Mini Project 17: Cloud Security Part 1

Introduction:

To fully prepare for the anticipated increase in claims, virtual machines will be deployed through the cloud provider, Microsoft Azure. Withstanding pricing models from other providers, the focus will be on the security that will be deployed on the virtual machines. It is critical that there are seamless experiences for employees responding to customers and customers filling out claims. Below, is a clear layout of how role-based access control will be used to ensure the confidentiality, integrity, and availability of data. Access controls will be broken into categories and each category will be defined for clarity; controls for each category will be given; the application of these controls using Azure Cloud will be explained. Because virtual machines will be used to offset expected claims increase, Cloud Security Alliance (CSA) Cloud Controls Matrix v3.0.1 controls will be used as guidelines.

The access categories are roles, secure remote access, policies, encryption, authentication(single sign-on), monitoring and logging, and authorization(resource permissions).

Access Control Categories:

Roles:

Definition: roles are mechanisms that are used to restrict system access. “It involves setting permissions and privileges to enable access to authorized users in the claims department, and accounting department” (Imperva, 2022).

Controls Recommendations: CSA-Control Domain Identity and Access Management recommends that user access policies and procedures need to be established. These policies, procedures, processes, and measures must incorporate the following:

• Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)(Control ID IAM-02).

Azure Implementation: Azure provides roles with its Azure Role-Based Access Control. Azure RBAC is supposed by Azure Resource Management APIs and Azure portal. Azure separates each role into three categories:

- Azure roles
- Azure Active Directory (Azure AD) roles
- Classic subscription administration roles.

To limit cost and exposure, 6 AD roles will be created and used to administer other roles. One Global Administrator manages access to all administrative features in Azure AD and services that federate to Azure AD, assign administrator roles to others, and reset the password for any other user and all other administrators. Two User Administrators who will create and manage all aspects of users and groups, manage support tickets, monitor service health, and change passwords for users, helpdesk admins, and other user admins. One Billing Administrator who makes purchases, manages subscriptions, manages support tickets, and monitors service health. One Cloud App Security Administrator who manages all aspects of the Defender for Cloud Apps product. One Cloud Application Administrator who creates and manages all aspects of app registrations and enterprise apps except App Proxy. Note that many of these roles may

already exist within the company's Microsoft Active Directory. Further administrative roles may be implemented that are not persistent and are applied and removed as needed.
In terms of the employees who will be using the VMs, we will group them in the Claims Employee group. There are many specific roles available to end users but general roles will be applied. Claims supervisors will be grouped and given contributor privileges, each other user will be assigned read/write/ owner customer privileges.

Secure Remote Access:
Definition: "Secure remote access can encompass a number of methodologies such as VPN, multi-factor authentication, and endpoint protection, amongst others" (VMware, n.d.).
Controls Recommendations: CSA-Control Domain Identity and Access Management recommends business case considerations for higher levels of assurance and multi-factor authentication for remote access.
Azure Implementation: To secure remote access to virtual machines (VMs) that run in an Azure Active Directory Domain Services (Azure AD DS) managed domain, you can use Remote Desktop Services (RDS) and Network Policy Server (NPS). Azure AD DS authenticates users as they request access through the RDS environment (Microsoft, 2023). "The recommended way to securely connect to your VMs in an Azure AD DS managed domain is using Azure Bastion, a fully platform-managed PaaS service that you provision inside your virtual network" (Microsoft, 2023). However, this option is additional pricing per hour based on SKU and instances, plus data transfer rates (Microsoft, 2023). We can achieve remote access through Remote Desktop Protocol (RDP) directly over Azure portal over SSL.

Policies:
Definition: A cybersecurity policy defines and documents a formal set of rules issued by an organization ensuring that access is granted to authorized users to comply with rules and guidelines related to the security of information.
Controls Recommendations: CSA recommends the following policies to be implemented:

1. Policies and procedures shall include defined roles and responsibilities supported by regular workforce training.
2. The Retention Policy prescribes backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.
3. Handling, Labeling, and Security Policies shall be established for the labeling, handling, and security of data and objects that contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.

Azure Implementation: The Recommended policies for Azure Virtual Machines are on the Overview page for virtual machines and under the Capabilities tab. Azure Backup should be enabled for Virtual Machines ensuring the protection of all Azure Virtual Machines. Azure Backup is a secure and cost-effective data protection solution for Azure. Azure provides policies for API management, configuration, platform, and services. More important is the policy for Azure Active Directory. One such policy states that Azure Active Directory should use the private link to access Azure services. Azure Private Link lets you connect your virtual networks

to Azure services without a public IP address at the source or destination. This option comes with additional charges.

Encryption:
Definition: The cryptographic transformation of data to produce ciphertext (NIST Computer Security Resource Center, n.d.)
Controls Recommendations: CSA recommends encryption or other equivalent security techniques be used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks (Control ID DSI-03). Additionally, policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem(Control ID EKM-02).
Azure Implementation: Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware (Microsoft, 2023). Transparent Data Encryption is used to encrypt data files in real-time, using a Database Encryption Key (DEK), which is stored in the database boot record for availability during recovery. According to Microsoft, data in transit is encrypted at the data link layer using the IEEE 802.1AE MAC Security Standards. Additionally, other protections are available including but not limited to TLS encryption, SMB encryption over Azure virtual networks, In-transit encryption in VMs, RDP sessions, and Secure access to Linux VMs with SSH for the Oracle machines.

Federation/Single Sign-on (SSO):
Definition: Federation is a process that allows for the conveyance of identity and authentication information across a set of networked systems.
Controls Recommendations: CSA recommends Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)(Control ID IAM-12).
Azure Implementation: Azure AD offers Seamless single sign-on that allows users to automatically be signed into both on-premises and cloud-based applications eliminating the need for repeated password login. Deploying and administering SSO requires no additional components needed on-premises to make this work; works with any method of cloud authentication - Password Hash Synchronization or Pass-through Authentication; can be rolled out to some or all your users using Group Policy. SSO can be enabled on enterprise applications by the Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.

Logging and monitoring:
Definition: “Security event logging and monitoring is a process that organizations perform by examining electronic audit logs for indications that unauthorized security-related activities have been attempted or performed on a system or application that processes, transmits, or stores confidential information” (Control Case, n.d.).
Controls Recommendations: CSA recommends higher levels of assurance for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect

potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach(Control ID IVS-01). Additionally, each operating system shall be hardened and have in place supporting technical controls such as antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template(Control ID IVS-07).
Azure Implementation: Azure Monitor is a comprehensive monitoring solution for collecting, analyzing, and responding to telemetry from your cloud and on-premises environments. You can use Azure Monitor to maximize the availability and performance of your applications and services. Azure offers Azure Monitor Logs, a feature of Azure Monitor that collects and organizes log and performance data from monitored resources. The logs give the capability to analyze data, get alerts, visualize query results on a dashboard, get insights, and retrieve, import and export data logs (Microsoft, 2023).

Resource permissions:
Definition: Resource permissions refer to the level of access users are allowed to get in regard to company assets and data. Permission refers to authorization.
Controls Recommendations: CSA recommends that provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, the provider shall inform the customer (tenant) of this user access, especially if the customer (tenant) data is used as part of the service and/or the customer (tenant) has some shared responsibility over the implementation of control(Control ID IAM-09).
Azure Implementation: Azure uses roles as a way of granting access to resources. The steps for granting access are:

1. Identify the needed scope
2. Open the Add role assignment page
3. Select the appropriate role
4. Select who needs access
5. Adding other conditional access controls.
6. Assign role

References

Cloud Security Alliance. (2019, March 8). *Cloud Controls Matrix v3.0.1*. CSF Tools. Retrieved March 6, 2023, from https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/

Control Case. (n.d.). *Security Event Logging and Monitoring Services*. ControlCase. Retrieved March 8, 2023, from https://www.controlcase.com/services/log-monitoring/

Imperva. (2022, October 26). *What is Role-Based Access Control | RBAC vs ACL & ABAC*? Imperva. Retrieved March 5, 2023, from https://www.imperva.com/learn/data-security/role-based-access-control-rbac/

Microsoft. (2023, January 30). *Secure remote VM access in Azure AD Domain Services*. Microsoft Learn. Retrieved March 7, 2023, from https://learn.microsoft.com/en-us/azure/active-directory-domain-services/secure-remote-vm-access

Microsoft. (2023, February 3). *About Azure Bastion*. Microsoft Learn. Retrieved March 7, 2023, from https://learn.microsoft.com/en-us/azure/bastion/bastion-overview#sku

NIST Computer Security Resource Center. (n.d.). *encryption - Glossary | CSRC*. NIST Computer Security Resource Center Glossary. Retrieved March 8, 2023, from https://csrc.nist.gov/glossary/term/encryption

VMware. (n.d.). *What is Secure Remote Access? - Definition*. VMware. Retrieved March 4, 2023, from https://www.vmware.com/topics/glossary/content/secure-remote-access.html