100 XP

Describe defense-in-depth

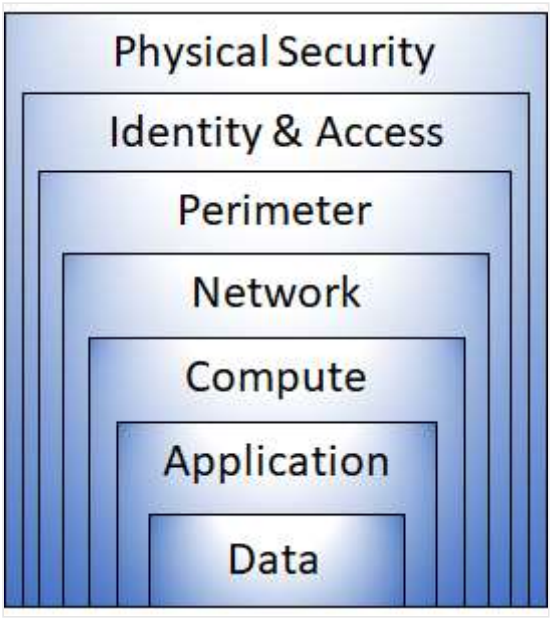
4 minutes

The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it.

A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.

Layers of defense-in-depth

You can visualize defense-in-depth as a set of layers, with the data to be secured at the center and all the other layers functioning to protect that central data layer.



Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert information that security teams can act upon, either automatically or manually.

Here's a brief overview of the role of each layer:

- The physical security layer is the first line of defense to protect computing hardware in the datacenter.

- The identity and access layer controls access to infrastructure and change control.
- The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The network layer limits communication between resources through segmentation and access controls.
- The compute layer secures access to virtual machines.
- The application layer helps ensure that applications are secure and free of security vulnerabilities.
- The data layer controls access to business and customer data that you need to protect.

These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications.

Azure provides security tools and features at every level of the defense-in-depth concept. Let's take a closer look at each layer:

Physical security

Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense.

With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately. Microsoft uses various physical security mechanisms in its cloud datacenters.

Identity and access

The identity and access layer is all about ensuring that identities are secure, that access is granted only to what's needed, and that sign-in events and changes are logged.

At this layer, it's important to:

- Control access to infrastructure and change control.
- Use single sign-on (SSO) and multifactor authentication.
- Audit events and changes.

Perimeter

The network perimeter protects from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.

At this layer, it's important to:

- Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

Network

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.

At this layer, it's important to:

- Limit communication between resources.
- Deny by default.
- Restrict inbound internet access and limit outbound access where appropriate.
- Implement secure connectivity to on-premises networks.

Compute

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.

At this layer, it's important to:

- Secure access to virtual machines.
- Implement endpoint protection on devices and keep systems patched and current.

Application

Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.

At this layer, it's important to:

- Ensure that applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.

Data

Those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

In almost all cases, attackers are after data:

- Stored in a database.
- Stored on disk inside virtual machines.
- Stored in software as a service (SaaS) applications, such as Office 365.
- Managed through cloud storage.

Next unit: Describe Microsoft Defender for Cloud

Continue >