Prüfungsnummer:SC-900

Prüfungsname:(deutsche Version und englische Version) Microsoft Security, Compliance, and Identity Fundamentals

Version:demo

Achtung: Aktuelle englische Version zu SC-900 bei uns ist gratis!!

1.Welches ist ein Anwendungsfall für die Implementierung von Richtlinien für Informationsbarrieren in Microsoft 365?

A.Um den nicht authentifizierten Zugriff auf Microsoft 365 einzuschränken.
B.Um Microsoft Teams-Chats zwischen bestimmten Gruppen innerhalb einer Organisation einzuschränken.
C.Um Microsoft Exchange Online E-Mail zwischen bestimmten Gruppen innerhalb einer Organisation einzuschränken.
D.Um die Datenfreigabe auf externe E-Mail-Empfänger zu beschränken.

Korrekte Antwort: C

Erläuterungen:

Mit Informationsbarrieren können Sie Richtlinien definieren, die bestimmte Benutzersegmente daran hindern sollen, miteinander zu kommunizieren, oder bestimmten Segmenten die Kommunikation nur mit bestimmten anderen Segmenten gestatten.Richtlinien für Informationsbarrieren können Ihrer Organisation helfen, die Einhaltung relevanter Branchenstandards und -vorschriften aufrechtzuerhalten und potenzielle Interessengruppen zu vermeiden.

Konzepte hinter Richtlinien für Informationsbarrieren

Wenn Sie Richtlinien für Informationsbarrieren definieren, arbeiten Sie mit Benutzerkontoattributen, Segmenten, "Blockieren" und/oder "Zulassen"-Richtlinien und Richtlinienanwendung.

Benutzerkontoattribute sind in Azure Active Directory (oder Exchange Online) definiert. Diese Attribute können Abteilung, Position, Standort, Teamname und andere Auftragsprofildetails umfassen.
Segmente sind Benutzergruppen, die im Security & Compliance Center mithilfe eines ausgewählten Benutzerkontoattributs definiert sind.
Mit Richtlinien für Kommunikationsbarrieren werden bestimmte Kommunikationsbeschränkungen festgelegt. Beim Definieren von Richtlinien für Informationsbarrieren können Sie aus zwei Arten von Richtlinien auswählen:
"Blockieren"-Richtlinien verhindern, dass ein Segment mit einem anderen Segment kommuniziert.
"Zulassen"-Richtlinien ermöglichen es einem Segment, nur mit bestimmten anderen

Segmenten zu kommunizieren.
Die Richtlinienanwendung erfolgt, nachdem alle Richtlinien für Kommunikationsbarrieren definiert wurden und Sie bereit sind, sie in Ihrer Organisation anzuwenden.
Derzeit werden Richtlinien für Informationsbarrieren im Office 365 Security & Compliance Center mithilfe von PowerShell-Cmdlets definiert und verwaltet.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Definieren von Richtlinien für Informationsbarrieren

2.Womit können Sie Azure-Ressourcen konsistent über mehrere Abonnements hinweg bereitstellen?

A.Azure Defender
B.Azure Blueprints
C.Azure Sentinel
D.Azure Policy

Korrekte Antwort: B

Erläuterungen:

Genau wie eine Blaupause, die einem Ingenieur oder Architekten die Skizzierung der Entwurfsparameter für ein Projekt ermöglicht, ermöglicht es Azure Blueprints Cloudarchitekten und zentralen IT-Gruppen, eine wiederholbare Gruppe von Azure-Ressourcen zu definieren, mit der die Standards, Muster und Anforderungen einer Organisation implementiert und erzwungen werden. Mit Azure Blueprints können Entwicklungsteams schnell neue Umgebungen bereitstellen und einrichten und dabei darauf vertrauen, dass sie die Konformitätsanforderungen der Organisation erfüllen und über eine Reihe integrierter Komponenten (z. B. Netzwerk) zur Beschleunigung der Entwicklung und Bereitstellung verfügen.

Blaupausen sind eine deklarative Möglichkeit zum Orchestrieren der Bereitstellung mehrerer Ressourcenvorlagen und anderer Artefakte wie etwa:

Rollenzuweisungen
Richtlinienzuweisungen
Azure Resource Manager-Vorlagen (ARM-Vorlagen)
Ressourcengruppen
Der Azure-Dienst für Blaupausen wird vom global verteilten Azure Cosmos DB-Dienst unterstützt. Blaupausenobjekte werden in mehreren Azure-Regionen repliziert. Diese Replikation bietet niedrige Wartezeiten, Hochverfügbarkeit und konsistenten Zugriff auf

Ihre Blaupausenobjekte – unabhängig davon, in welcher Region Ihre Ressourcen von Azure Blueprints bereitgestellt werden.

Unterschiede zu ARM-Vorlagen

Der Dienst soll die Umgebungseinrichtung vereinfachen. Diese Einrichtung umfasst häufig eine Reihe von Ressourcengruppen, Richtlinien, Rollenzuweisungen und Bereitstellungen von ARM-Vorlagen. Eine Blaupause ist ein Paket, in dem die einzelnen Artefakttypen zusammengeführt werden. Sie können das Paket zusammenstellen und versionieren, z. B. auch über eine CI/CD-Pipeline (Continuous Integration/Continuous Delivery). Letztlich wird jede in einem einzelnen Vorgang, der überwacht und nachverfolgt werden kann, einem Abonnement zugewiesen.

Nahezu alle Elemente, die Sie für die Bereitstellung in Azure Blueprints einfügen möchten, können über eine ARM-Vorlage eingefügt werden. Eine ARM-Vorlage ist aber ein Dokument, das in Azure nicht nativ vorhanden ist, sondern entweder lokal oder in der Quellcodeverwaltung gespeichert wird. Die Vorlage wird für die Bereitstellung einer oder mehrerer Azure-Ressourcen verwendet. Nach der Bereitstellung dieser Ressourcen besteht jedoch keine aktive Verbindung oder Beziehung mehr mit der Vorlage.

Mit Azure Blueprints bleibt die Beziehung zwischen der Blaupausendefinition (was soll bereitgestellt werden) und der Blaupausenzuweisung (was wurde bereitgestellt) erhalten. Diese Verbindung ermöglicht eine erweiterte Nachverfolgung und Überprüfung von Bereitstellungen. Mit Azure Blueprints lassen sich auch mehrere Abonnements, die der gleichen Blaupause unterliegen, gleichzeitig upgraden.

Es besteht nicht die Notwendigkeit, zwischen einer ARM-Vorlage und einer Blaupause zu wählen. Jede Blaupause kann null oder mehr Artefakte für ARM-Vorlagen umfassen. Dies bedeutet, dass bereits durchgeführte Leistungen zur Entwicklung und Verwaltung einer Bibliothek mit ARM-Vorlagen in Azure Blueprints genutzt werden können.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Was ist Azure Blueprint?

3.Wählen Sie für jede der folgenden Aussagen "Ja", wenn die Aussage wahr ist. Andernfalls wählen Sie "Nein".

(Für jede korrekte Markierung erhalten Sie einen Punkt.)

Abbildung

Aussagen	Ja	Nein
Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen.	○	○
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des Azure-Portals verwalten.	○	○
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten.	○	○

A.Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen: Ja
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des Azure-Portals verwalten: Ja
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten: Ja
B.Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen: Ja
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des Azure-Portals verwalten: Ja
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten: Nein
C.Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen: Ja
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des Azure-Portals verwalten: Nein
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten: Nein
D.Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen: Nein
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des Azure-Portals verwalten: Nein
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten: Ja
E.Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen: Nein
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des Azure-Portals verwalten: Ja
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten: Nein
F.Alle Lizenzeditionen von Azure Active Directory (Azure AD) enthalten dieselben Funktionen: Nein
Sie können einen Azure Active Directory (Azure AD)-Mandanten mithilfe des

Azure-Portals verwalten: Nein
Sie müssen virtuelle Azure-Computer bereitstellen, um einen Azure Active Directory (Azure AD)-Mandanten zu hosten: Nein

Korrekte Antwort: E

Erläuterungen:

Azure Active Directory (Azure AD) ist der cloudbasierte Identitäts- und Zugriffsverwaltungsdienst von Microsoft, mit dem sich Ihre Mitarbeiter anmelden und auf die folgenden Ressourcen zugreifen können:

Externe Ressourcen wie Microsoft 365, das Azure-Portal und Tausende andere SaaS-Anwendungen.

Interne Ressourcen (beispielsweise Apps im Netzwerk/Intranet Ihres Unternehmens oder selbst entwickelte Cloud-Apps Ihrer Organisation).

Microsoft Online-Unternehmensdienste wie Microsoft 365 oder Microsoft Azure benötigen Azure AD für die Anmeldung sowie zum Schutz von Identitäten. Wenn Sie einen Microsoft Online-Unternehmensdienst abonnieren, erhalten Sie automatisch Azure AD und damit Zugriff auf alle kostenlosen Features.

Zur Erweiterung Ihrer Azure AD-Implementierung können Sie auch kostenpflichtige Funktionen hinzufügen, indem Sie auf Azure Active Directory-Lizenzen vom Typ „Premium P1“ oder „Premium P2“ upgraden. Die kostenpflichtigen Azure AD-Lizenzen ergänzen Ihr kostenloses Verzeichnis und bieten Self-Service-Funktionen, eine erweiterte Überwachung, Sicherheitsberichte sowie sicheren Zugriff für Ihre mobilen Benutzer.

Azure AD kann auf verschiedene Weise verwaltet werden, einschließlich dem Azure Portal, Azure PowerShell und Azure CLI.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Was ist Azure Active Directory?

4.Wählen Sie die Antwort, die den Satz richtig vervollständigt.

(Wählen Sie zum Beantworten der Frage die entsprechende Option im Antwortbereich aus.)

Abbildung

Antwortbereich

A.Sie können Microsoft Intune mit dem Azure Active Directory Admin Center verwalten.
B.Sie können Microsoft Intune mit dem Microsoft 365 Compliance Center verwalten.
C.Sie können Microsoft Intune mit dem Microsoft 365 Security Center verwalten.
D.Sie können Microsoft Intune mit dem Microsoft Endpoint Manager Admin Center verwalten.

Korrekte Antwort: D

Erläuterungen:

Microsoft Intune ist ein cloudbasierter Dienst, der sich auf die Verwaltung mobiler Geräte (MDM, Mobile Device Management) und mobiler Anwendungen (MAM, Mobile Application Management) konzentriert. Sie bestimmen, wie die Geräte Ihres Unternehmens, einschließlich Mobiltelefone, Tablets und Laptops, genutzt werden. Sie können auch bestimmte Richtlinien konfigurieren, um Anwendungen zu steuern. Beispielsweise können Sie verhindern, dass E-Mails an Personen außerhalb Ihrer Organisation gesendet werden. Intune ermöglicht den Beschäftigten in Ihrer Organisation auch, ihre persönlichen Geräte für Schule, Uni oder Arbeit zu nutzen. Auf persönlichen Geräten sorgt Intune dafür, dass Ihre Unternehmensdaten geschützt bleiben, da Unternehmensdaten von persönlichen Daten isoliert werden können.

Intune ist Teil der Enterprise Mobility + Security-Suite (EMS) von Microsoft. Intune ist in Azure Active Directory (Azure AD) integriert, um zu steuern, wer auf was Zugriff hat. Zum Datenschutz besteht eine Integration in Azure Information Protection. Intune kann mit der Suite von Microsoft 365-Produkten verwendet werden. Beispielsweise können Sie Microsoft Teams, OneNote und andere Microsoft 365-Apps auf Geräten bereitstellen. Mit diesem Feature können die Beschäftigten in Ihrer Organisation auf all ihren Geräten produktiv arbeiten, während die Informationen Ihrer Organisation durch von Ihnen festgelegte Richtlinien geschützt sind.

Wenn Geräte in Intune registriert und verwaltet werden, können Administratoren folgende Aktionen ausführen:

Registrierte Geräte anzeigen und eine Bestandsaufnahme der Geräte erhalten, die auf Ressourcen der Organisation zugreifen.
Geräte konfigurieren, sodass sie den Sicherheits- und Integritätsstandards entsprechen. Beispielsweise möchten Sie wahrscheinlich Geräte mit Jailbreaks blockieren.

Zertifikate per Push an Geräte übermitteln, damit Benutzer problemlos auf Ihr WLAN zugreifen oder über ein VPN eine Verbindung mit Ihrem Netzwerk herstellen können.
Berichte zu Benutzern und Geräten anzeigen, die kompatibel und nicht kompatibel sind.
Organisationsdaten entfernen, wenn ein Gerät verloren geht, gestohlen wurde oder nicht mehr verwendet wird.
Intune-Richtlinien und -Profile für Geräte und Anwendungen werden im Microsoft Endpoint Manager Admin Center erstellt und verwaltet.

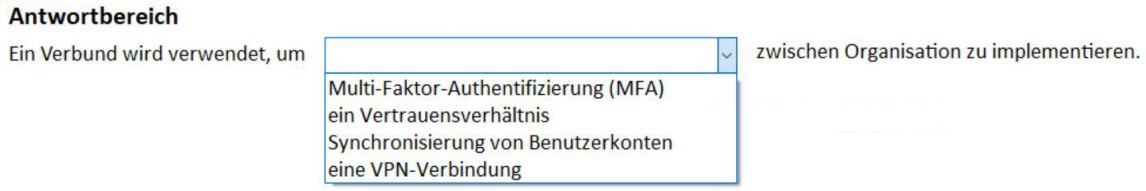
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Microsoft Intune ist ein MDM- und MAM-Anbieter für Ihre Geräte

5.Wählen Sie die Antwort, die den Satz richtig vervollständigt.

(Wählen Sie zum Beantworten der Frage die entsprechende Option im Antwortbereich aus.)

Abbildung



A.Ein Verbund wird verwendet, um Multi-Faktor-Authentifizierung (MFA) zwischen Organisation zu implementieren.
B.Ein Verbund wird verwendet, um ein Vertrauensverhältnis zwischen Organisation zu implementieren.
C.Ein Verbund wird verwendet, um Synchronisierung von Benutzerkonten zwischen Organisation zu implementieren.
D.Ein Verbund wird verwendet, um eine VPN-Verbindung zwischen Organisation zu implementieren.

Korrekte Antwort: B

Erläuterungen:

Ein Verbund ist eine Sammlung von Domänen mit gegenseitiger Vertrauensbeziehung. Der Vertrauensgrad kann variieren, beinhaltet aber in der Regel eine Authentifizierung und fast immer eine Autorisierung. Ein typischer Verbund kann eine Reihe von Organisationen umfassen, die sich gegenseitig vertrauen und gemeinsam auf bestimmte Ressourcen zugreifen.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Worum handelt es sich beim Verbund mit Azure AD?

6.Wählen Sie die Antwort, die den Satz richtig vervollständigt.

(Wählen Sie zum Beantworten der Frage die entsprechende Option im Antwortbereich aus.)

Abbildung

A.Das Archivieren einer Datei macht die Daten in der Datei lesbar und verwendbar für Betrachter, die über den entsprechenden Schlüssel verfügen.
B.Das Komprimieren einer Datei macht die Daten in der Datei lesbar und verwendbar für Betrachter, die über den entsprechenden Schlüssel verfügen.
C.Das Deduplizieren einer Datei macht die Daten in der Datei lesbar und verwendbar für Betrachter, die über den entsprechenden Schlüssel verfügen.
D.Das Verschlüsseln einer Datei macht die Daten in der Datei lesbar und verwendbar für Betrachter, die über den entsprechenden Schlüssel verfügen.

Korrekte Antwort: D

Erläuterungen:

Verschlüsselung ist die Methode, mit der Informationen in einen geheimen Code umgewandelt werden, der die wahre Bedeutung der Informationen verbirgt. Die Wissenschaft des Ver- und Entschlüsselns von Informationen wird Kryptographie genannt.

In der Computertechnik werden unverschlüsselte Daten auch als Klartext (Plaintext) bezeichnet und verschlüsselte Daten als Chiffretext (Cipher). Die zum Kodieren und Dekodieren von Nachrichten verwendeten Formeln werden Verschlüsselungsalgorithmen oder Chiffren genannt.

Um effektiv zu sein, enthält eine Chiffre eine Variable als Teil des Algorithmus. Die

Variable, die als Schlüssel bezeichnet wird, macht die Ausgabe einer Chiffre einzigartig. Wenn eine verschlüsselte Nachricht von einer nicht autorisierten Instanz abgefangen wird, muss der Eindringling erraten, mit welcher Chiffre der Absender die Nachricht verschlüsselt hat und welche Schlüssel als Variablen verwendet wurden. Die Zeit und die Schwierigkeit, diese Informationen zu erraten, machen die Verschlüsselung zu einem so wertvollen Sicherheitswerkzeug.

Die Verschlüsselung ist seit langem eine Methode, um sensible Informationen zu schützen. Historisch wurde es von Militärs und Regierungen verwendet. In der heutigen Zeit wird Verschlüsselung verwendet, um Daten zu schützen, die auf Computern und Speichergeräten gespeichert sind, sowie Daten, die über Netzwerke übertragen werden.

7.Wählen Sie für jede der folgenden Aussagen "Ja", wenn die Aussage wahr ist. Andernfalls wählen Sie "Nein".

(Für jede korrekte Markierung erhalten Sie einen Punkt.)

Abbildung

Aussagen	Ja	Nein
Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt.	○	○
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements bereitgestellt.	○	○
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst.	○	○

A.Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt: Ja
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements bereitgestellt: Ja
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst: Ja
B.Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt: Ja
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements bereitgestellt: Ja
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst: Nein
C.Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt: Nein
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements

bereitgestellt: Ja
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst: Nein
D.Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt: Nein
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements bereitgestellt: Ja
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst: Ja
E.Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt: Nein
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements bereitgestellt: Nein
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst: Ja
F.Azure Active Directory (Azure AD) wird in einer On-Premises Umgebung bereitgestellt: Nein
Azure Active Directory (Azure AD) wird als Teil eines Microsoft 365-Abonnements bereitgestellt: Nein
Azure Active Directory (Azure AD) ist ein Identitäts- und Zugriffsverwaltungsdienst: Nein

Korrekte Antwort: D

Erläuterungen:

Azure Active Directory (Azure AD) ist der cloudbasierte Identitäts- und Zugriffsverwaltungsdienst von Microsoft, mit dem sich Ihre Mitarbeiter anmelden und auf die folgenden Ressourcen zugreifen können:

Externe Ressourcen wie Microsoft 365, das Azure-Portal und Tausende andere SaaS-Anwendungen.

Interne Ressourcen (beispielsweise Apps im Netzwerk/Intranet Ihres Unternehmens oder selbst entwickelte Cloud-Apps Ihrer Organisation).

Azure AD ist für folgende Benutzer konzipiert:

IT-Administratoren. Als IT-Administrator können Sie mit Azure AD den Zugriff auf Ihre Apps und App-Ressourcen steuern, um die Anforderungen Ihres Unternehmens zu erfüllen. So können Sie mit Azure AD beispielsweise beim Zugriff auf wichtige Organisationsressourcen eine mehrstufige Authentifizierung erzwingen. Darüber hinaus können Sie mit Azure AD die Benutzerbereitstellung zwischen Ihrer vorhandenen Windows Server AD-Instanz und Ihren Cloud-Apps (einschließlich Microsoft 365) automatisieren. Azure AD bietet außerdem leistungsfähige Tools zum automatischen Schutz von Benutzeridentitäten und Anmeldeinformationen, um Ihre Anforderungen in puncto Zugriffssteuerung zu erfüllen.

App-Entwickler: Dank eines standardbasierten Ansatzes können Sie als App-Entwickler ihre App mithilfe von Azure AD mit einmaligem Anmelden (Single Sign-On, SSO) ausstatten und es Benutzern so ermöglichen, ihre bereits vorhandenen Anmeldeinformationen zu verwenden. Azure AD stellt außerdem APIs bereit, die Sie bei der Entwicklung personalisierter App-Umgebungen unter Verwendung vorhandener Organisationsdaten unterstützen.

Abonnenten von Microsoft 365, Office 365, Azure oder Dynamics CRM Online: Als Abonnent verwenden Sie bereits Azure AD. Jeder Mandant von Microsoft 365, Office 365, Azure oder Dynamics CRM Online ist automatisch auch ein Azure AD-Mandant. Sie können sofort mit der Verwaltung des Zugriffs auf Ihre integrierten Cloud-Apps beginnen.

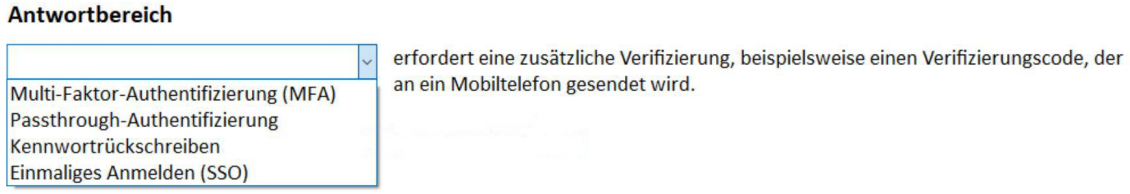
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Was ist Azure Active Directory?

8.Wählen Sie die Antwort, die den Satz richtig vervollständigt.

(Wählen Sie zum Beantworten der Frage die entsprechende Option im Antwortbereich aus.)

Abbildung



A.Multi-Faktor-Authentifizierung (MFA) erfordert eine zusätzliche Verifizierung, beispielsweise einen Verifizierungscode, der an ein Mobiltelefon gesendet wird.
B.Passthrough-Authentifizierung erfordert eine zusätzliche Verifizierung, beispielsweise einen Verifizierungscode, der an ein Mobiltelefon gesendet wird.
C.Kennwortrückschreiben erfordert eine zusätzliche Verifizierung, beispielsweise einen Verifizierungscode, der an ein Mobiltelefon gesendet wird.
D.Einmaliges Anmelden (SSO) erfordert eine zusätzliche Verifizierung, beispielsweise einen Verifizierungscode, der an ein Mobiltelefon gesendet wird.

Korrekte Antwort: A

Erläuterungen:

Multi-Factor-Authentifizierung (mehrstufige Authentifizierung) ist ein Prozess, bei dem

Benutzer während des Anmeldevorgangs zur Durchführung eines weiteren Identifizierungsverfahrens aufgefordert werden, z. B. per Eingabe eines Codes auf dem Smartphone oder per Fingerabdruckscan.

Wenn Sie zum Authentifizieren von Benutzern nur ein Kennwort nutzen, kann dies einen Angriffsvektor darstellen und mit Unsicherheit verbunden sein. Falls das Kennwort nicht sicher ist oder offengelegt wurde, können Sie nicht sicher sein, ob es wirklich der Benutzer ist, der sich mit dem Benutzernamen und dem Kennwort anmeldet, oder ein Angreifer. Wenn Sie ein zweites Authentifizierungsverfahren erzwingen, wird die Sicherheit erhöht, weil dieses zusätzliche Verfahren von einem Angreifer nicht ohne Weiteres nachvollzogen bzw. dupliziert werden kann.

Für Azure AD Multi-Factor Authentication sind mindestens zwei der folgenden Authentifizierungsverfahren obligatorisch:

Eine dem Benutzer bekannte Information (meist ein Kennwort).
Ein im Besitz des Benutzers befindliches Objekt, z. B. ein vertrauenswürdiges Gerät, das nicht ohne Weiteres dupliziert werden kann (Telefon oder Hardwareschlüssel).
Ein biometrisches Merkmal des Benutzers (Fingerabdruck- oder Gesichtsscan).
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

So funktioniert's: Azure AD Multi-Factor Authentication