Identity Concepts

Defining authenticataion and authorization

Authentication

The process of proving someone is who they say they are e.g. when buying something with a credit card, a username or password to use a device etc.

Authorization

Once authenticated, you'll need to decide what they can access - this pertains to permissions. What can the user do/see?

Identity as the primary security perimiter

Employees and partners need to collaborate with each other and access company resources anywhere, without productivity taking a hit. This means that the on-premises network (e.g. in the office) cannot be considered the "perimiter". It now includes:

- SaaS applications
- Personal devices employees use
- Unmanaged devices used by partners and customers
- IoT devices

The four pillars of an identity infrastructure

Administration

Administration refers to the creation/management and governance of identities for users, devices, and services.

Authentication

Tells how much an IT system knows about an identity to have proof they really are who they say they are.

Authorization

Processes the identity data to determine what level of access the person or service has within the application or service they are trying to access.

Auditing

Tracking who does what, where, and how. In-depth reporting, alerts, and governance are all part of identities.

The role of the identity provider

Modern authentication is the umberella term for authentication and authorization methods between a client (laptop, phone), and a server (website, application). Central to this is the role of an identity provider. An identity provider creates, maintains and manages identity information whilst offering authentication, authorization, and auditing services.

Single sign-on (SSO)

With SSO, the user logs in once and that credential is used to access multiple applications/resources. When SSO is set up between multiple identity providers it is called federation.

Concept of Directory Services and Active Directory

A directory is a hierarchical structure that stores information about objects on the network. A directory services stores directory data and makes it available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by MS as part of Win 2000 for on-prem domain based networks.

The b est known is Active Directory Domain Service (AD DS) which stores information about members of the domain (including devices and users), verifies credentials, and defines access rights. A server runing AD DS is a domain controller (DC)

Azure Active Directory (Azure AD) is the next evolution of this (because it can support mobile devices, SaaS apps, and LOB apps).

Concept of Federation

The simplest way to think about federation is as follows:

- Website in domain A uses the authentication services of Identity Provider A
- The user in domain B, authenticates with Identity Provider B
- Identity Provider A and B have a trust relationship configured

- When the user who wants to accss the website they are allowed to do so because it trusts the user due to the established relationship between identity providers.