ONE PAGE SUMMARY

IT & Software › Cyber Security › Zero Trust

Introduction to Zero Trust

Zero Trust: Trust No One, Verify Everything.

DEFINITION

> Zero Trust is a security model that assumes threats could be internal or external. It requires strict identity verification for every person and device trying to access resources.

KEY CONCEPTS

Least Privilege Access

Users are given the minimum level of access necessary to perform their tasks.

Micro-Segmentation

Networks are divided into smaller segments to limit access and contain potential breaches.

Continuous Monitoring

Constantly checking user activities and network traffic to detect and respond to threats.

Multi-Factor Authentication

Requires multiple forms of verification before granting access to sensitive information.

Identity Verification

Ensures that users and devices are authenticated before they can access resources.

EXAMPLES

→ A company requires employees to use a password and a fingerprint to log in.

→ An organization segments its network so that finance and HR departments cannot access each other's data.

→ A security system alerts administrators when unusual login attempts are detected.

MEMORY TIPS

★ Remember 'Never Trust, Always Verify' as the core principle of Zero Trust.

★ Think of a bank vault: only authorized personnel can enter, and they must show ID.

★ Use the acronym LMC (Least privilege, Micro-segmentation, Continuous monitoring) to recall key strategies.

COMMON MISTAKES

✗ Assuming internal users are always trustworthy.

✗ Neglecting to update access permissions regularly.

✗ Overlooking the importance of continuous monitoring.

QUICK RECAP

Zero Trust is a security approach that requires verification for every access attempt. It emphasizes least privilege access, micro-segmentation, and continuous monitoring to protect resources effectively.