AIM

AIM CYBER

High-touch services to help you navigate modern cyber threats.

WHAT IS ZERO TRUST AND WHY IS IT IMPORTANT

Zero Trust is a cybersecurity term that has been in the news more the past year or so. But what is it? And why now?

Before Zero Trust, security was implemented at the network level meaning the devices that controlled the network had responsibility for security also, such as access to applications and data.

That worked reasonably well for years. I say reasonably well because there were breaches.

What changed? Everything. BYOD or Bring Your Own Device means no longer is the company controlling the devices used on the network. Prior to BYOD, the company would provide devices to users who needed them and could control them. The advent of smart phones changed that. Everyone wanted a smart phone to monitor personal email, text friends, use social media, play games, and on and on. No one wanted to carry two devices, one personal and one business. And voila, BYOD.

Then the pandemic hit, and countless people began to work from home. Outside the company network and the network devices charged with security. The devices used at home were often personal computers with the same challenges to cybersecurity as personal smartphones.

Along with these two trends came the explosive growth of cloud services. As more applications moved off premises to the cloud, outside the company network, the traditional security model become even less useful.

Now the smartphones and home computers are used for personal and business needs. How do you secure a device that you have no control over? How do you secure devices that are outside the company network and firewalls? How do you secure applications that are in the cloud?

The answer is, yes, Zero Trust.

Zero Trust changes the cybersecurity model from residing in the network devices to residing in the applications and the end user devices. Each time a user connects they must be authenticated. That is zero trust. However, authentication doesn't have to be a burden. Zero Trust models have ways of simplifying it and making it user friendly. Zero Trust also controls access to information and applications restricting it to those with a need. This enhances security and regulatory compliance.

By moving to Zero Trust, you use a cybersecurity model that fits the new computing model.

The name is Zero Trust, but it actually increases trust in the employees and the way they work.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.