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 06**



Kompromittierte DNS-Server können von Angreifer:innen zur Steuerung von Botnetzen missbraucht werden. Weshalb sind diese Command-and-Control-Aktivitäten so schwer aufzudecken?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Dank der DNS-Sicherheitserweiterungen wird der gesamte DNS-Traffic in verschlüsselter Form übertragen, sodass die von den Angreifer:innen gesendeten Befehle nicht einmal durch modernste Paketanalyseverfahren erkannt werden. |
| Da autoritative DNS-Abfragen eine Seltenheit sind, ist es relativ einfach, DNS-Antworten zu spoofen. |
| Die DNS-Kommunikation per UDP erschwert die wechselseitige Identifizierung der Kommunikationspartner. |
| *DNS-Caching-Mechanismen ermöglichen die Übermittlung von Befehlen auch ohne direkte Verbindung zwischen dem kompromittierten DNS-Server und dem Opfersystem.* |





**FRAGE 97 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 07**



Welche der folgenden Aussagen benennt einen der Vorteile, die HTTP/2 gegenüber HTTP/1.1 auszeichnen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| HTTP/2 nutzt das UDP als Transportprotokoll, was die Latenzen der Antwortnachrichten spürbar verringert. |
| *In HTTP/2 können mehrere Anfragen synchron bearbeitet werden.* |
| HTTP/2 ist ein zustandsbehaftetes Protokoll, das die Übertragung redundanter Informationen überflüssig macht. |
| HTTP/2-Daten können von Browsern effizienter gecacht werden. |



**FRAGE 98 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 07**



Welche der folgenden Aussagen über das Simple Mail Transfer Protocol ist zutreffend?

**Wählen Sie eine Antwort:**

|  |
| --- |
| SMTP beinhaltet native Authentifizierungsmechanismen. |
| *SMTP ist zustandsbehaftetes Kommunikationsprotokoll.* |
| SMTP-Kommunikation setzt eine verschlüsselte Verbindung voraus. |
| In SMTP werden auftretende Fehler serverseitig behandelt. |





Ist HTTP/2 soweit kompatibel mit HTTP/1.1, dass ein ausschließlich für HTTP/2 konfigurierter Server HTTP/1.1-Anfragen bearbeiten kann?

**Wählen Sie eine Antwort:**



**FRAGE 99 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 07**

|  |
| --- |
| Ja, weil HTTP/2-Server über Downgrading -Mechanismen zur Anpassung von Verbindungen verfügen. |
| Ja, weil HTTP/2 dieselben Interaktionen wie HTTP/1.1 unterstützt. |
| *Nein, weil das Format der Header von HTTP/2 -Nachrichten von HTTP/1.1 abweicht.* |
| Nein, weil HTTP/2 verlangt, dass alle clientseitigen Anfragen vorab formuliert werden, damit der Server die Antworten parallel erstellen kann. |



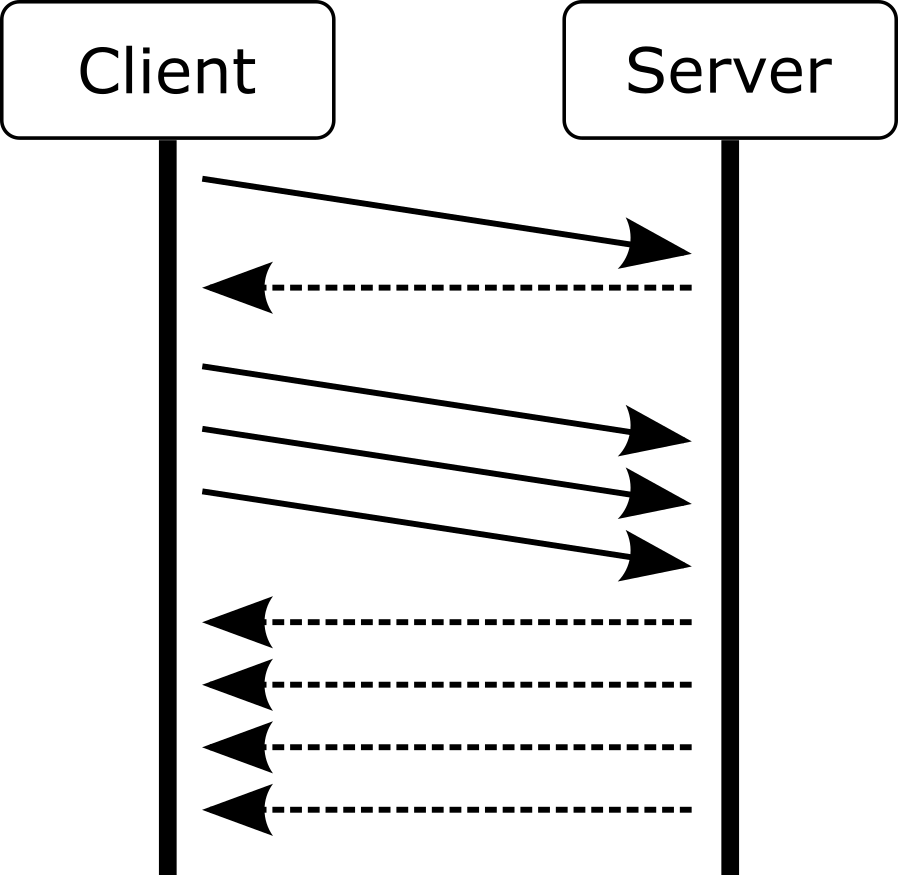


**FRAGE 100 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 07**



Sehen Sie sich den schematisch dargestellten Nachrichtenaustausch zwischen zwei Peers genauer an. Welches der folgenden Anwendungsprotokolle ist aller Wahrscheinlichkeit nach die Basis für diesen Dialog?



**Wählen Sie eine Antwort:**

|  |
| --- |
| *HTTP/2* |
| HTTP/1.1 |
| HTTP/1.0 |
| SMTP |





**FRAGE 101 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 07**



Warum ist HTTP/1.1 besser für die Interaktion mit modernen Webinhalten geeignet als HTTP/1.0?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *Moderne Webinhalte setzen sich aus vielen Elementen zusammen, für die in HTTP/1.0 jeweils eine eigene Verbindung eingerichtet werden müsste. Das erhöht den Ressourcenbedarf in beträchtlichem Maße.* |
| Moderne Webinhalte umfassen viele sensible Daten, die mit den in HTTP/1.1 enthaltenen Verschlüsselungsfunktionen geschützt werden müssen. |
| Moderne Webinhalte werden durch Skripte dynamisch erweitert. Hierfür ist HTTP/1.0 nicht ausgelegt. |
| Moderne Webinhalte umfassen hochauflösende Bilder. Diese können in HTTP/1.0 nur mit extremem Rechenaufwand verarbeitet werden. |



**FRAGE 102 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 07**



Load-Balancer sind spezielle Webserver, die empfangene Anfragen an nachgeschaltete Backend-Server übermitteln.

Bei Lastspitzen wird der eingehende Traffic auf mehrere Backend-Server verteilt. Welche grundlegende Eigenschaft welches Webprotokolls macht dies möglich?

**Wählen Sie eine Antwort:**



|  |
| --- |
| *Jede HTTP-Anfrage kann unabhängig von den vorherigen Anfragen bearbeitet werden, da HTTP ein zustandsloses Protokoll ist.* |
| Die von HTTP verwendeten Header stellen sicher, dass jeder Client immer nur mit demselben Backend-Server kommuniziert. |
| Eine eventuelle Verteilung des Traffics auf mehrere Backend-Server hat keine negativen Folgen, da HTTP/2 speziell für die simultane Verarbeitung mehrere Anfragen/Antworten konzipiert wurde. |
| Die Kontinuität des Dialogs wird dadurch sicherstellt, dass HTTP/1.1 die erneute Verwendung bestehender Verbindungen für Folgeanfragen erlaubt. |





**FRAGE 103 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 08**



Welches Protokoll wird von HTTP zur Sicherung der HTTP-Kommunikation genutzt?

**Wählen Sie eine Antwort:**

|  |
| --- |
| IPsec |
| *TLS* |
| DNSSEC |
| SSH |



**FRAGE 104 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 08**



Auf welcher Schicht des TCP/IP-Referenzmodells residiert der Secure-Shell-Protokollstack?

**Wählen Sie eine Antwort:**



|  |
| --- |
| SSH residiert auf der Transportschicht, da es direkt auf die Dienste der Internet- bzw. Netzwerkschicht zurückgreift. |
| SSH residiert auf der Verbindungsschicht, da es direkt auf die Dienste der Bitübertragungsschicht zurückgreift. |
| *SSH residiert auf der Anwendungsschicht, da es direkt auf die Dienste der Transportschicht zurückgreift.* |
| SSH residiert auf der Internet- bzw. Netzwerkschicht, da es direkt auf die Dienste der Verbindungsschicht zurückgreift. |



**FRAGE 105 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 08**



Root-Zertifikate bilden den Ankerpunkt einer Vertrauenskette. Wie werden sie signiert?

**Wählen Sie eine Antwort:**



|  |
| --- |
| Root-Zertifikate werden als Teil eines Betriebssystems ausgeliefert. Deshalb werden sie jeweils von der Zertifizierungsstelle signiert, die für das Betriebssystem zuständig ist. |
| *Root-Zertifkate sind selbstsignierte Zertifikate.* |
| Root-Zertifikate werden mit anderen Roott-Zertifikaten signiert. |
| Root-Zertifikate werden nicht signiert. |



**FRAGE 106 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 08**



Was ist eine Cipher-Suite?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Eine Cipher-Suite ist eine Softwarebibliothek, die kryptografische Algorithmen für verschiedene Zwecke enthält und die Vertraulichkeit der übertragenen Daten gewährleisten soll. |
| *Eine Cipher-Suite ist ein Set kryptografischer Algorithmen und Parameter, die während der Lebensdauer eines sicheren Kommunikationskanals für verschiedene Zwecke verwendet werden.* |
| Eine Cipher-Suite ist ein Spezifikationsdokument, das die für bestimmte Anwendungsprotokolle zulässigen kryptografischen Algorithmen und Parameter benennt. |
| Eine Cipher-Suite ist eine für ein bestimmtes Anwendungsprotokoll zertifizierte Software, die die Vertraulichkeit der übertragenen Daten sicherstellen soll. |



Welcher IPsec-Betriebsmodus unterstützt die Nutzung von NAT-Routern?

Warum?

**Wählen Sie eine Antwort:**



**FRAGE 107 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 08**



|  |
| --- |
| Im IPsec-Transportmodus werden nur die IIP-Nutzdaten geschützt, sodass der NAT-Router die Header der einzelnen Pakete wie gewohnt verarbeiten kann. |
| Im IPsec-Konversionsmodus werden nur die IP-Nutzdaten geschützt, sodass der NAT-Router die Header der einzelnen Pakete wie gewohnt verarbeiten kann. |
| *Im IPsec-Tunnelmodus werden die zu schützenden IP-Pakete in neuen Paketen gekapselt. Dadurch wird die Integrität der „inneren“, verschlüsselten Pakete bei der Netzwerkadressübersetzung nicht beeinträchtigt.* |
| Im IPsec-Routingmodus werden die zu schützenden IP-Pakete in neuen Paketen gekapselt. Dadurch wird die Integrität der „inneren“, verschlüsselten Pakete bei der Netzwerkadressübersetzung nicht beeinträchtigt. |





**FRAGE 108 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 08**

Ein Unternehmen verfügt über ein spezielles, intern entwickeltes System zur Verwaltung von Kundendaten. Dieses System soll im Zuge der Umstellung auf Telearbeit so angepasst werden, dass die Vertraulichkeit der dort bereitgestellten Daten auch bei externen Zugriffen bzw. bei der Übermittlung an externe Standorte gewahrt bleibt. Wie lässt sich dies realisieren?

**Wählen Sie eine Antwort:**



|  |
| --- |
| Das betreffende System kann durch die Anpassung der Firewallregeln für externe Nutzer:innen zugänglich gemacht werden. |
| Das betreffende System kann so konfiguriert werden, dass die Authentifizierung nur mit einem gültigen Zertifikat möglich ist. |
| Das betreffende System kann so konfiguriert werden, dass ein Datenaustausch mit externen Systemen nur über IPsec möglich ist. |
| *Das betreffende System kann so konfiguriert werden, dass ein Datenaustausch mit externen Systemen nur über Transport Layer Security möglich ist.* |





**FRAGE 109 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 09**



Die Erstellung von Regeln für verhaltensbasierte Intrusion-Detection-Systeme erfolgt ...

**Wählen Sie eine Antwort:**

|  |
| --- |
| ... manuell durch Cybersicherheitsexpert:innen mit einschlägiger Erfahrung. |
| ... automatisch durch das System, basierend auf beobachteten Angriffsmustern. |
| ... manuell durch das Team des IDS-Herstellers, auf Basis einer Wissensdatenbank. |
| *... automatisch durch das System, basierend auf Beobachtungsdaten aus dem Normalbetrieb.* |



**FRAGE 110 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 09**



Welche der folgenden verdächtigen Aktivitäten lässt sich durch die Überwachung des Datenflusses im Netzwerk aufdecken?

**Wählen Sie eine Antwort:**

|  |
| --- |
| wiederholte gescheiterte Authentifizierungsversuche |
| die Nutzung voreingestellter Benutzernamen und Passwörter |
| Änderungen an Logdateien kritischer Systeme |
| *die Nutzung gängiger Protokolle zur Kommunikation über nicht standardmäßige Ports* |





Bei welchem Schritt des „Information Security Incident Management“-Prozesses können Intrusion-Prevention-Systeme zum Einsatz kommen?

**Wählen Sie eine Antwort:**



**FRAGE 111 VON 120**

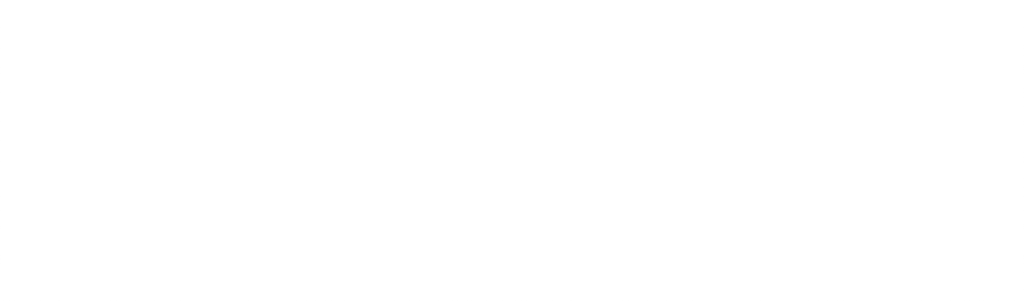
**DLBCSEINF01\_E\_MC\_mittel/Lektion 09**

|  |
| --- |
| Assess (Bewerten) |
| *Respond (Abwehren)* |
| Plan (Planen) |
| Detect (Erkennen) |



**FRAGE 112 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 09**



Ein signaturbasiertes Intrusion Prevention-System leitet automatisch Maßnahmen gegen einen festgestellten Denial-of-Service-Angriff ein.

Welcher Kategorie ist dieses Ereignis zuzuordnen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| *BLOCKED (blockiert)* |
| ALLOW (erlaubt) |
| SUSPICIOUS (verdächtig) |
| MALICIOUS (schädlich) |





**FRAGE 113 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 09**



Ein von einem Unternehmen dringend benötigtes Anwendungssystem wird noch im Auslieferungszustand auf seine Tauglichkeit getestet.

Das bedeutet unter anderem, dass die vom Hersteller standardmäßig eingerichteten Anmeldedaten zunächst ihre Gültigkeit behalten. Welche Art von Sicherheitssystem kann diesen potenziellen Angriffsvektor identifizieren?

**Wählen Sie eine Antwort:**

|  |
| --- |
| ein Intrusion-Detection-System |
| ein Intrusion-Detection-and-Prevention-System (IDPS) |
| ein Intrusion-Prevention-System |
| *ein SIEM-System* |



**FRAGE 114 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 09**



Ein Unternehmen lässt beim Management der Nutzeridentitäten nicht die nötige Sorgfalt walten. Daher kommt es immer wieder vor, dass die Anmeldedaten gelöschter Nutzerkonten auf einigen Systemen weiterhin gültig sind.

Welche Art von Sicherheitssystem kann solche Diskrepanzen erkennen?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Ein Intrusion-Detection-and-Prevention-System (IDPS) |
| *ein SIEM-System* |
| ein Intrusion-Detection-System |
| ein Intrusion-Prevention-System |





**FRAGE 115 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 10**



Welche Datendimension bzw. welche Art von Daten ist im Bereich Netzwerkforensik besonders wichtig und warum?

**Wählen Sie eine Antwort:**



|  |
| --- |
| Geodaten, weil der geografische Ursprung einer Cyberattacke Rückschlüsse auf die Absichten der Angreifer:innen erlaubt |
| Angaben zum Betriebssystem, weil einige Betriebssysteme besonders anfällig für Cyberangriffe sind |
| *Zeitdaten, weil die Erkennung und Dokumentation von Angriffsmustern eine genaue Rekonstruktion der Abfolge der Ereignisse erfordert* |
| Informationen zur Zugänglichkeit der betroffenen Software und Services, weil Testsysteme nicht als Angriffsvektoren missbraucht werden können |





**FRAGE 116 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 10**

Welche der folgenden Aussagen über Whois-Daten ist zutreffend?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Whois-Daten sind immer aktuell. |
| Whois-Daten enthalten geografische Informationen. |
| Whois-Daten sind ohne Einschränkungen öffentlich zugänglich. |
| *Whois-Daten erleichtern die Identifizierung verdächtiger Peers.* |





Welche Eigenschaft von Certiﬁcate Transparency (CT) ist der Grund dafür, dass CT-basierte Prozesse zur Identifizierung gefälschter Zertifikate relativ zuverlässig sind?

**Wählen Sie eine Antwort:**



**FRAGE 117 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 10**



Der Einsatz gefälschter digitaler Zertifikate ist eine gängige Methode für Man-in-the-Middle-Angriffe auf Systeme, die eine Public-Key-Infrastruktur zur Authentifizierung nutzen.

Hinter welcher der folgenden Bezeichnungen verbirgt sich ein zusätzlicher Verifizierungsstandard für Zertifikate?

**Wählen Sie eine Antwort:**

|  |
| --- |
| Certificate Revocation |
| Certificate Expiry |
| *Certiﬁcate Transparency* |
| Certificate Signing |

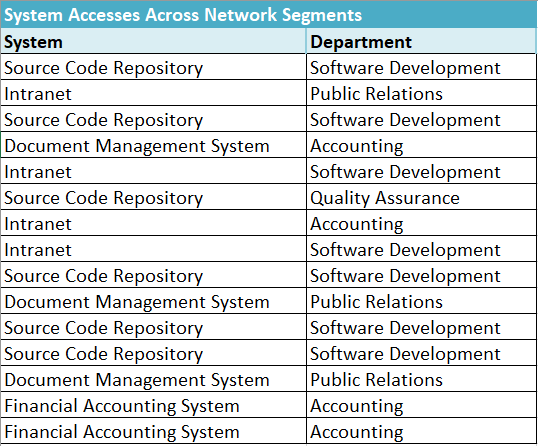


**FRAGE 118 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 10**

|  |
| --- |
| Öffentliche Zugänglichkeit |
| Redundanz |
| Rückverfolgbarkeit |
| *Unveränderlichkeit* |





Sehen Sie sich das abgebildete Datenset genauer an. Welcher Confidence-Wert ergibt sich daraus für die Assoziationsregel „Quellcode-Repository → Softwareentwicklung“?

**Wählen Sie eine Antwort:**

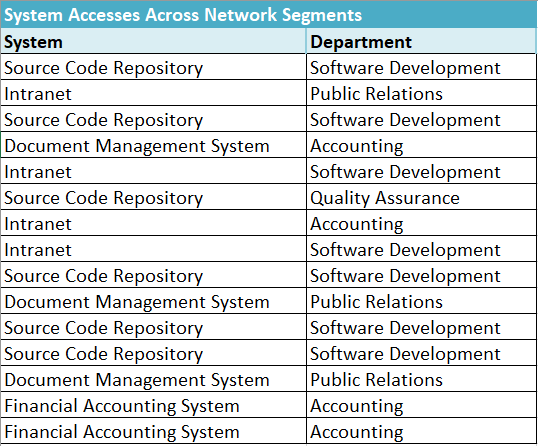


**FRAGE 119 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 10**

|  |
| --- |
| 4/7 |
| 5/7 |
| 6/7 |
| *5/6* |





Sehen Sie sich das abgebildete Datenset genauer an. Welcher Support-Wert ergibt sich daraus für die Assoziationsregel „Finanz- und Buchhaltungssystem → Buchführung“?

**Wählen Sie eine Antwort:**



**FRAGE 120 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 10**

|  |
| --- |
| 6 |
| *2* |
| 4 |
| 7 |