
# Modul Prüfungsvorbereitung Sicherheit

Nachfolgend finden Sie eine Themen- und Fragensammlung aus der Abschlussprüfung (2, Teil 1) rund um das Thema Sicherheit. Diese sollen Ihnen eigene Wissenslücken aufzeigen und Sie ggf. ermuntern, die jeweiligen Links zur Wissensaneignung zu nutzen.

Die anschließenden Fragen sollten vollständig von Ihnen verstanden worden sein, so dass Sie auch andere das Themengebiet betreffende Fragen, so zum Beispiel auch in offener Form, beantworten können.

* Erforderlich

* Dieses Formular wird Ihren Namen aufzeichnen. Bitte tragen Sie Ihren Namen ein.

## Teil 1:  Single-Sign On (SSO)

Authentifizierung und Autorisierung sind zwei eng verwandte, aber dennoch unterschiedliche Konzepte der Zugriffskontrolle.

**Authentifizierung** bezieht sich auf den Prozess der Überprüfung der Identität eines Benutzers, normalerweise durch die Eingabe von Anmeldeinformationen wie einem Benutzernamen und einem Passwort oder durch die Verwendung von biometrischen Daten wie Fingerabdrücken oder Gesichtserkennung. Authentifizierung ist der erste Schritt bei der Gewährung von Zugriff auf ein System oder eine Anwendung.

**Autorisierung** bezieht sich auf den Prozess der Überprüfung, ob ein authentifizierter Benutzer berechtigt ist, auf bestimmte Ressourcen innerhalb eines Systems oder einer Anwendung zuzugreifen. Die Autorisierung basiert auf den Rollen und Berechtigungen, die einem Benutzer zugewiesen wurden, und sie entscheidet, ob der Benutzer auf eine bestimmte Ressource zugreifen darf oder nicht.

Zusammenfassend kann man sagen, dass die Authentifizierung die Identität des Be-

1

Single-Sign ON (SSO) ist ein Verfahren zur:

- ◯ Autoinkrementierung
- ◯ Autolodierung
- ◯ Autorisierung (ausschließlich)
- ◯ Authentifizierung (ggf. auch Autorisierung)
- ◯ Autoritätierung

2

Was ist kein Vorteil von Single-Sign-On (SSO)?

- ◯ SSO vereinfacht den Anmeldevorgang für Benutzer, da sie sich nur einmal anmelden müssen, um auf mehrere Anwendungen oder Websites zuzugreifen.
- ◯ SSO reduziert die Notwendigkeit für Benutzer, sich an mehrere Passwörter und Anmeldeinformationen zu erinnern. Dies reduziert das Risiko, dass Benutzer Passwörter wiederverwenden oder schwache Passwörter verwenden, was zu einem höheren Sicherheitsrisiko führen kann.
- ◯ SSO erleichtert die Verwaltung von Anmeldeinformationen für IT-Administratoren, da sie nur einen einzigen Satz von Anmeldeinformationen pro Benutzer verwalten müssen.
- ◯ Die verwendeten Kennwörter verfügen durch SSO über eine höhere Passwortstärke.
- ◯ Kosteneinsparungen: Da SSO den Anmeldevorgang vereinfacht und die Verwaltung von Anmeldeinformationen erleichtert, kann es zu Kosteneinsparungen führen. Weniger Anmeldevorgänge und eine einfachere Verwaltung von Anmeldeinformationen können auch die Produktivität der Benutzer erhöhen.

3

Was ist kein Nachteil von Single-Sign-On (SSO)?

- ◯ Mit einem Zugang erhalten Angreifer Zugriff auf verschiedenste Systeme.
- ◯ Abhängigkeit von der Verfügbarkeit des Identity Providers (bspw. bei Systemausfall)
- ◯ Der Nutzer muss sich mehrere Passwörter überlegen
- ◯ Die Implementierung von SSO kann sehr komplex sein.
- ◯ Die Implementierung von SSO kann zusätzliche Kosten verursachen.

## Teil 2: OAuth

OAuth2 ist ein Protokoll zur Autorisierung von Anwendungen oder Diensten, das es Benutzern ermöglicht, einem Drittanbieter-Dienst den Zugriff auf ihre geschützten Ressourcen bei einem anderen Dienst zu gewähren, ohne ihre Anmeldeinformationen preisgeben zu müssen.

*Ein Beispiel für die Verwendung von OAuth2 ist, wenn ein Benutzer sich bei einer Anwendung mit seinem Google-Konto anmeldet, um auf dessen Kalender zugreifen zu können. In diesem Fall fungiert Google als Identitätsanbieter und die Kalender-App, die der Nutzer zusätzlich nun nutzen will, als Ressourcenanbieter. Sobald der Benutzer seine Identität bei Google bestätigt hat, gibt Google der Kalender-App ein Zugriffstoken zurück, das der App erlaubt, auf den Kalender des Benutzers zuzugreifen, ohne dass der Benutzer seine Anmeldeinformationen für Google an die Kalender-App weitergeben muss.*

***Weitere Informationen:*** *Sollten Ihnen der Begriff OAuth im Wesentlichen noch unbekannt sein, empfehlen wir Ihnen eine der folgendes Erklärungen in Ruhe anzuschauen bzw. zu lesen.*

4

Beschreiben Sie in Ihren Worten, um was es sich bei den Konzept von OAuth handelt. *

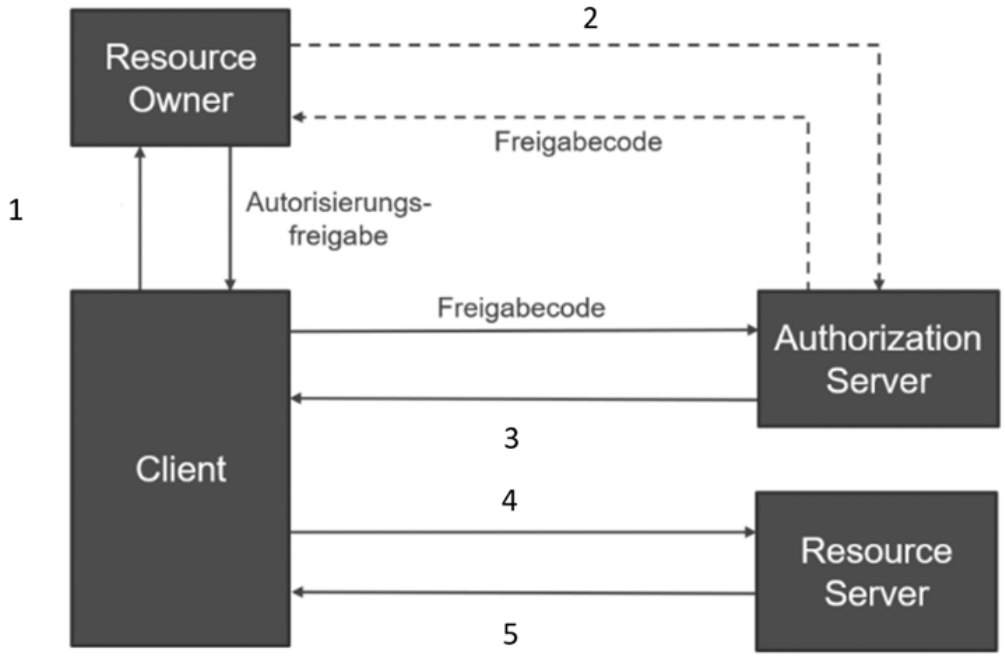
5

Bringen Sie die folgenden Schritte des OAuth2-Ablaufes in die richtige Reihenfolge:

- ◯ Der Benutzer gibt seine Anmeldeinformationen bei einem Dienst(Autorisierungsserver), ein, z.B. bei einem sozialen Netzwerk, um auf seine geschützten Ressourcen zuzugreifen.
- ◯ Der Benutzer autorisiert eine andere Anwendung oder Dienst, auf seine geschützten Ressourcen beim Dienst zuzugreifen.
- ◯ Der Drittanbieter-Dienst erhält ein Autorisierungstoken vom Dienst(Autorisierungsserver), das ihm den Zugriff auf die geschützten Ressourcen des Benutzers ermöglicht.
- ◯ Der Drittanbieter-Dienst verwendet das Autorisierungstoken, um auf die geschützten Ressourcen des Benutzers beim Dienst zuzugreifen.

6

Bringen Sie die nachfolgenden Fachbegriffe des OAuth2 Verfahrens (detaillierte Ablaufdarstellung) in der Nummerierung im Bild entsprechende richtige Reihenfolge:




Access-Token

Access-Token

Geschützte Ressource

Autorisierungsanfrage

Freigabecode

Authentifizierung, Autorisierung

## Teil 3: Verschlüsselung

Im folgenden werden Fragen rund um das Thema Verschlüsselung gestellt. **Bitte beantworten Sie diese Fragen erst, nachdem Sie sich über die wesentlichen Elemente des Themas informiert haben.**

Folgende Themen werden behandelt:

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- TLS
- HTTP vs. HTTPS

Für eine Einführung in das Thema kann folgendes Erklärvideo von Youtube zum Beispiel genutzt werden: https://youtu.be/NPHlmQnZhv4

7

Beschreiben Sie in Ihren Worten, um welche Art von Verschlüsselung es sich bei der Symmetrischen Verschlüsselung handelt.

**Hinweis:** Sollten Ihnen der Begriff Symmetrische Verschlüsselung gerade kryptisch vorkommen, empfehlen wir Ihnen, den Begriff in einer der folgenden Quellen kurz nachzulesen.

https://www.elektronik-kompendium.de/sites/net/1910101.htm *

8

Bringen Sie die Schritte der Symmetrischen Verschlüsselung in die richtige Reihenfolge

Der Empfänger verwendet denselben Schlüssel, um den Geheimtext zu entschlüsseln und den ursprünglichen Klartext wiederherzustellen.

Der Klartext wird mit dem Schlüssel verschlüsselt, um den Geheimtext zu erzeugen.

Der Geheimtext wird übertragen, normalerweise über ein unsicheres Netzwerk.

Der Verschlüsselungsschlüssel wird zufällig generiert.

9

Was ist der Hauptvorteil der symmetrischen Verschlüsselung gegenüber der asymmetrischen Verschlüsselung?

- ◯ Höhere Sicherheit
- ◯ Einfachere Schlüsselverwaltung
- ◯ Bessere Skalierbarkeit
- ◯ Höhere Geschwindigkeit

10

Was passiert, wenn der symmetrische Verschlüsselungsschlüssel in falsche Hände gerät?

- ◯ Der Angreifer kann die verschlüsselten Daten nicht entschlüsseln.
- ◯ Der Angreifer kann den Schlüssel nicht verwenden, ohne den verschlüsselten Datenverkehr zu unterbrechen.
- ◯ Der Angreifer kann den Schlüssel nur verwenden, um verschlüsselte Daten zu verschlüsseln, aber nicht um sie zu entschlüsseln.
- ◯ Der Angreifer kann die verschlüsselten Daten entschlüsseln.

11

Beschreiben Sie in Ihren Worten, um welche Art von Verschlüsselung es sich bei der Asymmetrischen Verschlüsselung handelt.

**Hinweis:** Sollten Ihnen der Begriff Asymmetrische Verschlüsselung gerade kryptisch vorkommen, empfehlen wir Ihnen, den Begriff in einer der folgenden Quellen kurz nachzulesen.

https://www.elektronik-kompendium.de/sites/net/1910101.htm *

12

Was ist der Sinn von SSL-Zertifikaten?

- ◯ Sie schützen eine Webseite vor Hackerangriffen.
- ◯ Sie verschlüsseln den Datenverkehr zwischen einem Client und einem Server.
- ◯ Sie verifizieren die Identität eines Web-Servers. Dies entspricht einer Autorisierungsprüfung
- ◯ Sie ermöglichen den Zugriff auf gesperrte Webseiten.
- ◯ Sie verifizieren die Identität eines Web-Servers. Dies entspricht einer Authentizitätsprüfung

13

Welches Protokoll wird in der Regel verwendet, um eine sichere Verbindung zwischen Webbrowsern und Webservern herzustellen?

- ◯ HTTP
- ◯ HTTPS
- ◯ SMTP
- ◯ FTP

14

Welchen Port nutzt HTTPS?

- ◯ 80
- ◯ 21
- ◯ 3306
- ◯ 443
- ◯ 33060

15

## Hybride Verschlüsselung:

Symmetrische Verschlüsselung und asymmetrische Verschlüsselung sind zwei grundlegende Arten der Verschlüsselung, während die hybride Verschlüsselung eine Kombination aus beiden ist.

**Symmetrische Verschlüsselung** verwendet denselben Schlüssel zum Verschlüsseln und Entschlüsseln von Daten. Der Schlüssel muss sicher zwischen Sender und Empfänger ausgetauscht werden, da sonst Dritte, die den Schlüssel abfangen, die verschlüsselten Daten entschlüsseln können.

**Asymmetrische Verschlüsselung** verwendet ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel kann zur Verschlüsselung von Daten verwendet werden, während der private Schlüssel zum Entschlüsseln von Daten verwendet wird. Der private Schlüssel muss geheim gehalten werden, während der öffentliche Schlüssel frei verfügbar ist.

**Hybride Verschlüsselung** kombiniert die Vorteile von symmetrischer und asymmetrischer Verschlüsselung, indem sie ein symmetrisches Schlüsselpaar verwendet, um Daten zu verschlüsseln, und anschließend den symmetrischen Schlüssel mit asymmetrischer Verschlüsselung verschlüsselt, um eine sicherere Schlüsselverteilung zu ermöglichen.

Und nun die Frage: Was ist der Zweck der hybriden Verschlüsselung?

- ◯ Sie verbessert die Geschwindigkeit der Verschlüsselung.
- ◯ Sie ermöglicht eine einfachere Schlüsselverteilung.
- ◯ Sie kombiniert die Vorteile symmetrischer und asymmetrischer Verschlüsselung

16

Welche Art von Verschlüsselung nutzt TLS (Transport Layer Security)?

- ◯ Asymmetrische Verschlüsselung
- ◯ Symmetrische Verschlüsselung
- ◯ Hybride Verschlüsselung

17

TLS (Transport Layer Security) ist ein Verschlüsselungsprotokoll, das zur Sicherung der Datenübertragung im Internet eingesetzt wird. Die Schritte einer typischen TLS-Verbindung können wie folgt beschrieben werden:

Die Authentifizierung: Bevor der Client Daten überträgt, überprüft dieser die Authentizität des Servers. Dies geschieht in der Regel durch die Verwendung von digitalen Zertifikaten, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurden. Der Server muss sich gegenüber dem Client authentifizieren, um sicherzustellen, dass der Client tatsächlich mit dem richtigen Server kommuniziert.

Die Beendigung der Verbindung: Wenn die Datenübertragung abgeschlossen ist, wird die TLS-Verbindung beendet. In diesem Schritt wird der symmetrische Schlüssel gelöscht, um sicherzustellen, dass keine weiteren Daten über diesen Schlüssel übertragen werden können.

Die TLS-Handshake-Phase: Zunächst wird eine TLS-Verbindung zwischen Client und Server aufgebaut. In diesem Schritt vereinbaren die beiden Parteien die Verschlüsselungsalgorithmen und die Art der Authentifizierung, die im weiteren Verlauf der Verbindung verwendet werden sollen.

Die Verschlüsselung der Datenübertragung: Ab diesem Zeitpunkt sind alle Daten, die zwischen Client und Server ausgetauscht werden, verschlüsselt. Der symmetrische Schlüssel wird nun verwendet, um die Daten mit einem Verschlüsselungsalgorithmus zu verschlüsseln.

Der Schlüsselaustausch: Der Server schickt seinen öffentlichen Schlüssel an den Client, damit dieser den Datenverkehr verschlüsseln kann. Der Client erzeugt dann einen zufälligen symmetrischen Schlüssel, der zur Verschlüsselung der Daten verwendet wird. Dieser Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel des Servers verschlüsselt und zurückgeschickt.

## Teil 4: Angriffsvektoren

Im folgenden werden Fragen rund um das Thema Angriffsvektoren gestellt. **Bitte beantworten Sie diese Fragen erst, nachdem Sie sich über die wesentlichen Elemente des Themas informiert haben.**

Folgende Themen werden behandelt:

- SQL-Injection
- Man in the middle
- Social Engineering
- Brute-Force-Angriff
- Randsomware-Angriff

18

Welche der folgenden Aussagen beschreibt am besten SQL Injection?

- ◯ Eine Methode, um eine Datenbank mit gefälschten Daten zu füllen
- ◯ Eine Methode, um eine Datenbank aus einem Backup wiederherzustellen
- ◯ Eine Methode, um eine SQL-Abfrage so zu manipulieren, dass sie unerwartete Ergebnisse liefert
- ◯ Eine Methode, um eine Datenbank zu verschlüsseln, um sie vor Angriffen zu schützen

19

Welcher der folgenden SQL-Injection-Codes kann dazu verwendet werden, um eine Authentifizierung zu umgehen und sich als Administrator anzumelden?

- ◯ SELECT * FROM users WHERE username = 'admin' AND password = 'password123';
- ◯ SELECT * FROM users WHERE username = 'admin' OR 1=1;
- ◯ UPDATE users SET is_admin = true WHERE username = 'hacker';
- ◯ INSERT INTO users (username, password) VALUES ('admin', 'password123');

20

Welcher der folgenden Angriffsvektoren ist am wahrscheinlichsten, um eine symmetrische Verschlüsselung zu kompromittieren?

- Brute-Force-Angriffe
- Phishing-Angriffe
- Ransomware-Angriffe
- Social Engineering

21

Welcher der folgenden Angriffsvektoren ist am wahrscheinlichsten, um eine asymmetrische Verschlüsselung zu kompromittieren?

- Brute-Force-Angriffe auf den öffentlichen Schlüssel
- Man-in-the-Middle-Angriffe
- Social Engineering
- Phishing-Angriffe

22

Welche der nachfolgenden Beispiele fällt nicht in die Kategorie des Social Engineering?

- Ein Angreifer gibt sich als IT-Techniker aus und ruft ein Unternehmen an, um den Zugriff auf das Netzwerk zu beantragen. Wenn ihm das gelingt, kann er sich Zugriff auf vertrauliche Informationen verschaffen oder sogar Malware auf dem System installieren.
- Ein Angreifer gab sich als CEO aus und rief einen Mitarbeiter an, um ihn dazu zu bringen, eine große Menge Geld zu überweisen. Der Mitarbeiter glaubte, dass der Anruf tatsächlich von seinem Chef kam und überwies das Geld. Der Angreifer hatte die Stimme des CEOs zuvor aufgenommen und konnte so glaubhaft auftreten.
- Ein Angreifer sendet eine E-Mail, die angeblich von einem Bekannten oder Kollegen stammt und bittet um die Weitergabe von vertraulichen Informationen. Wenn der Empfänger darauf hereinfällt, kann der Angreifer Zugang zu sensiblen Informationen erhalten.
- Ein Angreifer lässt absichtlich einen USB-Stick mit Malware darauf an einem öffentlichen Ort liegen, z.B. in der Cafeteria eines Unternehmens. Wenn ein Mitarbeiter den Stick findet und ihn in seinen Computer steckt, wird das System infiziert und der Angreifer erhält Zugriff auf das Netzwerk.
- Ein Computerprogramm versucht durch einen Brute-Force Angriff die Zugangscodes zu einen Content-Management-System (CMS) zu erlangen.

23

Welcher der nachfolgenden Social Engineeringfälle ist frei erfunden?

- ◯ Im Jahr 2014 wurde ein Mitarbeiter der US-Regierung von einem russischen Hacker per E-Mail kontaktiert und überredet, Malware auf seinen Computer herunterzuladen. Diese Malware gab dem Angreifer Zugriff auf vertrauliche Regierungsinformationen.
- ◯ Im Jahr 2017 fielen mehrere Mitarbeiter des Fernsehsenders HBO einem Social Engineering-Angriff zum Opfer, bei dem Hacker E-Mails fälschten und sich als Führungskräfte des Unternehmens ausgaben. Die Angreifer erbeuteten geheime Drehbücher und Episoden von "Game of Thrones".
- ◯ Im Jahr 2018 fielen Millionen von Facebook-Nutzern einem Social Engineering-Angriff zum Opfer, als eine App namens "thisisyourdigitallife" Daten von Nutzern und deren Freunden sammelte und an Cambridge Analytica weitergab. Dieser Angriff nutzte Facebook als Plattform, um Nutzerdaten zu sammeln, ohne dass die Betroffenen davon wussten.
- ◯ Im Jahr 2020 wurde eine Gruppe von Cyberkriminellen namens "SilentFade" entdeckt, die Facebook-Profile hackte und dann Anzeigen auf den gehackten Konten schaltete, um gefälschte Produkte zu bewerben und Kreditkartendaten zu sammeln. Sie nutzten eine Kombination aus Social Engineering-Methoden und Schwachstellen in Facebooks Werbesystem, um ihre Angriffe durchzuführen.
- ◯ Im Jahr 2022 überredet ein Auszubildender seinen IT Lehrer zur Herausgabe der streng geheimen IHK Prüfung, indem er sich als Alien ausgab, der mit Hilfe der IHK-Musterlösung einen intergalaktischen Krieg verhindern wollte.

---