WELCOME TO THE GEMINI IBD® INFOGRAPHICS NEWSLETTER

[VOLUME 9] 05-31-2020

UNDERSTANDING THE ZERO TRUST FRAMEWORK

INTRODUCING THE ZERO TRUST ARCHITECTURE

The adverse effects of a cyber-attack are well known. But there's a trending phrase in the cyberspace…And it's making people contain those threats. It's The Zero Trust Architecture, abbreviated as ZTA.

According to the dictionary, Zero means the lowest possible amount or level; it means nothing at all. Similarly, the cyberspace has made good use of this "nothingness" to fight cyber-attacks.

When applied to cyber-security, it means institutions should trust no one, no app, and no technology.

"Never Trust, Always Verify" is the mantra of the Zero Trust Approach.

HOW DOES MULTI-FACTOR AUTHENTICATION HELP YOU ACHIEVE ZERO TRUST?

We've seen how Zero Trust Architecture helps limit data breaches. It can contain most errors. It uses technologies like Micro-segmentation, encryption, and MFA to enforce least privileged access.

The initial stage of MFA involves access policies. This means traits are used to identify the user. It tries to get answers to questions like:

- Who is the user?
- Is the user in a risky user group?
- Which application is the user trying to access?
- Where is the user located?
- Is the user accessing a network or an app?

A strict application of Multi-Factor Authentication requires all users to double verify. So MFA is not applied on strange logins only.

WHY ZERO TRUST IS THE LAST LINE OF DEFENSE FOR YOUR CRITICAL SERVERS

ZTA uses a technology of network segmentation to protect digital environments. Micro-segmentation is the last theoretically possible approach to protect a digital environment. This results in the prevention of lateral movements of malware. An example is a breach where one infected computer spreads over an entire network of computers in an organization. Zero Trust can prevent lateral spreads.

The facts are zero trust technology has already been in existence. But the effective use of Zero Trust relies on the following technologies:

- Micro-Segmentation
- Granular Perimeter Enforcement
- MFA
- IAM
- Orchestration
- Analytics
- Encryption
- File system Permissions
- Push Notification Authentication

WHAT IS THE NEXT STEP?

Want to get started with Zero Trust? There are several steps involved. You have to begin by moving to the cloud. It's the digital environment for a successful ZTA implementation.

You also have to integrate technology with strategic insights found by testing. Keep educating IT professionals on the Zero Trust concept. And remember to always make continual improvement. Continual improvement is the only way to counter the ever-evolving cyber threats.