MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Cloud Governance & Security
im öffentlichen Sektor der Schweiz

Version 1.4

Microsoft

Zugehörige Dokumente

Dokumentname	
Microsoft Public Sector Cloud Design	
Dokument: Azure Services im öffentlichen Sektor der Schweiz V1.4	
Identifikation: Governance and Security Guideline Swiss Public Sector_V1.4	
Azure Blueprints for Public Sector (ISO 27001)	Microsoft Docs

Microsoft

Inhalt

Abbildungen

Disclaimer

Dieses Dokument enthält eine allgemeine Darstellung von Fragen, die unsere Kunden beim Einsatz von Cloud Computing Lösungen häufig stellen. Sie sollen damit in die Lage versetzt werden, die technischen und rechtlichen Hintergründe beim Einsatz einer Cloud Computing Lösung besser zu verstehen. Dieses Dokument beinhaltet keine einzelfallbezogene Prüfung individueller Rechtsverhältnisse. Für die individuelle und abschliessende rechtliche Beurteilung über die Zulässigkeit des Einsatzes von Microsoft Cloud Lösungen in einem konkreten Anwendungsfall müssen Sie daher eine separate rechtliche Beratung in Anspruch nehmen.

1 ZWECK DIESES DOKUMENTS

Dieses Dokument soll als Leitfaden und eine Empfehlung zur technischen Implementation einer standardisierten Cloud Plattformumgebung und deren Operationalisierung dienen. Es werden die im Microsoft Public Sector Cloud Design identifizierten Risiken adressiert. Als Basis wird der Sicherheitsstandard ISO 27001 für die Massnahmen und die Kontrollen herbeigezogen.

2 INHALT UND AUFBAU

Zur Realisierung einer standardisierten Landing Zone in der Azure Public Cloud nach ISO 27001 werden zur Verfügung gestellte Vorlagen für das Deployment von notwendigen Komponenten als auch Kontrollmechanismen verwendet. Hierfür wird zuerst auf die Grundlagenkonzepte der Komponenten und danach auf die einzelnen Kontrollen, welche die Effektivität prüfen, eingegangen.

Wo zutreffend, wird ein Hinweis auf ein identifiziertes und entgegnetes Risiko aus dem Microsoft Public Sector Cloud Design gegeben.

3 GRUNDLAGEN

Die ISO 27001 Vorlagen zum Deployment der Landing Zone Komponenten werden als Azure Blueprints[1] angewendet, welche auf ein oder mehrere Subscriptions appliziert werden. Hierbei werden, Ressourcen Gruppen, Ressourcen, Berechtigungen und Richtlinien erstellt.

- ISO 27001[2] → Dieser Blueprint enthält allgemeine Richtlinien zur Implementation von Massnahmen auf bestehende und zu erstellende Applikationsressourcen.
- ISO 27001: Gemeinsame Dienste[3] → Dieser Blueprint erstellt die nötigen zentralen, geteilten Ressourcen zur Unterstützung des Landing Zone Betriebs inkl. vordefinierter Rollenberechtigungen
- ISO 27001: ASE-/SQL-Workloads[4] → Dieser optionale Blueprint stellt eine oder mehrere standardisierte Web-basierte Applikationsumgebungen bereit, die mittels PaaS-Ressourcen des Typs «App Service» und «SQL DB» realisiert werden.

Zur Berichterstattung der Konformität zu den ISO 27001 Kontrollen wird der Azure Security Center verwendet. Dieser meldet alle Kontrollabweichungen bei Ressourcen in assoziierten Subscriptions. Dies wird durch eine weitere Applizierung einer Richtliniensammlung erreicht, wo lediglich der Auditierungseffekt pro Richtlinie hinterlegt ist.

3.1 LANDING ZONE DESIGN

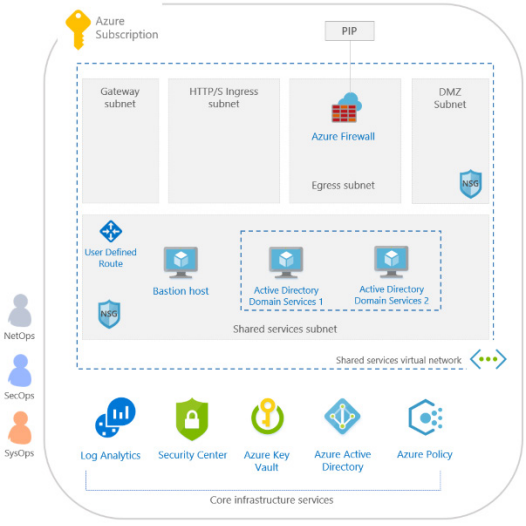

Abbildung 1 – Blueprint ISO 27001 Shared Services

Die Landing Zone basierend auf ISO 27001 ist ein Architekturansatz und eine Referenzimplementierung auf Unternehmensebene, welche die effektive Erstellung und Operationalisierung von Zielzonen in Azure im grossen Stil ermöglicht. Es ist auf die Azure-Roadmap und das Cloud-Adaption Framework[5] für Azure abgestimmt.

Die Architektur sieht einen zentralen, geteilten Bereich in eine Subscription, und weitere einzelne Bereiche für Applikationen (z.B. ISO 27001: ASE-/SQL-Workloads) in eigenen Subscriptions vor. Die einzelnen Komponenten des zentralen Bereichs sind in den nachfolgenden Kapiteln beschrieben.

Die technischen Überlegungen und Design-Empfehlungen dieser Architektur können je nach dem Szenario Ihres Unternehmens zu unterschiedlichen Kompromissen führen. Eine gewisse Abweichung ist zu erwarten, aber wenn Sie die Kernempfehlungen befolgen, wird die resultierende Zielarchitektur Ihre Organisation auf einen Pfad zur nachhaltigen Skalierung bringen.

[1] https://docs.microsoft.com/de-ch/azure/governance/blueprints/overview
[2] https://docs.microsoft.com/de-ch/azure/governance/blueprints/samples/iso-27001-2013
[3] https://docs.microsoft.com/de-ch/azure/governance/blueprints/samples/iso27001-shared
[4] https://docs.microsoft.com/de-ch/azure/governance/blueprints/samples/iso27001-ase-sql-workload
[5] https://docs.microsoft.com/de-ch/azure/cloud-adoption-framework/

3.2 ROLLEN UND ORGANISATION

Die erfolgreiche Einführung einer Cloud Plattform kann nur mit fähigem Personal erreicht werden, welches die anvertrauten Aufgaben mit den entsprechenden Berechtigungen ausführt, um klar definierte Unternehmensziele umzusetzen. Ein solch effektives Betriebskonzept hebt hervor, dass eine klar strukturierte Organisation realisiert werden muss, in der unterschiedliche Verantwortlichkeiten vordefinierten Rollen assoziiert werden, die wiederum ausgebildeten Teams und einzelnen Mitarbeitern zugewiesen sind.

Meist besteht schon eine gewisse IT-Organisation, die lediglich den neuen Gegebenheiten und Aufgaben einer Cloud Plattform wie Azure angepasst bzw. angepasst werden muss. Die folgenden Cloud Funktionen zeigen die nötigen Disziplinen auf, welche die Cloud Adoption vorantreiben und für die es gilt, Rollen zuzuweisen und in der Organisation zu verankern.

- Cloud Strategy → Adaption technisch neuer Gegebenheiten an Unternehmensanforderungen
- Cloud Governance → Unternehmensrisiken erkennen und Massnahmen bzw. Konformität definieren
- Cloud Platform Operations → Unterhalt und Betrieb der Cloud Plattform Landing Zone und deren Basisdienste
- Cloud Application Operations → Umsetzung und Betrieb von migrierten Applikationen und neuen Cloud Lösungen
- Cloud Competence Center → Erarbeitung, Einführung und Beratung von neuen Cloud Ansätzen und Technologien
- Cloud Automation → Beschleunigung der Cloud Adoption und deren neuen Prozesse
- Cloud Data → Erarbeiten und Definieren von Unternehmensdatenflüssen zu und aus der Cloud als auch die analytische Anreicherung von Daten in der Cloud mittels definierter Architekturen
- Cloud Security → Gewährleistung des Informationsschutzes und Betrieb sicherheitsrelevanter Aufgaben in der Cloud

Üblicherweise werden auf dem Weg zur Cloud all diese Funktionen und Disziplinen wahrgenommen, jedoch je nach Entwicklungsstadium in unterschiedlich stark differenzierten Ausprägungen der Rollen. Je länger und umfangreicher die Adaption vorangeschritten ist, desto definierter sind diese Rollen und ihre Verantwortungen, die schlussendlich in einer RACI Matrix verankert werden sollten.

3.3 ZUGRIFFSKONZEPTE (RBAC)

Mithilfe von Azure «Role Based Access Control» RBAC können Sie Administrationsaufgaben in Ihrer Organisation auf verschiedene Teams verteilen und Benutzerkonten nur den Zugriff auf Azure Ressourcen gewähren, den sie zur Ausführung ihrer Aufgaben benötigen. Anstatt allen Konten uneingeschränkte Berechtigungen in Ihrer Azure-Subscription oder Ihren Ressourcen zu gewähren, sollten Sie die Berechtigungen auf bestimmte Aktionen in einem bestimmten Bereich (Management Group; Subscription; Ressourcengruppe) beschränken.

Bei der Planung der Strategie für die Zugriffssteuerung hat es sich bewährt, Benutzern die geringsten Rechte zum Ausführen ihrer Aufgaben zu erteilen. Vermeiden Sie es, umfangreichere Rollen in umfassenderen Bereichen zuzuweisen, auch wenn dies anfänglich bequemer erscheint. Wenn Sie benutzerdefinierte Rollen erstellen, schliessen Sie nur die Berechtigungen ein, die Benutzer benötigen. Durch das Einschränken von Rollen und Bereichen, begrenzen Sie die Ressourcen, die gefährdet sind, falls der Sicherheitsprinzipal kompromittiert wird.

Das folgende Diagramm zeigt einen Vorschlag der Verschachtelung der Elemente zum Berechtigungszweck:

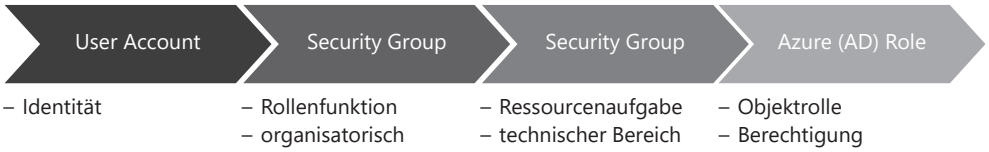

Abbildung 2 – RBAC Verschachtelung

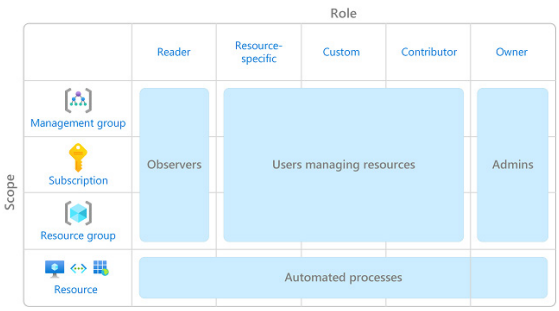

Abbildung 3 – Anwendungsbereiche Rollenberechtigungen

Das folgende Schema veranschaulicht die möglichen Bereiche, für die eine Rollenberechtigung an einen Benutzer mittels Gruppenzuweisung zugewiesen werden kann.

3.4 AZURE ARC

In aller Regel werden nicht auf einen Schlag sämtliche IT-Ressourcen in die Cloud verschoben. Allenfalls werden gar gewisse Ressourcen basierend auf einer Multi Cloud-Strategie in die Rechenzentren eines anderen Anbieters migriert. Azure Arc bietet für solche Hybrid- und Multi Cloud-Szenarien zentrale Verwaltungsmöglichkeiten. Damit ist es für den Kunden möglich, die umfassenden Sicherheits- und Konformitätsangebote auch für Ressourcen zu nutzen, welche sich nicht oder noch nicht in Azure befinden.

Anwendungsfälle und Szenarien

- Zentrale Visibilität über eine grosse Bandbreite an Ressourcen (Windows, Linux, Kubernetes)
- Organisation und Inventarisierung aller Ressourcen in Verwaltungsgruppen, Subscriptions, Ressourcengruppen oder Tags
- Ausweitung Automatisierung und Konfigurationsverwaltung
- Verwaltung von Sicherheitsrichtlinien
- Verwaltung von Zugriffen mit der rollenbasierten Zugriffssteuerung und Azure Lighthouse
- Provisionierung von Datenbanken (SQL, PostgreSQL) in Kubernetes-Cluster, lokal oder in einer anderen Cloud
- Suche in mehreren Umgebungen mittels Azure Resource Graph

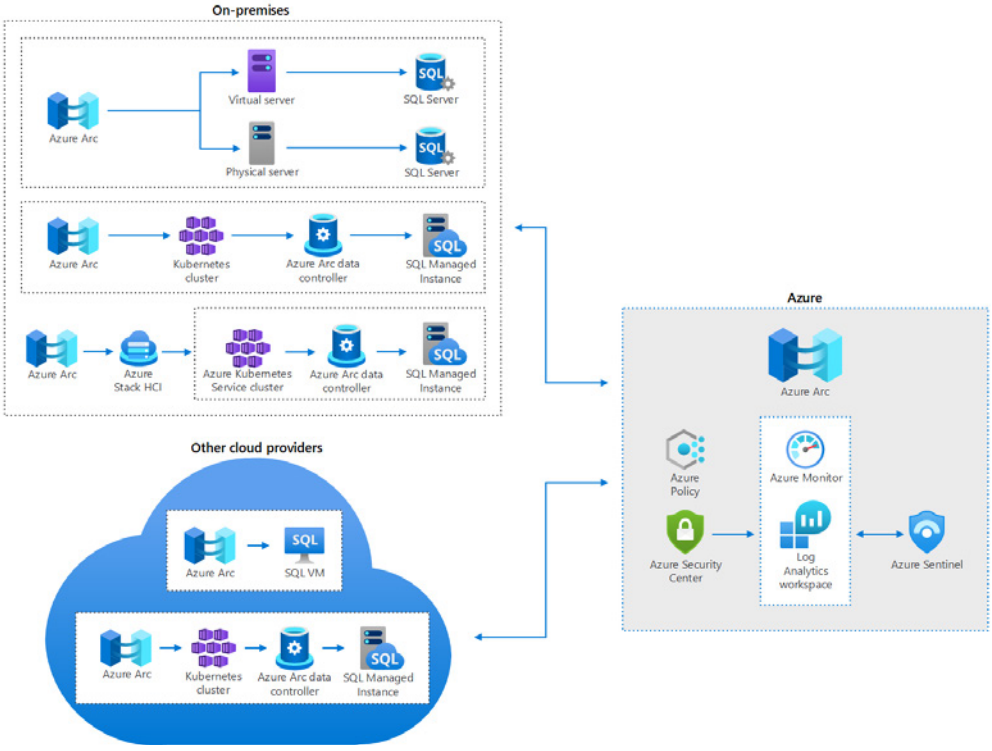

Abbildung 4 – Funktionsübersicht Azure Arc

3.5 POLICIES UND SICHERHEITSEINSTELLUNGEN

Azure Policy hilft bei der Durchsetzung von Organisationsstandards und bei der Bewertung der Compliance nach Bedarf. Über sein Compliance-Dashboard bietet der Dienst eine aggregierte Ansicht zur Bewertung des Gesamtzustands der Umgebung mit der Möglichkeit, einen Drilldown zur granularen Bewertung pro Ressource und Richtlinie durchzuführen. Ausserdem trägt er durch Massenwartung für vorhandene Ressourcen und automatische Wartung dazu bei, dass Ihre Ressourcen Compliance-Anforderungen erfüllen.

Häufige Anwendungsfälle für Azure Policy sind die Implementierung von Governance für Ressourcenkonsistenz, Einhaltung gesetzlicher Bestimmungen, Sicherheit, Kosten und Verwaltung. Richtliniendefinitionen für diese häufigen Anwendungsfälle sind in ihrer Azure-Umgebung bereits integriert bereitgestellt, um Ihnen den Einstieg zu erleichtern.

Azure Policy schränkt Aktionen nicht grundsätzlich ein, es stellt sicher, dass der Ressourcenzustand Ihren Geschäftsregeln entspricht, unabhängig davon, wer die Änderungen vorgenommen hat oder wer die Berechtigung hat, eine Änderung vorzunehmen.

Um einen Überblick über den aktuellen Status der Richtlinien zu erhalten, kann die Übersicht von Azure Policies selbst genutzt werden. Diese gibt einen Überblick über den aktuellen Status der bereitgestellten Richtlinien.

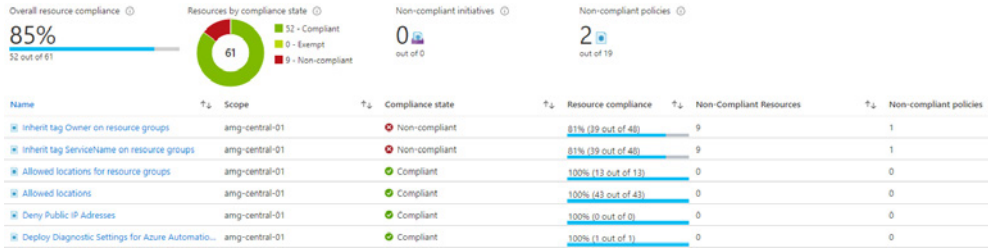

Abbildung 5 – Übersichtsbericht Compliance

Empfehlungen:

- Beginnen Sie jeweils mit einem Audit-Effekt anstelle eines Verweigerungseffekts, um die Auswirkungen Ihrer Richtliniendefinition auf die Ressourcen in Ihrer Umgebung zu verfolgen. Wenn Sie bereits über Skripte zur automatischen Skalierung Ihrer Anwendungen verfügen, kann die Einstellung eines Verweigerungseffekts solche bereits vorhandenen Automatisierungsaufgaben behindern.
- Beim Erstellen von Definitionen wird empfohlen, diese auf höchster Ebene zu erstellen, z.B. auf Management Group Ebene oder Subscription Ebene. Wenn Sie eine Definition auf der Ebene einer Management Group erstellen, kann die Zuweisung auf eine Subscription oder Resource Group innerhalb dieser Management Group erfolgen.
- Wir empfehlen, Initiativendefinitionen auch für eine einzelne Richtliniendefinition anzulegen und zuzuordnen. Beispiel: Sie haben eine Richtliniendefinition policyDefA und erstellen diese unter der Initiativendefinition initiativeDefC. Wenn Sie später eine weitere Richtliniendefinition für RichtlinieDefB mit ähnlichen Zielen wie RichtlinieDefA erstellen, können Sie sie unter InitiativeDefC hinzufügen und sie gemeinsam verfolgen.
- Sobald Sie eine Initiativenzuweisung erstellt haben, werden die der Initiative hinzugefügten Richtliniendefinitionen auch Teil der Zuweisungen dieser Initiative.
- Wenn eine Initiativenzuweisung bewertet wird, werden auch alle Richtlinien innerhalb der Initiative bewertet. Wenn Sie eine Richtlinie einzeln bewerten müssen, ist es besser, sie nicht in eine Initiative aufzunehmen.

3.5.1 Allowed Location Policy

Um sicherzustellen, dass Azure-Ressourcen nur an bestimmten Standorten bereitgestellt werden, können integrierte Richtlinien verwendet werden:

- Allowed locations
- Allowed locations for resource groups

Diese Richtlinien ermöglichen es, die Bereitstellung von Ressourcen in anderen Regionen zu verhindern.

3.6 MONITORING

Azure Monitor hilft Ihnen, die Verfügbarkeit und Leistung Ihrer Anwendungen und Dienste zu maximieren. Es bietet eine umfassende Lösung zum Sammeln, Analysieren und Verarbeiten von Telemetriedaten aus Ihren Cloud- und On-Premises-Umgebungen. Diese Informationen helfen Ihnen zu verstehen, wie Ihre Anwendungen funktionieren, um proaktiv Probleme zu erkennen.

Azure Monitor kann Daten aus vielen verschiedenen Quellen sammeln. Dies reicht von Ihrer Anwendung, allen Betriebssystemen und Diensten, von denen Sie abhängig ist, bis hin zur Plattform selbst. Azure Monitor sammelt Daten aus jeder der folgenden Schichten:

– Application monitoring data

– Guest OS monitoring data

– Azure resource monitoring data

– Azure subscription monitoring data

– Azure tenant monitoring data

Bei den meisten Azure Ressourcen können die entsprechenden Logdaten und Metriken über die Diagnostic Settings an eine zentrale Datenverwaltung gesendet werden, wie Log Analytics Workspace. Bei Azure VMs sollte der Log Analytics Agent bereitgestellt werden. Die Bereitstellung kann automatisch über das Security Center erfolgen.

Monitoring Szenarien sind:

– Sicherstellen, dass das System fehlerfrei bleibt

– Nachverfolgen der Verfügbarkeit des Systems und seiner Komponenten

– Verwalten von Leistung, um sicherzustellen, dass sich der Durchsatz des Systems nicht unerwartet verschlechtert, während die Arbeitslast sich erhöht.

– Sicherstellen, dass das System mit Kunden vereinbarte SLAs (Service Level Agreements) erfüllt.

– Schutz der Privatsphäre und der Sicherheit des Systems, der Benutzer und ihrer Daten.

– Verfolgen der Vorgänge, die zu Überwachungs- oder rechtlichen Zwecken ausgeführt werden.

– Überwachen der täglichen Nutzung des Systems und Ermitteln von Trends, die zu Problemen führen könnten, wenn sie nicht behandelt werden.

– Nachverfolgen von auftretenden Problemen, vom ersten Bericht bis zur Analyse der möglichen Ursachen, Berichtigung, folgende Softwareupdates und Bereitstellung.

– Ablaufverfolgung von Vorgängen und das Debuggen von Software-Versionen.

3.7 NETZWERK

Die Azure-Netzwerkdienste bieten eine Vielzahl von Netzwerkfunktionen, die einzeln oder zusammen verwendet werden können.

3.7.1 Was ist ein virtuelles Netzwerk in Azure?

Azure Virtual Network (VNET) ist der grundlegende Baustein für Ihr privates Netzwerk in Azure. Mit VNET können zahlreiche Arten von Azure-Ressourcen (beispielsweise virtuelle Azure-Computer) sicher untereinander sowie mit dem Internet und mit lokalen Netzwerken kommunizieren. VNET ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem Rechenzentrum betreiben, bietet jedoch zusätzliche Vorteile der Infrastruktur von Azure, z. B. Skalierbarkeit, Verfügbarkeit und Isolation.

In Azure gibt es verschiedene Ansätze wie Sie ihr Netzwerk aufbauen können. Es wird empfohlen eine sogenannte Hub- / Spoke Topology aufzubauen, was Vorteile wie Kosteneinsparungen, Workload Isolation und Umgehung von technischen Limitierungen von Azure Subscriptions mit sich bringt.

Hub-spoke network topology in Azure - Azure Reference Architectures | Microsoft Docs

3.7.2 Netzwerksegmentierung

Als Segmentierung wird ein Modell bezeichnet, in dem Sie mithilfe der Tools von Azure softwaredefinierte Perimeter für das Netzwerk erstellen. Anschliessend legen Sie Regeln für den Datenverkehr von bzw. zu diese(n) Perimeter(n) fest, sodass Sie für verschiedene Teile des Netzwerks unterschiedliche Sicherheitsstati festlegen können. Dies ist hilfreich, wenn Sie unterschiedliche Anwendungen (oder Teile einer bestimmten Anwendung) in diese Perimeter aufnehmen, um die Kommunikation zwischen diesen segmentierten Entitäten zu steuern. Dieses Modell bietet einen weiteren Vorteil: Wenn ein Teil des Anwendungsstapels gefährdet ist, können Sie die Auswirkungen dieser Sicherheitsverletzung besser eindämmen und ihre seitliche Ausbreitung im Rest des Netzwerks verhindern. Dies ist ein wichtiges Prinzip des Zero Trust-Modells von Microsoft, das Ihrer Organisation ein erstklassiges Sicherheitskonzept bietet.

Azure bietet dazu folgende Tools:

3.7.2.1 Network Security Groups NSGs

NSGs sind Zugriffssteuerungsmechanismen zum Steuern des Datenverkehrs zwischen Ressourcen in einem virtuellen Netzwerk und mit externen Netzwerken (z. B. mit dem Internet, anderen virtuellen Netzwerken usw.). In NSGs kann die Segmentierungsstrategie durch das Erstellen von Perimetern für ein Subnetz, eine Gruppe von VMs oder sogar eine einzelne VM differenzierter angewendet werden.

3.7.2.2 Application Security Groups ASGs

ASGs bieten ähnliche Steuerungsmechanismen wie NSGs, jedoch für einen Anwendungskontext. Sie können mit ihnen eine Gruppe von VMs unter einem Anwendungstag gruppieren und Datenverkehrsregeln definieren, die dann auf die einzelnen zugrunde liegenden VMs angewendet werden.

3.7.2.3 Firewall

Azure Firewall ist eine zustandsbehaftete (stateful) Firewall als Dienst in der Cloud, die in virtuellen Netzwerken oder in Bereitstellungen von Azure Virtual WAN-Hubs eingesetzt werden kann, um den Datenverkehr zwischen Cloudressourcen, dem Internet und lokalen Umgebungen zu filtern. Sie erstellen Regeln oder Richtlinien (mithilfe von Azure Firewall oder Azure Firewall Manager), wobei Sie mit Layer-3- bis Layer-7-Steuerungen Datenverkehr zulassen/verweigern. Sie können zum Verbessern der Filterung und des Benutzerschutzes auch den Datenverkehr aus dem Internet mithilfe von Azure Firewall und Drittanbietern filtern, indem Sie den gesamten Datenverkehr oder einen Teil davon über externe Sicherheitsanbieter leiten.

3.7.3 Netzwerkanbindung nach Azure

Es gibt 2 Möglichkeiten, die OnPremises Lokationen mit dem Azure Netzwerk zu verbinden, diese sind:

– ExpressRoute (Azure ExpressRoute Overview: Connect over a private connection | Microsoft Docs)

– Site to Site VPN (Informationen zu Azure VPN Gateway | Microsoft Docs)

Der Hauptunterschied dieser zwei Technologien besteht darin, dass bei ExpressRoute die Verbindung über eine private, kostenpflichtige Backbone Verbindung von Microsoft und beim VPN über das öffentliche Internet hergestellt wird. Jedoch sind beide Verbindungen verschlüsselt.

3.8 ACTIVE DIRECTORY

Für den Fall, dass in Azure weiterhin Windows Domain Member Server als IaaS VMs betrieben werden, sieht der ISO 27001 Blueprint im zentralen Bereich Active Directory Domain Controllers vor, welche für die Kerberos Authentisierung und Autorisierung innerhalb des virtuellen Netzwerkes zur Verfügung stehen. Über eine on-Prem Verbindung mittels VPN Gateway oder ExpressRoute im Gateway Subnet, replizieren die Domain Controller mit der bestehenden Active Directory.

Des Weiteren steht ein Bastion Service für den sicheren Fernzugriff auf diese VMs bereit, der es erlaubt dies ohne öffentliche IP-Adressen zu ermöglichen.

3.9 KEY VAULT

Für jegliche Art der Datenverschlüsselung mit kundenverwalteten Schlüsseln (CMK) kommt Azure Key Vault in Kombination mit einem HSM (Hardware-Sicherheitsmodul, lokal oder als Azure managed Service) zum Einsatz. Dieser speichert Chiffrierschlüssel, Passwörter und Zertifikate und gibt diese nur denjenigen Applikationen weiter, die dafür mit ihren Dienstkonten berechtigt sind. Somit wird der Risikofaktor Mensch in der Handhabung dieser Sicherheitselemente ausgeschlossen. Dies erhöht die Sicherheit, da diese «Secrets» nicht manuell eingegeben oder offen in Code hinterlegt werden müssen.

3.10 KOSTENKONTROLLE

Azure Cost Management bietet Tools, mit denen Sie Ihre Ausgaben planen, analysieren und reduzieren können, um Ihren Cloudnutzen zu maximieren. Mithilfe der Kostenkontrolle kann die Cloud Lösung optimiert werden, um die Kosten zu minimieren und um die Vorteile der Cloud zu nutzen.

- **Kostenanalyse** unterstützt Sie bei der Analyse der Kosten. Mit den entsprechenden Ansichten können die kumulierten Kosten auf verschiedene Arten dargestellt werden.
- Mit **Budgets** können entsprechende Warnregeln konfiguriert werden, welche Sie entsprechend bei Erreichung eines gewissen Schwellenwertes warnt.
- **Ratgeberempfehlung** hilft die ungenutzten oder zu wenig genutzten Ressourcen zu identifizieren, damit vorgängige Massnahmen ergriffen werden können um keine Ressourcen zu verschwenden.

Für die Kostenverwaltung können die einzelnen Ressourcen klassifiziert werden, um die Kosten zuzuordnen. Dies kann mittels Tagging umgesetzt werden, hierbei werden einer Ressource entsprechende Metadaten zugeordnet.

Das Tagging ist das wichtigste Verfahren, wenn es um das Verständnis der Daten im Rahmen der Kostenberichterstattung geht. Es ist ein wesentlicher Bestandteil jeder gut verwalteten Umgebung. Darüber hinaus ist dies der erste Schritt zur Erzielung von Governance für eine Umgebung.

Um Kosteninformationen übergreifend für Geschäftseinheiten, Umgebungen und Projekte genau nachverfolgen zu können, muss zunächst ein Standard für das Tagging definiert werden. Im zweiten Schritt wird sichergestellt, dass dieser Standard für das Tagging einheitlich angewendet wird. Mittels Azure Policy können wir sicherstellen, dass auch wirklich alle Ressourcen entsprechend einen Tag haben. Dies kann über ein automatisches Vererben des Tags geschehen oder sogar über das automatische Bereitstellen von Tags bei bestimmten Indikatoren.

3.11 SECURITY CENTER

Das Azure Security Center spielt eine wichtige Rolle in Ihrer Governance-Strategie. Es hilft den Überblick über die Sicherheitshaltung in Azure zu behalten, weil es:

- Bietet eine einheitliche Ansicht der Sicherheit über Ihre Workloads hinweg.
- Sammelt, durchsucht und analysiert Sicherheitsdaten aus einer Vielzahl von Quellen, zu denen auch Firewalls und andere Partnerlösungen gehören.
- Liefert umsetzbare Sicherheitsempfehlungen, um Probleme zu beheben, bevor sie ausgenutzt werden können.
- Kann verwendet werden, um Sicherheitsrichtlinien auf Ihre Hybrid-Cloud-Workloads anzuwenden, um die Einhaltung von Sicherheitsstandards zu gewährleisten. So können die ISO 27001 Standards via Azure Security Center bereitgestellt werden.

Viele Sicherheitsfunktionen, wie Sicherheitsrichtlinien und Empfehlungen, sind kostenlos verfügbar. Einige der fortschrittlicheren Funktionen, wie Just-in-Time-VM-Zugriff und Unterstützung für hybride Workloads, sind unter dem Security Center Standard-Tier verfügbar. Der Just-in-Time-VM-Zugriff kann dazu beitragen, die Angriffsfläche im Netzwerk zu reduzieren, indem der Zugriff auf Verwaltungsports auf Azure-VMs kontrolliert wird.

Mit Azure Security Center können Sie Ihren Sicherheitsstatus erhöhen. Sie erhalten mit dem Dienst Unterstützung beim Identifizieren und Durchführen von Aufgaben, die als bewährte Sicherheitsmethoden empfohlen werden, und implementieren sie dann für Ihre Computer, Datendienste und Apps. Dies umfasst auch die Verwaltung und Durchsetzung Ihrer Sicherheitsrichtlinien sowie die Sicherstellung, dass Ihre virtuellen Azure-Computer, Azure-externen Server und Azure PaaS-Dienste konform sind. Mit Security Center erhalten Sie die Tools, die Sie benötigen, um den Gesamtüberblick über Ihre Workloads und besonders über die Sicherheitseinrichtungen Ihres Netzwerks zu behalten.

4 ISO 27001 KONTROLLEN

Jedes der folgenden Steuerelemente ist mit einer oder mehreren Azure-Richtliniendefinitionen verknüpft. Diese Richtlinien können Ihnen helfen, die **Konformität** mit dem Steuerelement zu bewerten; allerdings gibt es oft keine eins-zu-eins oder vollständige Übereinstimmung zwischen einem Steuerelement und einer oder mehreren Richtlinien. Daher bezieht sich „**konform**" in Azure-Richtlinien nur auf die Richtlinien selbst; dies stellt nicht sicher, dass Sie alle Anforderungen eines Steuerelements vollständig einhalten. Darüber hinaus umfasst der Konformitätsstandard Kontrollen, die derzeit von keiner Azure-Richtliniendefinition angesprochen werden. Daher ist die Konformität in Azure-Richtlinien nur eine Teilansicht Ihres gesamten Konformitätsstatus. Die Zuordnungen zwischen Kontrollen und Azure-Richtlinien-Definitionen für dieses Compliance Blueprint-Beispiel können sich im Laufe der Zeit ändern.

In den folgenden Kapiteln werden diejenigen ISO 27001 Kontrollen aufgeführt, zu denen Microsoft im Security Center passende Richtlinien realisiert hat, um die Beurteilung technisch auswerten zu können. Abgeleitet von der Risikobeurteilung des Microsoft Public Sector Cloud Designs sind jeweils weitere, potenzielle Kontrollen und Massnahmen ergänzend aufgeführt, die über die Basis hinaus umgesetzt werden könnten.

4.1 A.6.1.2 AUFGABENTRENNUNG

Sich widersprechende Aufgaben und Verantwortungsbereiche müssen getrennt werden, um die Möglichkeiten einer unbefugten oder unbeabsichtigten Änderung oder eines Missbrauchs der Vermögenswerte der Organisation zu verringern.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/

Inhalt Blueprint

Wenn Sie nur einen Azure-Subscription-Besitzer haben, ist keine administrative Redundanz möglich. Umgekehrt kann eine zu hohe Anzahl von Azure-Subscription-Besitzern das Potenzial für einen Verstoss durch ein kompromittiertes Besitzerkonto erhöhen. Dieser Blueprint hilft Ihnen, eine angemessene Anzahl von Azure- Subscription-Besitzern aufrechtzuerhalten, indem Sie zwei Azure-Richtlinien-Definitionen zuweisen, die die Anzahl der Besitzer für Azure Subscriptions überprüfen. Die Verwaltung von Berechtigungen für Subscription-Besitzer kann Ihnen helfen, eine angemessene Aufgabentrennung zu implementieren.

– Es sollten maximal 3 Owner für Ihre Subscription bestimmt werden

– Ihrer Subscription sollte mehr als ein Owner zugewiesen sein

Ergänzende Massnahmen und Richtlinien

– Anzahl stehender Globaler Administratoren für den Notfall auf ein Minimum (Empfehlung: 2–3) beschränken.

– Rollenkonzept ohne Nutzung von Globalen Administration oder Subscription Owner implementieren.

4.2 A.8.2.1 KLASSIFIZIERUNG VON INFORMATIONEN

Informationen müssen in Bezug auf rechtliche Anforderungen, Wert, Kritikalität und Empfindlichkeit gegenüber unbefugter Offenlegung oder Änderung klassifiziert werden, idealerweise so, dass sie die Geschäftstätigkeit widerspiegeln, anstatt sie zu behindern oder zu erschweren.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-8-asset-management/

Inhalt Blueprint

Der Azure-Dienst „SQL Vulnerability Assessment" kann Ihnen dabei helfen, sensible Daten zu entdecken, die in Ihren Datenbanken gespeichert sind, und enthält Empfehlungen zur Klassifizierung dieser Daten.

– Sicherheitslücken in Ihren SQL-Datenbanken sollten behoben werden

Ergänzende Massnahmen und Richtlinien

– Ressourcen welche Daten enthalten, sollten mittels Resource Tags klassifiziert werden.

– Mittels Azure Purview können Dateninhalte in unterstützten Ressourcen übergreifend klassifiziert und zur Auffindung in einem Datenkatalog erfasst werden.

4.3 A.9.1.2 ZUGANG ZU NETZWERKEN UND NETZWERKDIENSTEN

Das Prinzip des geringsten Zugriffs ist der allgemeine Ansatz, der für den Schutz bevorzugt wird, anstatt unbegrenzten Zugriff und Superuser-Rechte ohne sorgfältige Abwägung.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Azure implementiert die Azure rollenbasierte Zugriffskontrolle (Azure RBAC), um zu verwalten, wer Zugriff auf Azure-Ressourcen hat. Dieser Blueprint hilft Ihnen, den Zugriff auf Azure-Ressourcen zu kontrollieren, indem Sie Azure-Richtlinien-Definitionen zuweisen. Diese Richtlinien überprüfen die Verwendung von Ressourcentypen und -konfigurationen, die einen freizügigeren Zugriff auf Ressourcen erlauben können. Das Verständnis von Ressourcen, die gegen diese Richtlinien verstossen, kann Ihnen helfen, Korrekturmassnahmen zu ergreifen, um sicherzustellen, dass der Zugriff auf Azure-Ressourcen auf autorisierte Benutzer beschränkt ist.

– Systemseitig zugewiesene verwaltete Identität hinzufügen, um Gastkonfigurationszuweisungen auf VMs ohne Identität zu aktivieren

– Systemseitig zugewiesene verwaltete Identität hinzufügen, um Gastkonfigurationszuweisungen auf VMs mit einer benutzerseitig zugewiesenen Identität zu aktivieren

– Linux-Computer überwachen, die Remoteverbindungen über Konten ohne Kennwörter zulassen

– Linux-Computer überwachen, die Konten ohne Kennwörter verwenden

– Virtuelle Computer überwachen, die keine verwalteten Datenträger verwenden

– Erweiterung für die Linux-Gastkonfiguration bereitstellen, um Gastkonfigurationszuweisungen für Linux-VMs zu aktivieren

– Speicherkonten sollten zu neuen Azure Resource Manager-Ressourcen migriert werden

– VMs sollten zu neuen Azure Resource Manager-Ressourcen migriert werden

Ergänzende Massnahmen und Richtlinien

– Berechtigungen auf virtuelle Netzwerkkomponenten nur verantwortlichen Rollen (Gruppen) ermöglichen.

– Verhinderung der freien Erstellung von öffentlichen IP Adress-Ressourcen.

4.4 A.9.2.3 VERWALTUNG VON PRIVILEGIERTEN ZUGRIFFSRECHTEN

Die Zuweisung und Verwendung von privilegierten Zugriffsrechten muss angesichts der zusätzlichen Rechte, die üblicherweise über Informationsbestände und die sie kontrollierenden Systeme vergeben werden, streng kontrolliert werden.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Dieser Blueprint hilft Ihnen, privilegierte Zugriffsrechte einzuschränken und zu kontrollieren, indem Sie Azure-Richtliniendefinitionen zuweisen, um externe Konten mit Owner- und/oder Schreibberechtigungen und Konten mit Owner- und/oder Schreibberechtigungen, die keine Multi-Faktor-Authentifizierung (MFA) aktiviert haben, zu überprüfen. Azure rollenbasierte Zugriffskontrolle (Azure RBAC) hilft bei der Verwaltung, wer Zugriff auf Azure-Ressourcen hat. Dieser Blueprint weist auch Azure-Richtlinien-Definitionen zu, um die Verwendung der Azure Active Directory-Authentifizierung für SQL Server und Service Fabric zu überprüfen. Die Verwendung der Azure Active Directory-Authentifizierung ermöglicht eine vereinfachte Verwaltung von Berechtigungen und eine zentralisierte Identitätsverwaltung von Datenbankbenutzern und anderen Microsoft-Diensten. Dieser Blueprint weist auch eine Azure-Richtlinien-Definition zu, um die Verwendung von benutzerdefinierten Azure RBAC-Regeln zu prüfen. Das Verständnis, wo benutzerdefinierte Azure RBAC-Regeln implementiert werden, kann Ihnen helfen, die Notwendigkeit und die richtige Implementierung zu überprüfen, da benutzerdefinierte Azure RBAC-Regeln fehleranfällig sind.

- Ein Azure Active Directory-Administrator sollte für SQL-Server bereitgestellt werden
- Audit der Verwendung von benutzerdefinierten RBAC-Regeln
- Externe Konten mit Besitzerrechten sollten aus Ihrer Subscription entfernt werden
- Externe Konten mit Schreibberechtigungen sollten aus Ihrer Subscription entfernt werden
- MFA sollte aktiviert sein bei Konten mit Schreibrechten auf Ihre Subscriptions
- MFA sollte auf Konten mit Besitzerrechte für Ihre Subscriptions aktiviert sein
- Service-Fabric-Cluster sollten nur Azure Active Directory für die Client-Authentifizierung verwenden

Ergänzende Massnahmen und Richtlinien

- Implementation von Azure AD Privileged Identity Management (PIM) zur zeit- und genehmigungsbasierten Aktivierung von privilegierten Rollen und Berechtigungen.
- Implementation von Azure AD Entitlement Management zum Unterhalt des Identitäts- und Zugriffslebenszyklus.

4.5 A.9.2.4 VERWALTUNG DER GEHEIMEN AUTHENTIFIZIERUNGSINFORMATIONEN VON BENUTZERN

Geheime Authentifizierungsinformationen sind ein Tor zum Zugriff auf wertvolle Vermögenswerte. Sie umfassen typischerweise Passwörter, Verschlüsselungsschlüssel usw. und müssen daher durch einen formalen Verwaltungsprozess kontrolliert und für den Benutzer vertraulich gehalten werden.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Dieser Blueprint weist drei Azure-Richtlinien-Definitionen zu, um Konten zu überprüfen, für die keine Multi-Faktor-Authentifizierung aktiviert ist. Die Multi-Faktor-Authentifizierung hilft dabei, Konten sicher zu halten, selbst wenn ein Teil der Authentifizierungsinformationen kompromittiert wird. Durch die Überwachung von Konten ohne aktivierte Multi-Faktor-Authentifizierung können Sie Konten identifizieren, die mit höherer Wahrscheinlichkeit kompromittiert werden können. Dieser Blueprint weist auch zwei Azure-Richtlinien-Definitionen zu, die die Linux-VM-Passwortdateiberechtigungen überprüfen, um zu warnen, wenn sie falsch eingestellt sind. Mit dieser Einrichtung können Sie Korrekturmassnahmen ergreifen, um sicherzustellen, dass Authentifikatoren nicht kompromittiert werden.

- Systemseitig zugewiesene verwaltete Identität hinzufügen, um Gastkonfigurationszuweisungen auf VMs ohne Identität zu aktivieren
- Systemseitig zugewiesene verwaltete Identität hinzufügen, um Gastkonfigurationszuweisungen auf VMs mit einer benutzerseitig zugewiesenen Identität zu aktivieren
- Linux-Computer überwachen, bei denen die passwd-Dateiberechtigungen nicht auf 0644 festgelegt sind
- Erweiterung für die Linux-Gastkonfiguration bereitstellen, um Gastkonfigurationszuweisungen für Linux-VMs zu aktivieren
- Für Konten mit Schreibberechtigungen für Ihre Subscriptions muss MFA aktiviert sein
- MFA sollte für Konten mit Besitzerberechtigungen in Ihren Subscriptions aktiviert sein
- MFA sollte für Ihre Subscription-Konten mit Leseberechtigungen aktiviert sein

4.6 A.9.2.5 ÜBERPRÜFUNG DER BENUTZERZUGRIFFSRECHTE

Eigentümer von Informationen und Systemen müssen die Zugriffsrechte der Benutzer in regelmässigen Abständen überprüfen, sowohl im Zusammenhang mit individuellen Änderungen (Onboarding, Rollenwechsel und Austritt) als auch mit umfassenderen Audits des Systemzugriffs. Berechtigungen für privilegierte Zugriffsrechte sollten in kürzeren Abständen überprüft werden, da sie mit einem höheren Risiko verbunden sind.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Azure rollenbasierte Zugriffskontrolle (Azure RBAC) hilft Ihnen zu verwalten, wer Zugriff auf Ressourcen in Azure hat. Über das Azure-Portal können Sie überprüfen, wer Zugriff auf Azure-Ressourcen und deren Berechtigungen hat. Dieser Blueprint weist vier Azure-Richtliniendefinitionen zu, um Konten zu überprüfen, die für die Überprüfung priorisiert werden sollten, einschliesslich abgeschriebener Konten und externer Konten mit erhöhten Berechtigungen.

- Veraltete Konten sollten aus Ihren Subscriptions entfernt werden
- Veraltete Konten mit Besitzerberechtigungen sollten aus Ihren Subscriptions entfernt werden
- Externe Konten mit Besitzerberechtigungen sollten aus Ihren Subscriptions entfernt werden
- Externe Konten mit Schreibberechtigungen sollten aus Ihren Subscriptions entfernt werden

Ergänzende Massnahmen und Richtlinien

Mittels Azure AD Access Review sollten stehende Rollenberechtigungen regelmässig überprüft werden, um sicherzustellen, dass keine nicht mehr zulässige Zugriffe stattfinden können.

4.7 A.9.2.6 AUFHEBUNG ODER ANPASSUNG VON ZUGRIFFSRECHTEN

Zugriffsrechte aller Mitarbeiter und externen Benutzer auf Informationen und Informationsverarbeitungseinrichtungen müssen bei Beendigung des Arbeitsverhältnisses, des Vertrags oder der Vereinbarung entfernt werden (oder bei einem Rollenwechsel angepasst werden, falls erforderlich).

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Azure rollenbasierte Zugriffskontrolle (Azure RBAC) hilft Ihnen zu verwalten, wer Zugriff auf Ressourcen in Azure hat. Mit Azure Active Directory und Azure RBAC können Sie Benutzerrollen aktualisieren, um organisatorische Änderungen widerzuspiegeln. Bei Bedarf können Konten für die Anmeldung gesperrt (oder entfernt) werden, wodurch die Zugriffsrechte auf Azure-Ressourcen sofort aufgehoben werden. Dieser Blueprint weist zwei Azure-Richtlinien-Definitionen zu, um ein abgeschriebenes Konto zu überprüfen, das für die Entfernung in Betracht gezogen werden sollte.

– Veraltete Konten sollten aus Ihren Subscriptions entfernt werden

– Veraltete Konten mit Besitzerberechtigungen sollten aus Ihren Subscriptions entfernt werden

Ergänzende Massnahmen und Richtlinien

– Mittels Azure AD Access Review sollten stehende Rollenberechtigungen regelmässig überprüft werden, um sicherzustellen, dass keine nicht mehr zulässige Zugriffe stattfinden können.

4.8 A.9.4.2 SICHERE ANMELDEVERFAHREN

Der Zugriff auf Systeme und Anwendungen muss durch ein sicheres Anmeldeverfahren kontrolliert werden, um die Identität des Benutzers nachzuweisen. Dies kann über den typischen Passwort-Ansatz hinausgehen und je nach Risiko eine Multi-Faktor-Authentifizierung, Biometrie, Smartcards und andere Mittel der Verschlüsselung umfassen.

Die sichere Anmeldung sollte so gestaltet sein, dass sie nicht leicht umgangen werden kann und dass alle Authentifizierungsinformationen verschlüsselt übertragen und gespeichert werden, um ein Abfangen und einen Missbrauch zu verhindern.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Dieser Blueprint weist drei Azure-Richtliniendefinitionen zu, um Konten zu überprüfen, für die die Multi-Faktor-Authentifizierung nicht aktiviert ist. Die Azure-Multifaktor-Authentifizierung bietet zusätzliche Sicherheit, indem sie eine zweite Form der Authentifizierung erfordert und eine starke Authentifizierung liefert. Durch die Überwachung von Konten ohne aktivierte Multi-Faktor-Authentifizierung können Sie Konten identifizieren, die mit höherer Wahrscheinlichkeit kompromittiert werden können.

– Für Konten mit Schreibberechtigungen für Ihre Subscriptions muss MFA aktiviert sein

– MFA sollte für Konten mit Besitzerberechtigungen in Ihren Subscriptions aktiviert sein

– MFA sollte für Ihre Subscription-Konten mit Leseberechtigungen aktiviert sein

Ergänzende Massnahmen und Richtlinien

– Mittels Azure AD Conditional Access sollten aufgrund der Beurteilung von Anwendungs- und Anwenderrisiken unterschiedliche Anmeldebeschränkungen eintreffen können

– Speicherkonten sollten den anonymen Zugriff nicht erlauben

4.9 A.9.4.3 PASSWORTVERWALTUNGSSYSTEM

Der Zweck eines Passwort-Management-Systems ist es, sicherzustellen, dass die Qualität der Passwörter den Anforderungen entspricht und konsequent angewendet wird.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-9-access-control/

Inhalt Blueprint

Dieser Blueprint hilft Ihnen, starke Passwörter durchzusetzen, indem Sie Azure-Richtlinien-Definitionen zuweisen, die Windows-VMs überprüfen, die die Mindeststärke und andere Passwortanforderungen nicht durchsetzen. Das Bewusstsein für VMs, die gegen die Passwortstärke-Richtlinie verstossen, hilft Ihnen, Korrekturmassnahmen zu ergreifen, um sicherzustellen, dass die Passwörter für alle VM-Benutzerkonten mit der Richtlinie konform sind.

- Systemseitig zugewiesene verwaltete Identität hinzufügen, um Gastkonfigurationszuweisungen auf VMs ohne Identität zu aktivieren
- Systemseitig zugewiesene verwaltete Identität hinzufügen, um Gastkonfigurationszuweisungen auf VMs mit einer benutzerseitig zugewiesenen Identität zu aktivieren
- Windows-Computer überwachen, die eine Wiederverwendung der vorherigen 24 Kennwörter zulassen
- Windows-Computer überwachen, für die kein maximales Kennwortalter von 70 Tagen gilt
- Windows-Computer überwachen, die kein Mindestkennwortalter von einem Tag verwenden
- Windows-Computer überwachen, auf denen nicht die Einstellung für die Kennwortkomplexität aktiviert ist
- Windows-Computer überwachen, für die keine Mindestkennwortlänge von 14 Zeichen festgelegt ist
- Erweiterung für die Windows-Gastkonfiguration bereitstellen, um Gastkonfigurationszuweisungen für Windows-VMs zu aktivieren

Ergänzende Massnahmen und Richtlinien

- Azure AD Passwörter müssen Textlängen- und Charakteranforderungen genügen
- Implementation von Azure AD Password Protection zur Verhinderung von qualitativ schlechten Passwörtern aus Wörterbüchern

4.10 A.10.1.1 RICHTLINIE FÜR DEN EINSATZ KRYPTOGRAFISCHER KONTROLLEN

Ordnungsgemässer und effizienter Einsatz von Kryptografie zum Schutz der Vertraulichkeit, Authentizität und/oder Integrität der Informationen.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-10-cryptography/

Inhalt Blueprint

Dieser Blueprint hilft Ihnen, Ihre Richtlinie zur Verwendung von Kryptografiesteuerungen durchzusetzen, indem Sie 13 Azure-Richtliniendefinitionen zuweisen, die bestimmte Kryptografiesteuerungen erzwingen und die Verwendung von schwachen kryptografischen Einstellungen überprüfen. Wenn Sie verstehen, wo Ihre Azure-Ressourcen möglicherweise nicht optimale kryptografische Konfigurationen aufweisen, können Sie Korrekturmassnahmen ergreifen, um sicherzustellen, dass die Ressourcen in Übereinstimmung mit Ihrer Informationssicherheitsrichtlinie konfiguriert sind. Insbesondere erfordern die von diesem Blueprint zugewiesenen Richtlinien Verschlüsselung für Blob-Speicherkonten und Data Lake-Speicherkonten; erfordern transparente Datenverschlüsselung auf SQL-Datenbanken; prüfen fehlende Verschlüsselung auf Speicherkonten, SQL-Datenbanken, Festplatten virtueller Maschinen und Automatisierungskontovariablen; prüfen unsichere Verbindungen zu Speicherkonten, Funktions-Apps, Web-Apps, API-Apps und Redis Cache; prüfen schwache Passwortverschlüsselung virtueller Maschinen und prüfen unverschlüsselte Service Fabric-Kommunikation.

- Funktion App soll nur über HTTPS erreichbar sein
- Webanwendung sollte nur über HTTPS erreichbar sein
- API-App sollte nur über HTTPS erreichbar sein
- Bereitstellen von Voraussetzungen zur Überprüfung von Windows-VMs, die keine Passwörter mit umkehrbarer Verschlüsselung speichern
- Auditergebnisse von Windows-VMs anzeigen, die keine Passwörter speichern
- Die Festplattenverschlüsselung sollte auf virtuellen Maschinen angewendet werden
- Automatisierungskonto-Variablen sollten verschlüsselt werden
- Nur sichere Verbindungen zu Ihrem Azure-Cache für Redis sollten aktiviert sein
- Die sichere Übertragung auf Speicherkonten sollte aktiviert sein
- Bei Service-Fabric-Clustern sollte die Eigenschaft ClusterProtectionLevel auf EncryptAndSign gesetzt sein
- Transparente Datenverschlüsselung auf SQL-Datenbanken sollte aktiviert sein

Ergänzende Massnahmen und Richtlinien

- Die Verschlüsselung von Speicherkonten sollte aktiviert sein
- Speicherkonten sollten nur über HTTPS erreichbar sein
- Die Verwendung von TLS 1.2 auf Speicherkonten sollte erzwungen werden

4.11 A.12.4.1 EREIGNISPROTOKOLLIERUNG

Ereignisprotokolle, die Benutzeraktivitäten, Ausnahmen, Fehler und Informationssicherheitsereignisse aufzeichnen, müssen erstellt, aufbewahrt und regelmässig überprüft werden.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Inhalt Blueprint

Mit diesem Blueprint können Sie sicherstellen, dass Systemereignisse protokolliert werden, indem Sie sieben Azure-Richtliniendefinitionen zuweisen, die Protokolleinstellungen auf Azure-Ressourcen überprüfen. Diagnoseprotokolle bieten Einblick in Vorgänge, die innerhalb von Azure-Ressourcen durchgeführt wurden.

- Audit Dependency Agent-Einsatz - VM-Image (OS) nicht aufgelistet
- Audit Dependency Agent-Bereitstellung in Skalierungssätzen für virtuelle Maschinen - VM-Image (OS) nicht aufgelistet
- Audit Log Analytics Agent-Bereitstellung - VM-Image (OS) nicht aufgelistet
- Einsatz des Audit Log Analytics-Agenten in den Skalierungssätzen für virtuelle Maschinen - VM-Image (OS) nicht aufgelistet
- Audit-Diagnoseeinstellung
- Auditing auf dem SQL-Server sollte aktiviert sein

Ergänzende Massnahmen und Richtlinien

- Mithilfe von Azure Policies kann nicht nur überprüft werden ob die entsprechenden Ressourcen auch mit den nötigen Loggingoptionen versehen sind, sondern kann diese auch gleich anwenden.

4.12 A.12.4.3 ADMINISTRATOR- UND BEDIENERPROTOKOLLE

Die Aktivitäten von Systemadministratoren und Systembedienern müssen protokolliert und die Protokolle geschützt und regelmässig überprüft werden. Für privilegierte Konten wie Systemadministratoren und Bediener sollte ein höheres Mass an Protokollierung in Betracht gezogen werden.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Inhalt Blueprint

Mit diesem Blueprint können Sie sicherstellen, dass Systemereignisse protokolliert werden, indem Sie Azure-Richtliniendefinitionen zuweisen, die Protokolleinstellungen auf Azure-Ressourcen überprüfen. Diagnoseprotokolle bieten Einblick in Vorgänge, die innerhalb von Azure-Ressourcen durchgeführt wurden.

- Überwachen der Diagnoseeinstellung
- Die Überwachung in SQL Server muss aktiviert werden
- Die Überwachung in SQL Server muss aktiviert werden
- Für die aufgelisteten VM-Images muss der Dependency-Agent aktiviert werden
- Für die aufgelisteten VM-Images muss der Dependency-Agent in VM-Skalierungsgruppen aktiviert werden
- Für die aufgelisteten VM-Images muss der Log Analytics-Agent aktiviert werden
- Für die aufgelisteten VM-Images muss der Log Analytics-Agent in VM-Skalierungsgruppen aktiviert werden

Ergänzende Massnahmen und Richtlinien

- Überwachen der Azure AD Anmelde- und Auditierungsprotokolle

4.13 A.12.4.4 SYNCHRONISATION DER UHR

Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder eines Sicherheitsbereichs müssen auf eine einzige Referenzzeitquelle synchronisiert werden.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Inhalt Blueprint

Mit diesem Blueprint können Sie sicherstellen, dass Systemereignisse protokolliert werden, indem Sie Azure-Richtliniendefinitionen zuweisen, die Protokolleinstellungen auf Azure-Ressourcen überprüfen. Azure-Protokolle basieren auf synchronisierten internen Uhren, um eine zeitkorrelierte Aufzeichnung von Ereignissen über Ressourcen hinweg zu erstellen.

– Überwachen der Diagnoseeinstellung

– Die Überwachung in SQL Server muss aktiviert werden

– Für die aufgelisteten VM-Images muss der Dependency-Agent aktiviert werden

– Für die aufgelisteten VM-Images muss der Dependency-Agent in VM-Skalierungsgruppen aktiviert werden

– Für die aufgelisteten VM-Images muss der Log Analytics-Agent aktiviert werden

– Für die aufgelisteten VM-Images muss der Log Analytics-Agent in VM-Skalierungsgruppen aktiviert werden

4.14 A.12.5.1 INSTALLATION VON SOFTWARE AUF BETRIEBLICHEN SYSTEMEN

Es müssen Verfahren implementiert werden, um die Installation von Software auf Betriebssystemen zu kontrollieren.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Inhalt Blueprint

Die adaptive Anwendungskontrolle ist eine Lösung von Azure Security Center, mit der Sie kontrollieren können, welche Anwendungen auf Ihren in Azure befindlichen VMs ausgeführt werden können. Dieser Blueprint weist eine Azure-Richtliniendefinition zu, die den Satz der erlaubten Anwendungen überwacht. Diese Fähigkeit hilft Ihnen, die Installation von Software und Anwendungen auf Azure-VMs zu kontrollieren.

– Adaptive Anwendungssteuerung zum Definieren sicherer Anwendungen muss auf Computern aktiviert sein

4.15 A12.6.1 MANAGEMENT VON TECHNISCHEN SCHWACHSTELLEN

Informationen über technische Schwachstellen der eingesetzten Informationssysteme müssen rechtzeitig eingeholt, die Gefährdung der Organisation durch solche Schwachstellen bewertet und geeignete Massnahmen zur Behebung des damit verbundenen Risikos getroffen werden.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Inhalt Blueprint

Dieser Blueprint hilft Ihnen bei der Verwaltung von Schwachstellen in Informationssystemen, indem Sie Azure-Richtlinien-Definitionen zuweisen, die fehlende System-Updates, Betriebssystem-Schwachstellen, SQL-Schwachstellen und Schwachstellen virtueller Maschinen in Azure Security Center überwachen. Azure Security Center bietet Berichtsfunktionen, mit denen Sie in Echtzeit einen Einblick in den Sicherheitsstatus der bereitgestellten Ressourcen erhalten.

– Auf Ihren virtuellen Computern muss eine Lösung zur Sicherheitsrisikobewertung installiert werden

– Fehlenden Endpoint Protection-Schutz in Azure Security Center überwachen

– Ermittelte Sicherheitsrisiken für SQL-Datenbanken müssen behoben werden

– Systemupdates sollten auf Ihren Computern installiert sein

– Sicherheitsrisiken in der Sicherheitskonfiguration für Ihre Computer sollten beseitigt werden

4.16 A.12.6.2 EINSCHRÄNKUNGEN BEI DER SOFTWAREINSTALLATION

Es müssen Regeln für die Installation von Software durch Benutzer festgelegt und implementiert werden. Diese Kontrolle bezieht sich auf die Einschränkung der Fähigkeit von Benutzern, Software zu installieren, insbesondere auf lokalen Geräten (Arbeitsstationen, Laptops usw.).

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Inhalt Blueprint

Die adaptive Anwendungskontrolle ist eine Lösung von Azure Security Center, mit der Sie kontrollieren können, welche Anwendungen auf Ihren in Azure befindlichen VMs ausgeführt werden können. Dieser Blueprint weist eine Azure-Richtliniendefinition zu, die den Satz der erlaubten Anwendungen überwacht. Einschränkungen bei der Softwareinstallation können Ihnen helfen, die Wahrscheinlichkeit der Einführung von Softwareschwachstellen zu verringern.

– Adaptive Anwendungssteuerung zum Definieren sicherer Anwendungen muss auf Computern aktiviert sein

Ergänzende Massnahmen und Richtlinien

– Sekundäre Source Control Management (SCM) Schnittstellen (z.B. Kudu, GitHub Integration, etc.) von unterstützten Ressourcen sind abzusichern

4.17 A.13.1.1 NETZWERKSTEUERUNG

Netzwerke müssen verwaltet und kontrolliert werden, um Informationen innerhalb von Systemen und Anwendungen zu schützen.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-13-communications-security/

Inhalt Blueprint

Dieser Blueprint hilft Ihnen bei der Verwaltung und Kontrolle von Netzwerken, indem Sie eine Azure-Richtliniendefinition zuweisen, die Netzwerksicherheitsgruppen mit permissiven Regeln überwacht. Regeln, die zu freizügig sind, können unbeabsichtigten Netzwerkzugriff erlauben und sollten überprüft werden. In diesem Blueprint werden ausserdem drei Azure-Richtliniendefinitionen zugewiesen, die ungeschützte Endpunkte, Anwendungen und Speicherkonten überwachen. Endpunkte und Anwendungen, die nicht durch eine Firewall geschützt sind, sowie Speicherkonten mit unbeschränktem Zugriff können unbeabsichtigten Zugriff auf enthaltene Informationen innerhalb des Informationssystems ermöglichen.

– Der Zugriff über den internetfähigen Endpunkt sollte eingeschränkt werden

– Speicherkonten sollten den Netzwerkzugriff einschränken

Ergänzende Massnahmen und Richtlinien

- Erzwungene Zuweisung von NSGs auf Subnetzen zur Einschränkung des erlaubten Datenverkehrs.
- Erzwungene Zuweisung von Routing Tables auf Subnetzen zum Steuern des ausgehenden Datenverkehrs über eine Firewall.
- Implementation von Private Endpoints für alle unterstützten PaaS Dienste zur Einschränkung der Netzwerkkommunikation zwischen Applikationskomponenten auf private Netzwerke
- Einsatz von gesicherten Netzwerkfunktionen zur Publizierung von Web-Anwendungen ins oder Zugriff aus dem Internet:
  - Application Gateway (für Web Applikationen)
  - Azure Front Door (für Multiregion Web Apps)
  - Load Balancer (für eine public IP für Applikationen)
  - NAT Gateway (public IP für ausgehenden Internetverkehr)
  - Bastion Host (für remote Desktop Zugriff auf VMs)

4.18 A.13.2.1 RICHTLINIEN UND VERFAHREN ZUR INFORMATIONSÜBERTRAGUNG

Es müssen formale Übertragungsrichtlinien, -verfahren und -kontrollen vorhanden sein, um die Übertragung von Informationen durch die Nutzung aller Arten von Kommunikationseinrichtungen zu schützen.

Dokumentation des ISO-Controls: https://www.isms.online/iso-27001/annex-a-13-communications-security/

Inhalt Blueprint

Der Blueprint hilft Ihnen dabei, die Sicherheit der Informationsübertragung mit Azure-Diensten zu gewährleisten, indem Sie zwei Azure-Richtlinien-Definitionen zuweisen, um unsichere Verbindungen zu Speicherkonten und Redis Cache zu überprüfen.

- Für Azure Redis Cache dürfen nur sichere Verbindungen aktiviert sein
- Sichere Übertragung in Speicherkonten sollte aktiviert werden

Ergänzende Massnahmen und Richtlinien

- Übertragung nur über HTTPS in App Services sollte aktiviert werden
- Übertragung nur über HTTPS in Front Door sollte aktiviert werden
- Übertragung nur über HTTPS in Application Gateway sollte aktiviert werden

Microsoft

Danke
Merci
Grazie
Engraziel