Kevane
Grant Thornton

Advisory

Businesses

Security

How zero adds value

January 18, 2021

Opportunities and challenges in adopting a Zero Trust security strategy.

As the nature of business continues to change, we must change how we secure our information assets. Many factors have driven this increased complexity, including a distributed workforce, the incorporation of contractors and vendors into internal business processes, the shift from on-premise data centers to a blend of on-premise and cloud-based data centers and software as a service, a drastic increase in external access points and the introduction of personal devices into business networks. This growing complexity has reduced visibility. Ultimately, poor visibility can lead to data breaches that expose organizations to legal and regulatory liability, as well as reputational damage.:

The Zero Trust model

The Zero Trust model emerged as a response to growing IT complexity and offers an alternative to the prevailing but outdated view of inherently trusting any system or person with access to the network while focusing security efforts on protecting the perimeter of the network.

The skepticism of the Zero Trust model takes the form of five questions. These questions are not one-time gateways; rather, they represent an ongoing attempt to ensure security.

1. Has the device attempting to connect been compromised?
2. Is the user who they claim to be?
3. Is a third party listening?
4. If a system has been compromised, how are we minimizing what it can do and see?
5. Is the environment continually monitoring for possible suspicious behavior and taking action if it is found?

Given the breadth of implementation – it will touch every process, transaction, asset, and user in an organization – it's important to start with some strategic questions.

Focus on 3 key areas

Once an organization determines its strategy, prioritizing the assets it wants to protect and the threats it faces, it should look to adapt its cybersecurity capabilities in these three areas:

Identity and access management

This entails rigorous initial verification of users upon setup, the application of the "least privileged" principle to limit a user's rights to the data that is absolutely necessary to do their jobs, ongoing adaptive and risk-aware authentication, timely deprovisioning as users' roles change, the scouring of obsolete access credentials and finally continual monitoring that feeds intelligence into risk-aware components.

Network security

Encryption, while not new, is invaluable and is increasingly low impact. Next-generation firewalls can account for applications, users and content to intelligently restrict the movement of users within the network. Along with appropriate firewall usage, micro-segmentation is another important tool to help control network traffic flow.

Data protection

Protecting an organization's sensitive data is a primary goal of any cybersecurity program. This starts with identifying the sensitive data itself. Once the data is identified, it should be encrypted when it is not in use or in transit, and tokenized when it moves to less-secure environments.

Implementation and cultural change

Zero Trust strategies work. But how do organizations make them work? First, they must understand the enterprise-wide nature of the implementation and the expanding sense of what an enterprise is. A Zero Trust model can be viewed as burdensome and unnecessary by some, so it is important to gain consensus on the dangers currently faced and reassure people that any impact on their day-to-day jobs will be minimized where possible while being focused on better securing the organization's IT assets.

The evolution to a Zero Trust model is a journey that will take many steps for most organizations. It should start with having a clear picture of the users and devices accessing an organization's IT resources and the underlying infrastructure that an organization's systems and data reside on. Once there is a good understanding of who needs to access systems and where those systems are located, an organization can assess where its highest risks are and prioritize the implementation of cyber capabilities that can address those risks.

It should be clear why Zero Trust matters. In addition to protecting against data breaches, it promises much greater visibility and adaptability.

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.

Marta Rodríguez
Advisory Senior Manager
E marta.rodriguez@pr.gt.com

Aixa González
Advisory Senior Manager
E aixa.gonzalez@pr.gt.com

Neysha Otero
Advisory Manager
E neysha.otero@pr.gt.com

grantthornton.pr

DISCLAIMER: This update and its content do not constitute advice. Clients should not act solely on the basis of the material contained in this publication. It is intended for information purposes only and should not be regarded as specific advice. In addition, advice from proper consultant should be obtained prior to taking action on any issue dealt with this update.