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 requires strict identity verification for every user and device. It assumes that threats could be both outside and inside the network.

KEY CONCEPTS

Least Privilege Access

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

Micro-Segmentation

Dividing the network into smaller segments to contain potential breaches and limit lateral movement.

Continuous Monitoring

Constantly observing user behavior and network traffic to detect anomalies and threats.

Identity Verification

Every user and device must be authenticated before accessing resources, regardless of location.

Assume Breach

The mindset that a breach has already occurred, leading to proactive security measures.

EXAMPLES

→ A company requires multi-factor authentication for all remote access.

→ An organization segments its network to isolate sensitive data from general access.

→ Employees must verify their identity every time they access critical applications.

MEMORY TIPS

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

★ Use the acronym 'LIMCA' for Least privilege, Identity, Micro-segmentation, Continuous monitoring, Assume breach.

★ Visualize a fortress where every entry point requires a key and a password.

COMMON MISTAKES

✗ Assuming internal users are always trustworthy.

✗ Neglecting to update access permissions regularly.

✗ Failing to implement strong authentication methods.

QUICK RECAP

Zero Trust is a proactive security approach that requires verification for all users and devices. It emphasizes the principles of least privilege, continuous monitoring, and assuming breaches to enhance protection.