**ASSIGNMENT NO # 3**

**VIRTUALIZATION & CLOUD COMPUTING**

**TANZEELA SAFDER(13676)**

Q) Briefly discuss how Microsoft Azure provides security?

**MICROSOFT AZURE:**

Microsoft Azure is a cloud computing service offered by Microsoft. There are over 600 services that fall under the Azure umbrella, but broadly speaking, it is a web-based platform on which applications and services can be built, tested, managed, and deployed.

A wide range of Microsoft’s software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) products are hosted on Azure. Azure offers three core areas of functionality; Virtual Machines, cloud services, and app services

|  |  |
| --- | --- |
| Microsoft Azure – IaaS, PaaS and SaaS |  |
| ·         Flexible – Move compute resources up and down as needed |  |
| ·         Open – Supports almost any OS, language, tool, or framework |  |
| ·         Reliable – 99.95% availability SLA and 24×7 tech support |  |
| ·         Global – Data housed in geo-synchronous data centers |  |
| ·         Economical – Only pay for what you use |  |
|  |

**AZURE DATA FACTORY:**

Similar to the Common Data Service for Microsoft’s productivity tools, the Azure Data Factory is a service designed to allow developers to integrate previously siloed data sources, both on-premises and in the cloud. ADF offers access to on-premises data in SQL Server through a data management gateway, and cloud data in Azure Storage and Azure SQL Database.

**AZURE SECURITY:**

Microsoft has ensured that Azure is as secure as possible, spending more than $1bn a year on round-the-clock security monitoring.

The Security Development Lifecycle (SDL) addresses security at every development phase and ensures that Azure is continually updated to make it even more protected. Operational Security Assurance (OSA) builds on SDL knowledge and processes to supply a framework that helps provide secure operations throughout the lifecycle of cloud-based services. Azure Security Center makes Azure the only public cloud platform to offer continuous security-health monitoring.

Microsoft Azure has been integrated with Microsoft Active Directory to allow users to be authenticated once and gain access to their Azure applications as well as Office 365 and other Software as a Software (SAAS) applications. This integration is called Azure AD Connect, and it’s built on three components:

* Synchronization – This component keeps track of all users and groups on-site and ensures that they match what’s in the cloud.
* AD FS (Active Directory Federation Services) – This is an optional component that is used to address complicated authentication issues.
* Azure AD Connect Health – This component allows you to monitor all your on-site identities as well as the Synchronization and AD FS components.

Developed to be the best and most secure in the industry, Azure is trusted by major organizations like Geico, Uber, Whole Foods, and the United States Government

**STORAGE SERVICES:**

Azure Storage includes these data services:

* Azure Blobs: A massively scalable object store for text and binary data.
* Azure Files: Managed file shares for cloud or on-premises deployments.
* Azure Queues: A messaging store for reliable messaging between application components.
* Azure Tables: A NoSQL store for schemaless storage of structured data.

Each service is accessed through a storage account.

**STORAGE SERVICE TO SECURE AZURE:**

### Role-Based Access Control (RBAC):

You can secure your storage account with Role-Based Access Control (RBAC). Restricting access based on the [need to know](https://en.wikipedia.org/wiki/Need_to_know) and [least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege) security principles is imperative for organizations that want to enforce Security policies for data access. You can use [built-in RBAC roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles), such as Storage Account Contributor, to assign privileges to users.

### Shared Access Signature:

A [shared access signature (SAS)](https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1) provides delegated access to resources in your storage account. The SAS means that you can grant a client limited permissions to objects in your storage account for a specified period and with a specified set of permissions.

### Encryption in Transit:

Encryption in transit is a mechanism of protecting data when it is transmitted across networks. With Azure Storage, you can secure data using:

* [Transport-level encryption](https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations), such as HTTPS when you transfer data into or out of Azure Storage.
* [Wire encryption](https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations), such as [SMB 3.0 encryption](https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations) for [Azure File shares](https://docs.microsoft.com/en-us/azure/storage/files/storage-dotnet-how-to-use-files).
* Client-side encryption, to encrypt the data before it is transferred into storage and to decrypt the data after it is transferred out of storage.

### Encryption at rest:

For many organizations, data encryption at rest is a mandatory step towards data privacy, compliance, and data sovereignty. There are three Azure storage security features that provide encryption of data that is “at rest”:

* [Storage Service Encryption](https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption) allows you to request that the storage service automatically encrypt data when writing it to Azure Storage.
* [Client-side Encryption](https://docs.microsoft.com/en-us/azure/storage/common/storage-client-side-encryption) also provides the feature of encryption at rest.
* [Azure Disk Encryption](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview) allows you to encrypt the OS disks and data disks used by an IaaS virtual machine.

### OPERATIONS TO SERCURE AZURE:

**Security and Audit Dashboard:**

The [Security and Audit solution](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro) provides a comprehensive view into your organization’s IT security posture with [built-in search queries](https://blogs.technet.microsoft.com/msoms/2016/01/21/easy-microsoft-operations-management-suite-search-queries/) for notable issues that require your attention. The [Security and Audit](https://technet.microsoft.com/library/mt484091.aspx) dashboard is the home screen for everything related to security in Azure Monitor logs. It provides high-level insight into the Security state of your computers. It also includes the ability to view all events from the past 24 hours, 7 days, or any other custom time frame.

### Azure Resource Manager

[Azure Resource Manager](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/deployment-models) enables you to work with the resources in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. Azure Resource Manager template-based deployments help improve the security of solutions deployed in Azure because standard security control settings and can be integrated into standardized template-based deployments. This reduces the risk of security configuration errors that might take place during manual deployments.

### Application Insights:

[Application Insights](https://docs.microsoft.com/azure/application-insights/) is an extensible Application Performance Management (APM) service for web developers. With Application Insights, you can monitor your live web applications and automatically detect performance anomalies. Application Insight thus becomes a valuable security tool because it helps with the availability in the confidentiality, integrity, and availability security triad.

**APPLICATION GATEWAY TO SECURE AZURE:**

### Web Application Firewall:

Web Application Firewall is a feature of [Azure Application Gateway](https://docs.microsoft.com/en-us/azure/application-gateway/overview) that provides protection to web applications that use application gateway for standard Application Delivery Control (ADC) functions. Web application firewall does this by protecting them against most of the OWASP top 10 common web vulnerabilities.

* SQL injection protection
* Common Web Attacks Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack
* Protection against HTTP protocol violations
* Protection against HTTP protocol anomalies such as missing host user-agent and accept headers
* Prevention against bots, crawlers, and scanners
* Detection of common application misconfigurations (that is, Apache, IIS, etc.)

## NETWORKS TO SECURE AZURE:

### Network Layer Controls:

Network access control is the act of limiting connectivity to and from specific devices or subnets and represents the core of network security. The goal of network access control is to make sure that your virtual machines and services are accessible to only users and devices to which you want them accessible.

#### Network Security Groups:

A [Network Security Group (NSG)](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm) is a basic stateful packet filtering firewall and it enables you to control access based on a [5-tuple](https://www.techopedia.com/definition/28190/5-tuple). They can be used to control traffic moving between subnets within an Azure Virtual Network and traffic between an Azure Virtual Network and the Internet.

#### Route Control and Forced Tunneling:

The ability to control routing behavior on your Azure Virtual Networks is a critical network security and access control capability. For example, if you want to make sure that all traffic to and from your Azure Virtual Network goes through that virtual security appliance, you need to be able to control and customize routing behavior. You can do this by configuring User-Defined Routes in Azure.

**COMPUTE TO SECURE AZURE:**

### Hardware Security Module:

Encryption and authentication do not improve security unless the keys themselves are protected. You can simplify the management and security of your critical secrets and keys by storing them in [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/overview). Key Vault provides the option to store your keys in hardware Security modules (HSMs) certified to FIPS 140-2 Level 2 standards.

### Virtual machine backup:

[Azure Backup](https://docs.microsoft.com/en-us/azure/backup/backup-overview) is a solution that protects your application data with zero capital investment and minimal operating costs. Application errors can corrupt your data, and human errors can introduce bugs into your applications that can lead to security issues. With Azure Backup, your virtual machines running Windows and Linux are protected.

### Azure Site Recovery:

An important part of your organization's [business continuity/disaster recovery (BCDR)](https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions) strategy is figuring out how to keep corporate workloads and apps up and running when planned and unplanned outages occur.