# Describe the concepts of security, compliance, and identity (10-15%)

# Describe the capabilities of Microsoft identity and access management solutions (25-30%)

# Describe the capabilities of Microsoft Security solutions (25-30%)

# Describe the capabilities of Microsoft compliance solutions (25-30%)

**Cyber Security Concepts**

Gain illegal access to computer to cause damage or harm.

Global economic and social disruption

Cyber security – Technology,process and training – helps protect systems, nw, program and data.

Cyber security – Achieve Confidentiality, Integrity and Availability (**CIA**)

**Confidentiality** – Information visible only to the right people

**Integrity** – Information to be changed by the right people or processes

**Availability** – Information must be visible and accessible whenever needed

Threat Landscape – Email, Social Media acc, Mobile devices, Tech infra, Cloud services, People

Malware – Malicious + Software. Software used by cyber criminals to infect systems and carry out actions

Malware – Steals data. Disrupts normal usage and processes.

Malware components – Propagation (How it spreads) and Payload

**Propagated as below – 3 types**

Malware -> Virus, Worms, Trojans

Virus – Means of entry required, can cause harm once inside.

Worm – No user action required. Worm finds vulnerable systems. Spreads to other systems.

Trojan – Pretending to be genuine. Secretly performs malicious actions like stealing information.

**Payloads as below – 4 types**

Malware – Ransomware, Spyware, Backdoors, Botnet

Ransomware – Locks systems, asks ransom. Encrypts

Spyware – Spies on devices. Keyboard scans, collecting passwords and transmitting back to attacker

Backdoor – Bypass existing security measure via exploit. Hiding malicious code in software. This is backdoor

Botnet – Group of infected devices. Like crypto miners

**Mitigation Strategies – 4 types**

MFA, Browser Security , User education, Threat intelligence,

MFA – Multiple forms of identification.

Browser security – Uptodate, unauthorized extension removal,, block sites

Education – Training

Threat intelligence – Policies for security devices, user access and more.

Cryptography -

Encryption – combine large random prime numbers to create keys.

Asymmetric Encryption – public and private keys

UserA and UserB has public keys

UserA uses UserB’s public key and encrypts. UserB uses its private key to decrypt.

Types of Encryptions –

**DES** Data Encryption Standard, **Triple DES**. – one of the first symmetric encryption std.

**AES** Advanced Encryption Standard – Replaced DES

**RSA**. – One of the first asymmetric encryption standard

Hashing – Verifying data like documents and images and see if it’s tampered with.

Hashing uses algorithm known as **hashing function**.

Hashing function – Converts the original text to unique fixed length value called **hash value**

Each time the text is hashed – same value is produced. This hash will be used as unique identifier

Hashing is not encryption.

Hashing does not use keys

Hashed value cannot be decrypted back to original

Hash Function – SHA. Secure Hash Algorithm. Produces hash value of 256 bits long.

**Digital Signing – Requires digital signing service. Like Docu Sign and Adobe Sign**

Uses asymmetric key pair.

Used to prove the document is not changed

Uses private to prove the identity since no one has that private key

User A signs publicly available hash algorithm – Creates Hash

Encrypts the Hash using his private key and attaches it to the document as document signature

User A send it to User B

User B creates Hash using publicly available Hashing algorithm

Decrypts the signature using User A’s public key

If the decrypted signature matches the hash of the document, then document is not changed

Digital Certificates

Issued by CA. Verify identity subject.

Data in certificate includes – subject information, subjects public key

Certificate links user A identity with the public key.

Authentication based attacks

Brute force, dictionary, credential surfing, keylogging, social engineering (Phishing, pretexting,Baiting)

**Authorization Security Techniques** – Conditional access, Least privileged access, Lateral movement, zero trust

**Zero Trust – Never trust. Always verify**

Verify explicitly – Each request is fully authenticated and authorized. (MFA + CA)

LPA – Authorize only with minimum rights

Assume breach – Additional layers of security.

Common Network Attacks

Man in the middle – intercepting the packets

DDoS – compromise availability of services

Common Wireless attacks

Wardriving – Attacker searches for unsecuried wifi.Uses the compromised network

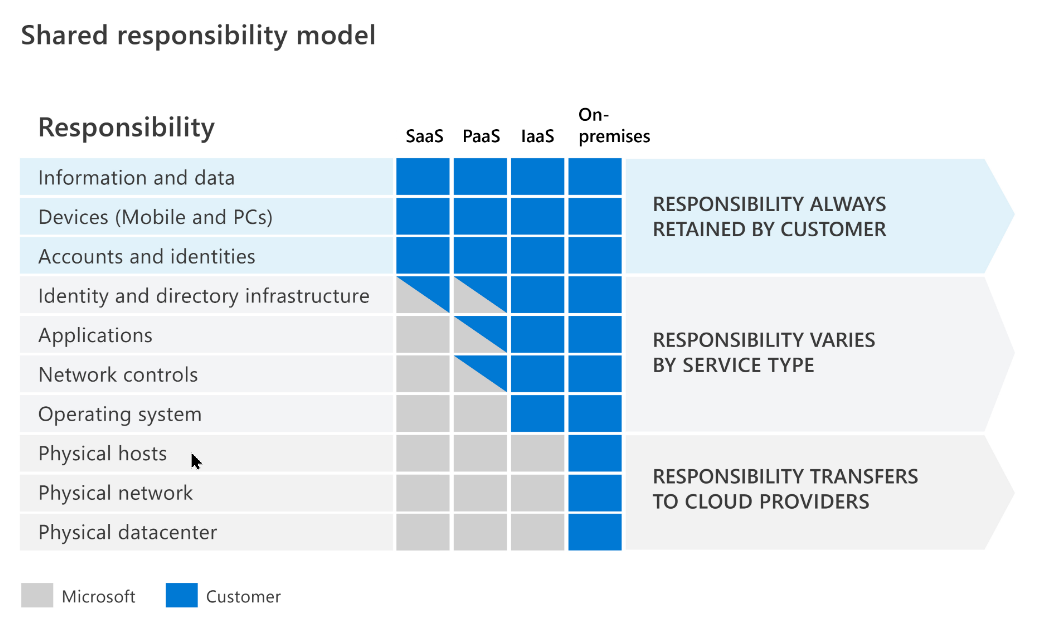
Spoofing wifi hotspots – free wifi attack

Session replay attack – stealing cookies

A zero-day vulnerability is any flaw that is previously unknown to the application owner and unpatched.

Shared Responsibility model

In cloud responsibility is shared between customer and cloud provider



SaaS – Cloud provider is responsible for everything except Data, Devices, Accounts and Identities

Responsibilities always by customer – Data, devices, Accounts and identities

**Describe Defense in Depth**

Layered approach to slow the advance of the attack.

Each layer provides protection. One layer breached the next layer will prevent

1. Physical – Limit DC access
2. Identity and access – MFA or Conditional based access
3. Perimeter – DdoS
4. Network – Network segmentation and Network ACL
5. Compute – Access to VM. Port Security
6. Application – Vulnerability management
7. Data – Encryption of data

**Zero Trust guiding principles**

Verify Explicitly

Least privilege access – Just In Time, Just Enough Access

Assume breach – NW segmentation, user, dev, apps. Encryption, analytics

**6 foundational pillars in Zero Trust – IDADIN**

* Identity – Verify with strong authentication
* Devices – Monitor for compliance
* Applications – Manage permission and access. Discover apps
* Data – Classify, label, encrypt.
* Infrastructure – Assess versions, configs and JIT access. Use telemetry to detect attacks. Block or tag risky behavior
* Networks – Segment. RTTP, End to end encryption, monitoring, and analytics

Identity has become the new security perimeter.

An identity may be associated with a user, an application, a device or something else.

Four pillars of identity

1. Administrator
2. Authentication
3. Authorization
4. Auditing

**Role of Identity Provider**

Modern authentication – Token and information is stored and managed by the identity provider.

The centralized idp is supplying the authN service

Cloud based authN provider – Azure AD. Twitter, Google, Amazon, LinkedIn and GitHub

Single Sign-On -

Federation – SSO between multiple Identity Providers

AD –

AD DS doesn’t natively support Mobile devices, SaaS apps, LOB apps that require modern authN

Federation – Trust is not always bidirectional

Azure AD DS – IdaaS Identity as a service – Solution for apps across cloud and on premise

Azure AD provides API – Allows developers to build personalized app using existing organizational data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Azure AD Free | Office 365 Apps | Azure AD P1 | Azure AD P2 | Pay as you go |
| Sync on prem  Basic reports  Self service password change for cloud users  SSO across Azure, m365 and SaaS apps | All in Free + Self service password reset for cloud users  Device Write back  AD is with 365 E1,3,5, F1 and F3 | Dynamic Groups  Self service group mgt  MS identity manager (On premise identity and access management suite)  Cloud Writeback – SSPR for on premise users | All P1  Azure AD IDP  Conditional Access to your apps and company data  PIM – help discovery, restrict and monitor administrators and their access.  Just In Time access | Azure B2C – ID and access mgt for customer facing apps |

Employees and Guests are both called Users in Azure AD

**Azure B2B** – Collaboration. External identity feature – Can add Guest User

Organization can securely share apps and services with guest users from another organization

**Azure AD Identity Types**

|  |  |  |  |
| --- | --- | --- | --- |
| User | Service Principal | Managed Identity | Device |
| Employees and guest  B2B – External Identities  B2B collaboration – securely share apps and services with guest users from other organization | Identity for an application  If application needs to delegate its Identity and access functions to azure ad.  App to register with azure AD for enabling integration  After registration SP is created in each Azure AD where app is used.  Enables authN and authZ  Developers must manage and protect SP credential | Same like SP but developers don’t need to manage it  Provides an identity for apps to use  Resources must support Azure AD authentication  No cost  Types – System assigned & User Assigned  **System Assigned** – Tied to the life cycle of the service instance.  If resource is deleted, azure automatically deletes the identity  Only Azure resource can use this identity to request tokens from azure AD  Cannot be shared  **User Assigned**  Standalone azure resource  Assigned to one or more instances of azure service.  Identity is managed separately from the resources  Can be shared | Mobile, laptop, server or printers.  **Azure AD registered devices** BYOD  No organizational account required  Win10, IOS, Android, MacOS  **Azure AD Joined**  Joined via Organizational account.  Owned by organization  Win 10 except home,  Win server 2019 VM running in azure  **Hybrid Azure AD Joined**  Need Organizational account to sign in |
|  |  |  |  |

Graphical user interface, text, application, email

Description automatically generated

To enable single sign to cloud based resources – register and join devices to Azure AD

Azure Ad Joined devices can SSO to resources and apps that rely on on prem AD

MDM and MAM – Microsoft Intune

**Types of External Identities**

External Identities - Access to organization’s apps and data to external users. Bring Their Own Identities BTOI

External IDP – Azure AD tenant, Facebook, google or Enterprise Identity Providers

Using the above, customers and partners can use their own identity to access apps

Federation is created by our Admin to the External Identity Providers

**2 types of Azure AD External Identities**

B2B - Share your apps and resources with external users

B2C - Identity Management solution for consumer and customer facing apps

|  |  |
| --- | --- |
| B2B colloboration | B2C Access Management |
| Share org apps and services with external people  We maintain our own Data control  Uses Invitation and redemtption process  Self service sign up user flow can be enabled  User who signup will be shown as guests in Azure AD  SSO to all Azure AD connected apps are supported  Guests can be added to same groups as employees |  |

SC 900 CRAM

**Defense in depth**

Data – Encryption at rest, Encryption at transit

Application protection

Compute protection

Network – Segmenting, NSG

Perimeter Protection – DdoS

Identity – MFA

Physical Security

Confidentiality – Encryption

Integrity – Not tampered with

Availability – Available to those who needs it

**Security**

Threats – **Identity thefts**

Data breach, Dictionary attacks (**Azure AD Smart Lockouts** can protect ad account)

Phishing – Email coming to users

Spearfishing - focused attack. Like email from manager

**Availability / Disruptive attacks**

Ransomware – Encrypt data

DDoS – Service attack

**Zero Trust**

Assume compromise

Trust nothing and Verify Everything

Authentication + Authorization

Least privilege – Just in Time (Get permission only when required)

Just enough administration – Just enough privilege

Assume breach – Segment everywhere in the network, Encrypt, Detect threats

**Focus on**

Identity

Device monitoring

Applications

Data classifications – Encrypt + DLP

Infrastructure protection

**Encryption Types – 2 types**

Symmetric Encryption - Uses same key

Asymmetric Encryption – Uses public and private key pairs

Integrity – Making sure no one messed with data.

Hashing does integrity

Data encrypted with private key -> Send to person with hash value

Person gets data and runs hash algorithm and decrypt the hash value with public key and sees if the hash matches

**6 Key Privacy Principles**

1. Control – putting customer in control
2. Transparent – what is collected etc..
3. Security –
4. Strong legal protection – respecting local laws, rights
5. No Content based target – no personal content advertising
6. Benefits to you – collecting data and using6.

**Trust**

Service Trust Portal – servicetrust.microsoft.com

Documents, reports, whitepapers, Audit reports, compliance manager

Compliance manager – improvements and management

STP – library to save documents

**Azure AD**

1.Azure

2.Microsoft365

|  |  |
| --- | --- |
| Azure | M365 |
| Administration  Modern Authentication  Token  Consenting  Policy  Audit  Risk  Authentication  Authorization  Audit |  |

AAD Cloud is the new name

AAD Connect – Sync, seamless

Azure AD –

Users, Groups, Guests ( B2B – different AD, MS Account, outside people)

Service Principle – application registration

Managed identity – Resource getting identity

Groups – 1. Assigned (Manually) 2. Dynamic (Query)

Group – assign licenses or roles

Devices – 1. Joined – authenticate with Azure AD

2. Registered – Personal devices (ios, wind10, macos, android)

3. Hybrid – both azure AD and On prem AD connected

Separate tenant B2C - Customers – Azure AD Business to Customers

FB, Twitter – can authenticate to Azure AD

Azure AD Pricing

M365 licenses free

Premium AD – conditional access,

P2 – PIM, id protection, JIT, etc..

No Password authentication – TPM on laptop (creates private public key), Hello 4 Business

MFA Fraud alert – not initiated 2fa request

Per User MFA and Conditional Access **(p1 or p2 license)**

CA – policies and do MFA

M365 – **Per user MFA**

SSPR – Change, reset unlock accounts

Block simple password

Authorization –

RBAC

Azure AD & M365

Conditional Access

Terms of use – make them accept

Location – Public IP, geo location

Policy

Session control – something like no save only read, login in intervals etc.

**Auditing & governance**

[P2] Azure Ad doesn’t have governance natively

[P2] Dynamic Group based on user attributes

[P2] Privileged Identity Management

[P2] Access reviews (App, role, group)

[P2] Azure AD ID protection

Root of azure is

azure AD tenant –

Root Management group –

Management Groups –

Subscription –

Resource Groups –

Resources – (Locking - Cannotdelete, Read Only) These are in management plane. Not in Data plane.

RBAC, Policy , Budgets

ARM Template – Declarative, JSON

Blue print - Deploy resources in standard way . Define RG, RBAC, Policy and ARM templates

Blue print – Collection of things, standard set of configs

Guard Rails - Policy. Only use these region, this tags, this resource

Cloud Adoption Framework – Set of documents and guidelines of Best practice.

Strategy, planning, ready, adopt, migration, innovation etc..

Network and Data and Virtual Network

VNET - > NSG – IP + Port + Protocol

Allow / deny rules

ASG – Has tag on the network interface or IP

Public IP address – DdoS – Basic and Standard (Traffic monitoring, machine learning, custom policies)

Azure firewall – Appliance in virtual network. Native HA. Filter on IP, FQDN. Outbound SNAT

Web application firewall – exploit protection

Azure Bastion – From Azure portal – connect via Bastion – RDP/SSH connection to Virtual networks

**Storage Accounts –**

Encryption at rest –

Platform Managed Key – Microsoft manages, stores/rotates

Customer Managed Key – Key vault

VM – Azure Disk Encryption

Key vault –

Certs , Secrets – data , keys to perform crypto operations (cant be retrieved)

**Azure Security Center**

Secure score, Regulatory compliance, Recommendations, Azure defender

Tells the compliance state, protection

**Azure Sentinel**

Log analytics work space.

Has connectors. Connectors to Azure AD, M365 etc

Adds machine learning to give analysis. SIEM + SOAR

**M365 – Defender**

Defender for Identity – Looks on premise for security

Defender for endpoint – anti malware. Forensic analysis. Win, android, linux, macos

Cloud app security – What application from corporation speaks to azure, byod, discovery, Conditional access and proxy control

* Data exfilteration control

Defender for Office365 –

Office 365 Defence of Depth – Identity, Device, Data

Security Center – Secure score, Reporting, incident

**Device Security** –

Intune – policy, health (Macos, windows, android,ios) , app push custom as well

MDM – Mobile device management – enrolling device

MAM – Mobile App Management – App policies

**Security baseline for windows 10 devices**

**Data – Classify and Protect**

**Ediscovery – Find and Action**

Content search

Core ediscovery – Case, search, hold, export

Advanced ediscovery - all above + process data, add custodians etc..

**Hold will take 24 hrs**

**Compliance Solutions**

**Insider risk management** – Alert + Triage – Notification. Helping detect and prevent insider actions

**Communication compliance** –

**Information Barrier** – Users shouldn’t communicate with each other via teams sharepoint and onedrives

**PAM** – Task and scope.

**Customer lockbox –** Access to data by customer support

Microsoft Defender for Endpoint -= Microsoft ATP

**Compliance.microsoft.com**

Compliance Manager – Measures opportunity to protect data and comply with standards and regulations

Classifiers – Identify, protect and govern sensitive data.

Microsoft Purview – Compliance portal

Compliance Score – Reduce risk around data protection and regulations

Defender for Endpoint – Security Platform.

Helps prevent, detect, investigate and respond to advanced threats.

**Modern authentication**

Center is Identity Provider

Supports SSO

**Azure Active Directory**

Employee, guest and others

4 types of identiies - Users, service principal, managed identity, device

Text

Description automatically generated

External Identities

B2B – Share your apps and resources with external users

B2C –

MFA – Phone, MS Auth, OAuth.

Password less – Biometrics, Microsoft Auth, FIDO2

Reset password – 1 or 2

Global banned password list

Custom banned password list

Protecting against password spray

Hybrid security

Conditional Access – AD Premium feature

Graphical user interface, application

Description automatically generated with medium confidence

**RBAC -**

Built in Roles

Custom Roles

Azure AD RBAC

Only grant the access users need

**Identity Protection and governance capabilities**

Entitlement Management –

Manage identity and access lifecycle at scale

Automates access request, workflows, access assignments, reviews and expiration

Create access packages. User can go and request that package to get access

Expiration policies can be set

**PIM – Privileged Identity Management**

Just In Time. Access only when needed and how much needed

Time bound – start and end dates

Approval based

Notifications

Auditable

Text, letter

Description automatically generated

**Azure Security**

**NSG**

Limit what type of traffic in / out vNet – **Network security group**

**NSG** Rule properties – Name, Source, Dest, Direction, Action, Priority, Protocol, Port Range

Multiple subnets / security groups association

Cannot delete default rules but can override using priority

Network interface to be associated with NSG

**Azure DDoS Protection** – Analyze network traffic and discards DDoS

Basic + Standard

Azure has built in DDoS protection – basic

Standard – extra monitoring and mitigation tools

**Azure Firewall** – Protect perimeter

Graphical user interface, text, application

Description automatically generated

Azure Bastion

Graphical user interface, text

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

**Azure Encryption – Data at Rest**

**Graphical user interface, application, website

Description automatically generated**

TDE – SQL DB and Data warehouse, backups and logs

Organizational secrets – Central place for all app secrets

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Policy – Default allow / deny – Resources based

Blueprint – policy can be included in blueprint.

**Azure management tools for security**

**CSPM**

Central security management

**Graphical user interface

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**Security center -**  shows multiple subscriptions

**Azure Defender**

Graphical user interface, application

Description automatically generated

Table

Description automatically generated

**Azure Sentinel** – Collect, Detect, Investigate and Response

**Graphical user interface

Description automatically generated with medium confidence**

SIEM – collect data, alert

SOAR – Gather alert and trigger workflow

XDR – Automated response

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated