Armaan Shamsaasef

Zero Trust

Notes: Zero Trust (SY0-701 - 1.2)

Core Concept: Zero Trust is a security model that operates on the fundamental principle of "never trust, always verify." It eliminates the concept of trust from an organization's network architecture.

- Traditional Model (Trust but Verify): Once you are inside the corporate network, you are generally trusted and have broad access.
- Zero Trust Model: No user or device is trusted by default, regardless of whether they are inside or outside the corporate network. Every access request must be authenticated, authorized, and encrypted.

Key Principles of Zero Trust

1. Assume Breach: Operate under the assumption that your network is already compromised.
2. Verify Explicitly: Authenticate and authorize every access request based on all available data points (user, device, location, application, etc.).
3. Use Least Privilege Access: Grant users and devices only the minimum access they need to perform a specific task, and for the shortest time necessary.

How Zero Trust is Implemented

A Zero Trust architecture uses a variety of technologies and strategies to enforce its principles.

1. Microsegmentation

- Definition: Dividing a network into small, isolated segments (zones) to control traffic between them.
- Example: In a data center, a web server, an application server, and a database server would each be in their own secure segment. Communication between them is strictly controlled by policy, so a breach in the web server doesn't automatically grant access to the database.

2. Role-Based Access

- Definition: Granting access based on a user's specific role within the organization.
- Example: A user in the HR department would have access to HR systems but would be explicitly blocked from accessing financial or engineering resources, even if they are on the corporate network.

3. Firewalls and VPNs

- These are used to create the secure boundaries for microsegments and to provide secure remote access, enforcing the "verify explicitly" principle.

4. Identity and Access Management

- Centralized control of user identities and enforcing strong authentication (like MFA) is critical for verifying every user.

Real-World Analogy: A Secure Office Building

- Traditional Model: Once you swipe your badge at the front door, you have access to the entire building.
- Zero Trust Model: Swiping at the front door gets you into the lobby. You then need separate authorization (like a different key or escort) to enter the R&D lab, the CFO's office, or the server room. Access is granted on a per-room basis.

Key Takeaway

Zero Trust is a strategic shift from a perimeter-based security model to a data-centric one. The goal is to protect resources by strictly enforcing access control and minimizing trust zones, thereby limiting the ability of an attacker to move laterally through a network after a breach.