Is your cyber security stuck in the middle ages?

A False Sense Of Security

Yesterday's security technologies have not kept pace with today's evolved security challenges. Twenty years ago, organizations had centralized IT with a physical perimeter. Similar to the medieval approach of building a mote around the castle. Today, it is almost impossible to secure corporate infrastructure using technologies that have not fundamentally improved for over two decades.

Historically organizations built hardened perimeters with firewalls, VPNs and Network Access Controls (NACs) to protect their internal networks. However, these antiquated tools are complex and expensive to operate and no longer are a deterrent for cyber criminals to attack. As a company you may feel you have the best antivirus, the best firewall in place. However, you cannot account for human error. More than 99% of attacks in the past year relied on human error to gain access.

Today's IT strategies reveal a disparity between users and network resources. Your people and the cyber risk extend beyond the boundaries of the network, the footprint of risk is much broader. Applications are in globally-distributed public clouds, running on third-party managed hosting platforms, collocated in data centers, and corporate data centers. Yet users are mobile and distributed, connecting to business systems from home offices and airport lounges on personal and corporate devices. And these users aren't just your employees.

"Instead of attacking computer systems and infrastructure, threat actors focused on people, their roles within an organization, the data to which they had access, and their likelihood to 'click here' –2019 Human Factor Report

Where The Truth Lies

The reality is we live in a connected, hybrid world, where our systems and users need simple – and secure – methods of connecting and interacting with customers, partners and vendors.

With old security models in place, attackers find it much easier to exploit opportunities both internally and externally. It's been the case despite the moat and castle strategies that have failed in securing assets inside the castle. The perimeter doesn't exist. It's gone. Perimeter security must begin elsewhere.

Zero Trust Framework

Just as the name suggests, Zero Trust framework is a strategy that lives by its name of trusting nothing. It's a strategy that enforces protection even within the network on the assumption that it's already compromised. The strategy aims to identify, isolate and minimize the extent of the exploit. A system might have been hacked already, but the incident isn't determined yet. As a company, it is important to consider your environment may already be compromised.

Today, a phishing attack on a midsize business costs on average of $1.6 million

Zero Trust is going mainstream. The entire security industry is talking about Zero Trust, and numerous vendors have embraced it and now use it to market and position their capabilities as well as guide their future road maps. The time to implement the Zero Trust Framework into your organization's security plan is now.

95% of all hacking attacks and data breaches involve email

Diamond Technologies Cyber Edge is helping customers implement Zero Trust. Our cyber security experts believe you don't need an expensive platform or software package to better protect against threat, it starts with transforming your organization into a security-positive culture. ■

Jennifer Peters, Cyber Security Program Director, Diamond Technologies, Inc.