algosec

Secure application connectivity.
Anywhere.

Azure security best practices checklist: Secure your cloud environment

This checklist provides a concise summary of actionable steps to fortify your Azure environment, based on insights from "Azure Security Best Practices":

Protecting secrets

☐ **Avoid hardcoding secrets:** Utilize environment variables or configuration management tools to store sensitive information.

☐ **Leverage Azure key vault:** Centralize and safeguard secrets, keys, and certificates with robust encryption, access control, and logging.

☐ **Implement secret scanning:** Employ tools like Azure DevOps Credential Scanner to identify and address secrets embedded in code.

☐ **Rotate secrets regularly:** Automate rotation within Key Vault and establish manual processes for others, purging unused secrets.

☐ **Distribute secrets securely:** Use secure sharing mechanisms and incorporate secret recovery into disaster recovery plans. Assign unique keys for each consumer.

Database and data security

☐ **Utilize confidential compute VMs:** Opt for AMD/Intel-based VMs with hardware-managed key encryption for data in memory.

☐ **Enable default encryption:** Take advantage of built-in encryption for Azure Storage and Azure SQL Database.

☐ **Implement privileged access workstations:** Secure sensitive tasks with dedicated workstations to minimize the attack surface.

☐ **Enforce endpoint protection:** Apply consistent security policies across devices accessing data.

☐ **Secure data transfer:** Employ SSL/TLS, HTTPS, and Azure VPN Gateway for safe data transmission.

☐ **Consider transit isolation:** Utilize VPNs or ExpressRoute for heightened security when transferring data between on-premises and Azure.

☐ **Leverage Azure confidential computing:** Protect sensitive data in the cloud with Azure's confidential computing solutions.

☐ **Safeguard email and documents:** Classify, label, and protect sensitive data with Azure Information Protection and RMS.

Identity management

☐ **Centralize identity management:** Consolidate directories with a unified Microsoft Entra ID.

☐ **Enable single sign-on (SSO):** Streamline access with SSO across applications.

☐ **Deploy role-based access control (RBAC):** Assign granular permissions based on user roles using Azure RBAC.

☐ **Regulate resource creation:** Use Azure Resource Manager to define policies for resource creation locations.

☐ **Mandate multifactor authentication (MFA)**: Enforce MFA for all users with Entra Security Defaults or Conditional Access.

Network security

- □ **Utilize Azure firewall and bastion:** Establish a secure perimeter and controlled access points for managing virtual machines.
- □ **Implement network security groups (NSGs)**: Control inbound and outbound traffic within subnets with NSGs.
- □ **Adopt the hub-spoke model:** Centralize services in the hub and isolate workloads in spokes for improved security and scalability.
- □ **Route traffic through Azure Firewall:** Enforce security policies for inter-spoke communication.
- □ **Leverage Azure Virtual Network:** Integrate and manage network components seamlessly.
- □ **Monitor network performance:** Utilize Azure Monitor and Network Watcher for continuous monitoring and diagnostics.

Operational security

- □ **Implement patch management:** Automate patching to keep software up-to-date.
- □ **Enforce compliance:** Use Azure Policy for rule enforcement and compliance management.
- □ **Organize with management groups:** Centralize governance across multiple subscriptions.
- □ **Monitor and audit:** Employ Azure Monitor for comprehensive monitoring and security event management.
- □ **Automate DevOps security:** Integrate security into your CI/CD pipeline with Azure DevOps.

Remember, security is an ongoing process. Regularly review and adapt your security measures as your Azure environment evolves. If managing security across multiple clouds becomes challenging, consider tools like AlgoSec Cloud for enhanced visibility and control.

Download this checklist and start strengthening your Azure security today!

algosec

AlgoSec.com