**Lektion 1**

**1.1**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Netzwerkforensik zielt auf die proaktive Verhinderung von Angriffen.
* Netzwerkforensik kommt erst dann zur Anwendung, wenn bereits Schäden entstanden sind.
* *Networkforensik hilft bei der Aufdeckung aktueller Sicherheitsbedrohungen.*

1. Nennen Sie zwei grundlegende Zielsetzungen der Netzwerkforensik.

*Netzwerkforensik unterstützt die Optimierung der IT-Sicherheit.*

*Netzwerkforensik liefert Beweismittel für Strafverfolgungsbehörden.*

*Netzwerkforensik versetzt Sicherheitsteams in die Lage, akute Angriffe und Sicherheitsvorfälle aufzudecken.*

*Netzwerkforensik versetzt Sicherheitsteams in die Lage, den durch einen Sicherheitsvorfall entstandenen Schaden zu begutachten.*

*Netzwerkforensik versetzt Sicherheitsteams in die Lage, die von einem Sicherheitsvorfall betroffenen Systeme zu identifizieren.*

1. Bitte vervollständigen Sie den folgenden Satz:

Damit die erfassten Daten vor Gericht verwendet werden können, müssen sie manipulationssicher aufbewahrt werden.

**1.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Rohdaten sind eine ausreichende Basis für die Untersuchung eines Vorfalls.
* *Der Prozessschritt „Incident Response“ kann direkte Gegenmaßnahmen einschließen.*
* Die zur Netzwerküberwachung eingesetzten Systeme müssen weder aktualisiert noch gewartet werden.

1. Bitte vervollständigen Sie den folgenden Satz:

Damit der Untersuchungsprozess reibungslos ablaufen kann, müssen die gesammelten Daten chronologisch *synchronisiert/geordnet* sein.

**1.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Verschiedenartige IDS sollten stets in Kombination eingesetzt werden.*
* IDS können Angreifergruppen identifizieren.
* IDS können unerwünschten Netzwerktraffic blockieren.

1. Beschreiben Sie zwei Arten von IDS und stellen Sie die Unterschiede zwischen ihnen dar.

*Hostbasierte IDS überwachen einzelne Systeme, netzwerkbasierte IDS überwachen komplette Netzwerksegmente.*

*Verhaltensbasierte IDS melden Abweichungen vom Normalprofil der Betriebsprozesse, signaturbasierte IDS identifizieren Vorfälle auf der Grundlage vordefinierter Regeln.*

1. Bitte vervollständigen Sie den folgenden Satz:

Damit ein Sicherheitsereignis als Sicherheitsvorfall klassifiziert werden kann, muss es *bestätigt* und *vor dem Hintergrund der geltenden Sicherheitsrichtlinien bewertet* werden.

**1.4**

1. Bitte vervollständigen Sie den folgenden Satz:

Denial-of-service-Angriffe verursachen *Ausfälle netzwerkbasierter Services*, indem sie eine extrem hohe Zahl von *Anfragen* senden.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Die Identifizierung der Urheber:innen eines (D)DoS-Angriffs ist trivial.
* *(D)DoS-Angriffe sollen möglicherweise von anderen Hackeraktivitäten ablenken.*
* *(D)DoS-Angriffe sind einfach zu erkennen, lassen sich aber nur mit Schwierigkeiten abwehren.*

**1.5**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Splunk wird für die Konsolidierung und Analyse von Daten eingesetzt.*
* Wireshark ist ein netzwerkbasiertes IDS.
* Die Analyse des Datenverkehrs im Netzwerk ist nur mit teuren kommerziellen Produkten möglich.

1. Nennen Sie zwei netzwerkbasierte Intrusion-Detection-Systeme.

*Zeek*

*Snort*

*Suricata*

**Lektion 2**

**2.1**

1. Bitte vervollständigen Sie den folgenden Satz:

Die oberen Schichten des TCP/IP-Modells sind unabhängig von *physischen* Infrastrukturen.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Das TCP/IP-Modell lässt sich nur in Netzwerkinfrastrukturen der neuesten Generation umsetzen.
* *Die Managementfunktionen der Darstellungs- und Sitzungsschicht aus dem ISO/OSI-Modell werden im TCP/IP-Modell auf der Anwendungsschicht bereitgestellt.*
* Die Verbindungsschicht ist für die Übertragung von Bits zwischen zwei Peers verantwortlich.

1. Beschreiben Sie eine Funktion der Transportschicht.

*die Zuordnung übermittelter Informationen zu Prozessen*

*die Abschirmung der Anwendungsschicht von technischen Detailfragen der unteren Ebenen*

**2.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Verbindungslose Protokolle stellen sicher, dass gesendete Daten von allen Peers empfangen wurden.
* *Verbindungsorientierte Protokolle korrigieren Übertragungsfehler und -pannen.*
* *Verbindungslose Protokolle unterstützen die simultane Übertragung von Daten an verschiedene Peers.*

1. Bitte vervollständigen Sie den folgenden Satz:

Die Kommunikation bzw. der Datenaustausch über verbindungsorientierte Protokolle weist die Struktur eines *Gesprächs* oder *Telefonanrufs* auf.

**2.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Die IETF ist ein nicht weiter untergliedertes Gremium, das Internetstandards veröffentlicht.
* *Vorgeschlagene Standards müssen einen langwierigen Prozess durchlaufen, bevor sie zu Internetstandards werden.*
* Vorgeschlagene Standards müssen verschiedene Implementierungsszenarien enthalten.

1. Bitte vervollständigen Sie den folgenden Satz:

Die *IANA/ICANN* ist die höchste Vergabestelle für Protokollnummern.

**Lektion 3**

**3.1**

1. Bitte vervollständigen Sie den folgenden Satz:

Das UDP ermöglicht eine *schnelle/effiziente/latenzarme* Datenübertragung. Allerdings geht dies zulasten der *Zuverlässigkeit/Wahrung der ursprünglichen Ordnung der Daten/garantierten Zustellung*.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Das UDP ist vom Internet Protocol unabhängig.
* Es gibt keine Möglichkeit, die Integrität UDP-basierter Datensendungen sicherzustellen.
* Die Integrität UDP-basierter Datensendungen muss durch den User, d. h. das auf der übergeordneten Schicht residierende Anwendungsprotokoll sichergestellt werden.

**3.2**

1. Bitte vervollständigen Sie den folgenden Satz:

Das TCP sorgt bei der Datenübertragung für *Zuverlässigkeit/die Wahrung der ursprünglichen Ordnung der Daten/die Fehlererkennung/die Datenflusskontrolle*. Allerdings geht dies mit Defiziten in puncto *Übertragungsgeschwindigkeit/Effizienz/Latenz* einher.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Das TCP ist vom Internet Protocol unabhängig.
* *Das TCP ermöglicht die Übertragung von Datenströmen unbestimmter Länge.*
* Die Integrität TCP-basierter Datensendungen muss durch das auf der übergeordneten Schicht residierende Anwendungsprotokoll sichergestellt werden.

**3.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Der Verlust eines TCP-Segments wird durch den Sender erkannt.*
* Der Verlust eines TCP-Segments wird durch den Empfänger erkannt.
* Bei einem fehlenden TCP-Segment bittet der Empfänger den Sender um dessen erneute Übertragung.

**3.4**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *SOCKS-Proxys ermöglichen die lokale Aufhebung von Firewallregeln.*
* *SOCKS-Proxys werden zwischen der Transportschicht und der Anwendungsschicht implementiert.*
* SOCKS-Proxys werden zwischen der Transportschicht und der Netzwerkschicht implementiert.

**3.5**

1. Bitte vervollständigen Sie den folgenden Satz:

Für Angriffe auf die Transportschicht (d. h. auf TCP- oder UDP-Kanäle) werden keine Schwachstellen in der *Anwendungs*software ausgenutzt.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Denial-of-Service-Angriffe richten sich immer direkt gegen das intendierte Opfersystem.
* *SYN-Flood-Angriffe zielen auf die Überlastung der Systemressourcen.*
* TCP-Verbindungen sind vor Lauschangriffen geschützt.

1. Beschreiben Sie das Vorgehen bei einem UDP-Reflection-Angriff.

*Die Angreifer:innen senden gefälschte Anfragen an einen UDP-basierten Service auf einem Zielsystem. Daraufhin schickt der UDP-basierte Service seine Antworten an das eigentliche Opfer der Attacke. Der Angriff ist erfolgreich, wenn das Volumen der Antworten die Netzwerkkapazitäten des Opfersystems übersteigt.*

**Lektion 4**

**4.1**

1. Bitte vervollständigen Sie den folgenden Satz:

Das Internet Protocol dient der Implementierung der *Netzwerk*schicht.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Routingmechanismen trennen Netzwerksegmente voneinander.
* Routingtabellen werden stets manuell von Netzwerkarchitekt:innen erstellt.
* *Routingprozesse basieren auf den Routingtabellen von Routern und anderen zwischengeschalteten Geräten.*

1. Nennen Sie einen Einsatzbereich des ICMP.

*Meldung nicht verfügbarer Ressourcen/Systeme*

*Messung der Rundtripzeiten übertragener Pakete*

*Verfolgung der Routen/Netzwerkpfade übertragener Pakete*

**4.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Bei der automatischen Wahl einer IP-Adresse ist der Internetzugriff bereits vor Abschluss des Konfigurationsprozesses möglich.
* *DHCP ist ein Protokoll, das auf Anfrage Konfigurationsdaten an neue Netzwerkhosts übermittelt.*
* Jedes Netzwerk kann immer nur einen DHCP-Server enthalten.

1. Bitte vervollständigen Sie den folgenden Satz:

DHCP ermöglicht die Kommunikation mit neuen Clients, da UDP-Datagramme auch ohne gültige *Quell*-Adresse ihr Ziel erreichen, wenn sie an die lokale *Broadcast*-Adresse gesendet werden.

**4.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Alle relevanten Informationen über eine IP-Adresse sind bei der IANA gespeichert.
* Anwendungsdienste können nur über die von der IANA festgelegten Ports kommunizieren.
* *Die IANA ist für die Zuweisung von IP-Adressbereichen an regionale Registrierungsstellen zuständig.*

**4.4**

1. Bitte vervollständigen Sie den folgenden Satz:

Netzwerkadressübersetzung ermöglicht Geräten aus *privaten* Netzwerken die Kommunikation mit dem Internet.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Firewalls trennen miteinander verbundene Netzwerksegmente auf der Netzwerkschicht.*
* *Firewalls trennen miteinander verbundene Netzwerksegmente auf der Transportschicht.*
* Firewalls trennen miteinander verbundene Netzwerksegmente auf der Verbindungsschicht.

**4.5**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* SOCKS ist ein Protokoll der Netzwerkschicht.
* Eine SOCKS-Verbindung wird durch den SOCKS-Client zur Übertragung von Daten an dritte Systeme genutzt.
* *SOCKS-Proxys ermöglichen die Umgehung von Firewalls.*

**Lektion 5**

**5.1**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* ARP-Antwortnachrichten enthalten Authentifizierungsdaten.
* *ARP-Antwortnachrichten ziehen Änderungen an der ARP-Tabelle des Empfängersystems nach sich.*
* ARP-Antwortnachrichten werden in festgelegten Intervallen versendet.

**5.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Der Austausch von RIP-Nachrichten erfolgt über TCP.
* RIP-Nachrichten sind verschlüsselt.
* *Der Austausch von RIP-Nachrichten erfolgt über Router.*

1. Nennen Sie drei Gründe, die einen Router zum Versand einer RIP-Nachricht veranlassen.

*Der Router erhält eine RIP-Anfrage.*

*Ein Timer ist abgelaufen.*

*Es wurde eine lokale Veränderung der Netzwerktopologie festgestellt.*

1. Bitte vervollständigen Sie den folgenden Satz:

Das RIP optimiert den Datenfluss im Netzwerk mithilfe eines *Distanzvektor*-Algorithmus.

**5.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Das Border Gateway Protocol nutzt UDP für die Übermittlung von Routinginformationen.
* *Das Border Gateway Protocol wird zur Implementierung von Routingrichtlinien verwendet.*
* Das Border Gateway Protocol wird zur Ermittlung der effizientesten Route zwischen autonomen Systemen eingesetzt.

**5.4**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *AS-Nummern werden für das Interdomainrouting mit BGP benötigt.*
* AS-Nummern werden für das Intradomainrouting mit BGP benötigt.
* AS-Nummern werden für das Interdomainrouting mit RIP benötigt.

**5.5**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Der wichtigste Gesichtspunkt bei der Entwicklung des RIP war der Schutz vor Cyberangriffen.
* BGP ist gegen Angriffe immun, weil es TCP als Transportprotokoll nutzt.
* *ARP-Poisoning ist eine von Angreifer:innen genutzte Methode zur Imitation eines Zielsystems.*

**Lektion 6**

**6.1**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Unterdomänen werden von der IANA zugewiesen.
* *Vollqualifizierte Domainnamen (FQDNs) fungieren als weltweit eindeutige Kennung von mit dem Internet verbundenen Systemen.*
* Es gibt genau einen DNS-Rootserver.

**6.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Das Domain Name System kann als verteilte Datenbank beschrieben werden.*
* Das Domain Name System umfasst ausschließlich IP-Adressen und deren Klarnamen.
* Das Domain Name System beantwortet Anfragen stets korrekt.

1. Nennen Sie zwei Arten von DNS-Einträgen, bei denen es sich nicht um zu einem Klarnamen gehörige IP-Adressen handelt.

*SRV*

*MX*

*CNAME*

*SOA*

*TXT*

*NS*

1. Bitte vervollständigen Sie den folgenden Satz:

Beim einem *autoritativen* DNS-Lookup werden die angefragten Informationen direkt von dem für die jeweilige Zone verantwortlichen DNS-Server abgerufen.

**6.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* DNSSEC wird zur Verschlüsselung des DNS-Traffics im Netzwerk genutzt.
* *DNSSEC ermöglicht die Authentifizierung von DNS-Antworten.*
* Ein wichtiger Aspekt bei der Entwicklung des Domain Name System war die Datenintegrität.

**6.4**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* SPF verhindert Phishing-Angriffe mit gestohlenen Identitäten.
* DMARC verhindert Phishing-Angriffe mit gestohlenen Identitäten.
* *DMARC bietet die Möglichkeit zur Definition öffentlich zugänglicher Richtlinien, aus denen die Empfänger illegitimer E-Mails ersehen können, wie sie in einem solchen Fall mit der mutmaßlichen Ursprungsdomain interagieren sollen.*

**Lektion 7**

**7.1**

1. Bitte vervollständigen Sie den folgenden Satz:

HTTP-Kommunikation basiert auf einem *Anfrage/Antwort-*Schema.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* HTTP ist nur für die Übertragung von Hypertext-Dokumenten geeignet.
* HTTP ist ein zustandsbehaftetes Kommunikationsprotokoll.
* *HTTP verfügt über Fehlermeldungsmechanismen.*

**7.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* HTTP/2 ist eine inkrementell verbesserte Version von HTTP/1.1.
* *HTTP/2 würde für höhere Übertragungsgeschwindigkeiten konzipiert.*
* Das Nachrichtenformat von HTTP/2 ist exakt mit dem Nachrichtenformat von HTTP/1.1 identisch.

**7.3**

1. Bitte vervollständigen Sie den folgenden Satz:

SMTP ist ein Protokoll für den Austausch von *E-Mails*.

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* SMTP wird genutzt, um E-Mails aus einem Remotepostfach abzurufen.
* *SMTP ist ein zustandsbehaftetes Kommunikationsprotokoll.*
* SMTP-Anwendungen kommunizieren über UDP.

**Lektion 8**

**8.1**

1. Nennen Sie drei Dienste bzw. Funktionen, die mithilfe des SSH-Protokolls bereitgestellt werden können.

*Remote-Terminals / interaktive Befehlszeilenschnittstellen*

*Dateiübertragung*

*Portweiterleitung*

*X11-Weiterleitung*

*Ausführung von Remotebefehlen*

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Beim Diffie-Hellman-Schlüsselaustausch werden private Schlüssel über das Netzwerk übertragen.
* *Beim Diffie-Hellman-Schlüsselaustausch wird der öffentliche Schlüssel des Remotepeers und der private Schlüssel des lokalen Peers zur Berechnung des geheimen gemeinsamen Schlüssels genutzt.*
* Beim Diffie-Hellman-Schlüsselaustausch nutzt jeder Peer einen eigenen Schlüssel für den sicheren Kommunikationskanal.

1. Bitte vervollständigen Sie den folgenden Satz:

Bei asymmetrischen Verschlüsselungsverfahren werden die übertragenen Daten mit *öffentlichen* Schlüsseln verschlüsselt und mit *privaten* Schlüsseln entschlüsselt.

**8.2**

1. Nennen Sie zwei Unterprotokolle aus dem IPSec-Protokollstack:

*Internet Key Exchange / IKEv2*

*Encapsulating Security Payload / ESP*

*Authentication Header / AH*

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* IPsec verschlüsselt stets die Quell- und Zieladresse der übertragenen Pakete.
* IPsec-Peers kommunizieren über UDP.
* *IPsec wird zur sicheren Verbindung von Netzwerksegmenten genutzt.*

1. Bitte vervollständigen Sie den folgenden Satz:

Bei den Peers von Sicherheitsgateways kann es sich um *andere Sicherheitsgateways* oder *einzelne Hosts* handeln.

**8.3**

1. Nennen Sie zwei Sicherheitsfeatures des TLS-Protokollstacks.

*Vertraulichkeit*

*Authentifizierung*

*Integrität*

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *TLS wird immer in Kombination mit anderen Protokollen eingesetzt.*
* In TLS werden stets alle Peers authentifiziert.
* Anwendungsprotokolle können mit TLS geschützt werden, ohne dass dies in ihrem Quellcode berücksichtigt werden muss.

1. Bitte vervollständigen Sie den folgenden Satz:

TLS ist im TCP/IP-Referenzmodell auf der *Transportschicht* zu verorten.

**8.4**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Man-in-the-Middle-Angriffe setzen eine erfolgreiche Attacke auf eine der unteren Schichten voraus.*
* Man-in-the-Middle-Angriffe lassen sich mithilfe von Verschlüsselungsmethoden komplett unterbinden.
* Man-in-the-Middle-Angriffe sind keine Gefahr, wenn Public-Key-Infrastrukturen zur Authentifizierung genutzt werden.

1. Bitte vervollständigen Sie den folgenden Satz:

Um Man-in-the-Middle-Angriffe zu vereiteln, überprüft SSH den *digitalen Fingerabdruck* des Serverschlüssels.

**8.5**

1. Nennen Sie drei Pflichtfelder in Zertifikaten.

*Name des Inhabers*

*Öffentlicher Schlüssel des Inhabers*

*Name des Ausstellers*

*Gültigkeitszeitraum*

*signatureAlgorithm*

*signatureValue*

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Zertifikate sind unbegrenzt gültig.
* Zertifikate enthalten private Schlüssel.
* *Zertifikate dienen der Authentifizierung ihrer Inhaber.*

1. Bitte vervollständigen Sie den folgenden Satz:

Root-Zertifkate sind *selbstsignierte* Zertifikate, die als *Vertrauensanker* fungieren.

**Lektion 9**

**9.1**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Signaturbasierte IDS- und IPS-Lösungen sind ineffizient.
* *Verhaltensbasierte IDS- und IPS-Lösungen sind anfällig für Fehlalarme.*
* Netzwerkbasierte Intrusion-Detection-Systeme verhindern Angriffe über das Netzwerk.

**9.2**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Bei der Überwachung des Netzwerktraffics stehen historische Daten im Vordergrund.
* *Bei der Überwachung des Netzwerktraffics werden Informationen über gängige Protokolle zur Aufdeckung verdächtiger Aktivitäten genutzt.*
* Die Überwachung des Netzwerktraffics liefert keine Hinweise auf die Nutzung unbekannter Protokolle.

**9.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Verhaltensbasierte IDS- und IPS-Lösungen sind anfällig für Fehlalarme.*
* Signaturbasierte IDS- und IPS-Lösungen sind anfällig für Fehlalarme.
* Falsch-negativ-Fehler sind einfach zu identifizieren.

**9.4**

1. Nennen Sie zwei Arten von Daten, die in eine SIEM-Lösung eingespeist werden können.

*Systemprotokolle/Logdateien*

*Daten zum Patchstatus*

*Performancedaten*

**9.5**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Intrusion-Detection-Systeme sind in der Vorbereitungsphase des zyklischen Incident-Response-Modells hilfreich.
* *SIEM-Lösungen sind in der Vorbereitungsphase des zyklischen Incident-Response-Modells hilfreich.*
* Intrusion-Prevention-Systeme sind in der Bewertungs- und Analysephase des zyklischen Incident-Response-Modells von Nutzen.

**Lektion 10**

**10.1**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Bei der Rekonstruktion von Angriffsverläufen kommt es entscheidend auf die geografische Aggregation der verfügbaren Daten an.
* Bei der Rekonstruktion von Angriffsverläufen kommt es entscheidend auf die korrekte Einstufung der betroffenen Daten nach Datenschutzgesichtspunkten an.
* *Bei der Rekonstruktion von Angriffsverläufen kommt es entscheidend auf akkurate Zeitstempel an.*

**10.2**

1. Nennen Sie zwei DND-basierte Datenquellen.

*DNS-Sperrlisten/DNSBLs*

*passive DNS-Daten*

*DNS-Repositories*

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Passive DNS-Daten enthalten sämtliche DNS-Einträge einer Domain.
* Für DNS-Sperrlisten gelten verbindliche Aufnahmekriterien.
* *DNS-Einträge können sich im Laufe der Zeit in rascher Folge ändern.*

**10.3**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Regionale Internet-Registrierungsstellen sind für die Bereitstellung von GeoIP-Daten zuständig.
* *Regionale Internet-Registrierungsstellen sind für die Bereitstellung von Daten zu autonomen Systemen zuständig.*
* Regionale Internet-Registrierungsstellen und die IANA sind von länderspezifischen und internationalen Datenschutzregelungen ausgenommen.

**10.4**

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* Zertifikate können nicht widerrufen werden.
* Einträge in CT-Logs können nachträglich verändert werden.
* *Certificate Transparency stellt eine alternative Infrastruktur für die Prüfung von Zertifikaten bereit.*

**10.5**

1. Nennen Sie drei Klassifizierungsalgorithmen.

*Naiver Bayes-Klassifikator*

*Bayessche Netze*

*Markov-Ketten*

*Entscheidungsbaumalgorithmen*

*Stützvektormaschinen*

*künstliche neuronale Netze*

1. Bitte markieren Sie die korrekte(n) Aussage(n) mit einem Haken.

* *Clusteranalysen basieren auf unüberwachten Lernmethoden.*
* Datenklassifizierungsverfahren basieren auf unüberwachten Lernmethoden.
* *Assoziationsregeln lassen sich anhand von Kenngrößen hinsichtlich ihrer Zuverlässigkeit unterscheiden.*