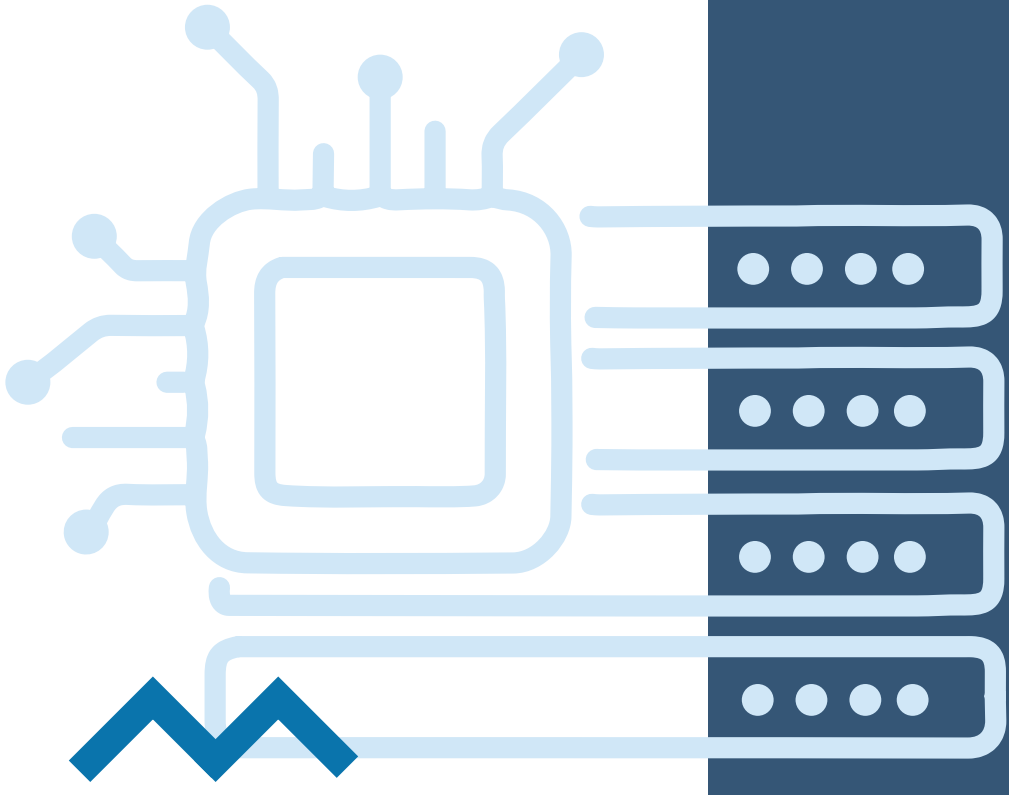
75 Jahre
IHK-Partner

Raik Pöhl

Fachinformatiker/ Fachinformatikerin Systemintegration

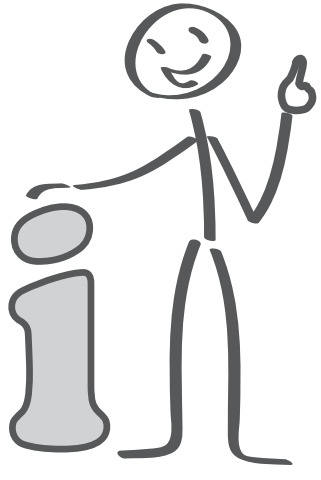
Abschlussprüfung Teil 2



u-form

Best.-Nr. 75722

2. Auflage 2023



Achtung!

Sollte es für diese Lernkarten Korrekturen oder Änderungen geben, kannst du diese herunterladen unter

www.u-form.de/addons/75722-2024.pdf

Ist dieser Link nicht verfügbar, so haben wir noch keine Änderungen, Korrekturen oder Zusatzinfos hinterlegt.

Hinweis: Auf Lernkarten ist der Platz begrenzt und die hier beschriebenen Themen sind komplex. Auch wenn mehrheitlich von Kunden, Nutzern oder Administratoren die Rede ist, sind stets alle möglichen Geschlechter gemeint.

Frage

Nennen Sie Vorteile und Nachteile der Nutzung von Single Sign-On (SSO).

Single Sign-On (SSO) ist ein Authentifizierungsdienst, der es erlaubt, mit einem Satz von Anmeldeinformationen auf mehrere Anwendungen zuzugreifen.

Vorteile:
- einmalige Anmeldung, um auf mehrere Anwendungen zuzugreifen
- reduziert das Risiko vergessener Passwörter
- es besteht die Möglichkeit, schnell und zentralisiert auf Sicherheitsvorfälle zu reagieren

Nachteile:
- ein Ausfall oder eine Kompromittierung des SSO-Dienstes kann den Zugriff auf alle Anwendungen beeinträchtigen
- technisch komplex zu implementieren und zu verwalten
- Anbieterabhängigkeit: Risiken im Zusammenhang mit der Verwendung eines externen SSO-Dienstleisters

Frage

Es gibt verschiedene Tools und Technologien, die bei der Updateverwaltung eingesetzt werden können.

Erklären Sie kurz WSUS, SCCM und APT.

WSUS (Windows Server Update Services) ist ein Microsoft-Tool, das zur Verwaltung von Updates für Windows-Betriebssysteme und andere Microsoft-Produkte verwendet wird.

SCCM (System Center Configuration Manager) ist eine umfassendere Lösung von Microsoft für das IT-Management. Es bietet Funktionen zur Bereitstellung, Überwachung und Verwaltung von Softwareupdates für eine Vielzahl von Betriebssystemen und Anwendungen.

APT (Advanced Packaging Tool) ist ein Paketverwaltungssystem, das in verschiedenen Linux-Distributionen verwendet wird. Es ermöglicht das einfache Herunterladen, Installieren, Aktualisieren und Entfernen von Softwarepaketen.

Frage

Erläutern Sie die Bedeutung von „Recovery Time Objective“ (RTO) und „Recovery Point Objective“ (RPO).

Recovery Time Objective (RTO) und Recovery Point Objective (RPO) sind zwei Schlüsselkonzepte im Bereich der Disaster Recovery Planung.

Recovery Time Objective (RTO) ist die maximale tolerierbare Zeit, die ein System nach einem Ausfall oder einer Störung ausfallen darf, bevor es zu erheblichen Schäden kommt. In anderen Worten, es ist die Zeit, die benötigt wird, um die Funktionsfähigkeit wiederherzustellen.

Die **Recovery Point Objective** (RPO) bezieht sich auf die maximale Menge an Daten, die ein Unternehmen sich leisten kann zu verlieren, bevor es zu erheblichen Schäden kommt. Dies wird oft in Zeiteinheiten gemessen.

Frage

Erklären Sie den Unterschied zwischen einer Offline USV und einer Line Interactive USV.

Gehen Sie hierbei auch auf die Bedeutung der Abkürzungen VFD und VI ein.

Die **Offline USV** (VFD - Voltage and Frequency Dependent) schaltet bei einem Stromausfall automatisch von der Hauptstromquelle auf die Batterieversorgung um. Die Umschaltung erfolgt in der Regel innerhalb weniger Millisekunden. Diese USVs bieten grundlegende Schutzfunktionen, jedoch kann es zu einer kurzen Unterbrechung in der Stromversorgung kommen.

Line Interactive USVs (VI - Voltage Independent) sind ähnlich wie Offline USVs, bieten jedoch zusätzliche Spannungsregulierung und Filterung. Sie sind in der Lage, kleinere Schwankungen in der Stromversorgung zu korrigieren, ohne auf die Batterieversorgung umschalten zu müssen.

Frage

Nennen Sie drei Dienstleistungsmodelle im Cloud-Computing.

Dienstleistungsmodelle von Cloud-Computing:

- **„Software-as-a-Service“ (SaaS):** Servicemodell, bei dem Anwendungen über das Internet bereitgestellt werden
- **„Infrastructure-as-a-Service“ (IaaS):** Servicemodell, bei dem virtuelle Ressourcen, wie z. B. Server und Speicher über das Internet bereitgestellt werden
- **„Platform-as-a-Service“ (PaaS):** Servicemodell, das eine Entwicklungsplattform über das Internet bereitstellt
- **„Desktop-as-a-Service“ (DaaS):** ist ein Servicemodell, bei dem ein virtueller Desktop über das Internet bereitgestellt wird
- **„Everything-as-a-Service“ (XaaS):** ist ein erweitertes Konzept, bei dem alle IT-Dienstleistungen über das Internet bereitgestellt werden

Frage

Was sind die Unterschiede zwischen Cloud-, Fog- und Edge-Computing?

Cloud-, Fog- und Edge-Computing unterscheiden sich in Bezug auf ihre Position in der Datenverarbeitungshierarchie und ihre jeweiligen Standorte:

- **Cloud-Computing** bezieht sich auf die Bereitstellung von IT-Ressourcen über das Internet. Datenverarbeitung und -speicherung erfolgen in großen Rechenzentren, die von Cloud-Anbietern betrieben werden.
- **Fog-Computing** ist eine dezentrale Ergänzung zur Cloud und liegt zwischen der Cloud und den Edge-Geräten. Es erfolgt eine dezentrale Verarbeitung der Daten am Rande des Netzwerks.
- **Edge-Computing** bezieht sich auf die Datenverarbeitung und -speicherung in unmittelbarer Nähe zur Datenquelle.

Frage

Was ist eine Next-Generation Firewall (NGFW)?

Eine **Next-Generation Firewall** (NGFW) ist eine fortschrittliche Firewall, die über die Funktionen herkömmlicher Firewalls hinausgeht. Sie kombiniert Funktionen wie Intrusion Detection/Prevention System (IDS/IPS), Content-Filtering, Anwendungssteuerung und mehr. Durch die Kombination dieser Funktionen ermöglicht eine Next-Generation Firewall eine effektive Sicherheitskontrolle und Bedrohungserkennung.

Frage

Was bedeutet Deep Packet Inspection (DPI)?

Deep Packet Inspection (DPI) ist eine Technologie, bei der der Netzwerkverkehr auf tiefer Ebene analysiert wird, indem der Inhalt der Pakete untersucht wird. DPI geht über die herkömmliche Paketfilterung hinaus, indem es den gesamten Paketinhalt, einschließlich der Nutzdaten, inspiziert. Mithilfe von Algorithmen und Mustererkennungstechniken interpretiert DPI den Paketinhalt, erkennt Protokolle, Anwendungen, Dateitypen und spezifische Inhalte. Es ermöglicht eine umfassende Überwachung, Kontrolle und den Schutz des Netzwerkverkehrs, um Bedrohungen zu erkennen und Richtlinien durchzusetzen.

Frage

Was sind ACLs (Access Control Lists)?

ACLs (Access Control Lists) steuern den Zugriff auf Ressourcen in einem Computersystem. Eine ACL enthält eine Liste von Berechtigungen, die einem bestimmten Benutzer oder einer Gruppe zugeordnet sind.

ACLs definieren, welche Aktionen ein Benutzer oder eine Gruppe auf eine Ressource ausführen darf. Jeder Eintrag in der ACL enthält eine Kombination aus dem Sicherheitsprinzipal (z. B. Benutzername oder Gruppenname) und den zugehörigen Zugriffsrechten. Das Betriebssystem oder die Anwendung überprüft die ACL, wenn ein Zugriffsversuch auf eine Ressource erfolgt, und gewährt oder verweigert den Zugriff basierend auf den definierten Berechtigungen.

Frage

Erklären den Ablauf der DHCP-Kommunikation nach dem DORA-Prinzip.

DHCP-Discover: Ein Gerät, das eine Netzwerkverbindung herstellt, sendet eine Broadcast-Nachricht, um DHCP-Server im Netzwerk zu suchen.

DHCP-Offer: Der DHCP-Server antwortet mit einer Broadcast-Nachricht, in der er dem Gerät eine IP-Adresse und andere Konfigurationsinformationen anbietet.

DHCP-Request: Das Gerät wählt eine der angebotenen IP-Adressen aus und sendet eine Broadcast-Nachricht, um den ausgewählten DHCP-Server über seine Wahl zu informieren.

DHCP-Acknowledgement: Der DHCP-Server antwortet mit einer Broadcast-Nachricht, in der er dem Gerät die zugewiesene IP-Adresse und andere Konfigurationsoptionen bestätigt.