Armen Melkumyan • 1st
Technical / Solutions Architect
1mo • 🌐

···

Zero Trust Security: Why "Trust" is the Biggest Security Risk

For years, security has been built on the idea that everything inside the network is safe, and threats are only on the outside. But that mindset is outdated and dangerous.

Today, attackers don't just come from the outside. Phishing, credential leaks, misconfigurations, and insider threats mean that assuming trust is a liability. This is where Zero Trust Security comes in.

What is Zero Trust?

Zero Trust is exactly what it sounds like: "Never trust, always verify." No one whether they're an employee, a vendor, or even a system inside your own network gets a free pass. Every access request must be authenticated, authorized, and continuously monitored.

Why Does It Matter?

🔷 Remote Work & Cloud → Employees log in from anywhere, using personal devices. No traditional network perimeter exists.

🔷 Cyber Threats are Evolving → Hackers don't break in they log in with stolen credentials.

🔷 Compliance is Getting Stricter → Regulations like GDPR, HIPAA, and PCI DSS now require stronger security measures.

How Do You Build a Zero Trust System?

✅ Verify Every Access Request – Use Multi-Factor Authentication (MFA) and identity-based security (OAuth, SAML, OpenID).

✅ Limit Access to the Minimum Needed – Apply least privilege access for users and applications. No one should have more access than they need.

✅ Assume Breach – Monitor traffic, log all access, and use automated alerts to detect suspicious activity.

✅ Segment Everything – Prevent attackers from moving across your system by isolating workloads and restricting internal access.

#SystemDesign #ZeroTrust #CyberSecurity #DataProtection #CloudSecurity

Armen Melkumyan and 25 others 3 comments 1 repost