Zero Trust Security

With cyberattacks evolving in frequency and sophistication, organizations like yours need a cybersecurity approach that can keep these threats at bay. Adopting a **zero-trust cybersecurity** model — which is grounded in the idea that no device or user in your network should automatically be trusted without verification — can help address the cyberthreats and security challenges facing your business today.

Steps to adopting Zero Trust Security[1]

STEP 1: Identify all users and non-person entities on the network

• Identify all your subjects and users. It could be humans and machines with access to your systems and networks.

• Pay special attention to users with special privileges.

• Apply logs and audit actions to verify and authenticate privileged access while monitoring access behavior patterns.

STEP 2: Identify your assets

• Identify and manage all the assets and devices that are directly or indirectly part of your organization.

• The assets could include laptops, phones, Internet of Things (IoT) devices and digital artifacts, such as user accounts and applications.

• Additionally, monitor and configure changes to effectively evaluate access requests.

STEP 3: Identify key processes and evaluate risks associated with execution

• Identify and rank your business processes and data flow.

• Your business processes should clearly define how access requests are granted or denied.

• Consider starting with a low-risk business process as your zero trust candidate to avoid any negative impact on your organization due to disruptions.

STEP 4: Formulate zero trust policies

• Identify and evaluate the risk associated with all your business processes and data flow.

• Improve security as part of zero trust integration.

• Establish a process to limit or restrict access during after-office hours or on weekends.

STEP 5: Identify candidate solutions

• Identify and evaluate a zero trust solution that best fits your business workflows and ecosystem.

• Check for components that could limit or restrict the use of personal devices at work or cross-agency collaborations.

• Determine if the solution works for your business process that exists entirely on-prem or in the cloud.

• Ensure the solution supports a wide range of use cases, such as web or email.

• Consider modeling an existing business process as a pilot program to test the zero trust architecture.

STEP 6: Initial deployment and monitoring

• After selecting a solution, consider initially running your new zero trust approach in reporting mode to ensure your policies are effective.

• Continue to monitor and adjust the nework and assets.

• As you gain confidence in the process, you can start planning the next phase of zero trust deployment.

1 - NIST Special Publication 800-207

Like any large-scale strategic change, a zero trust implementation can be intimidating.

To simplify the process, consider partnering with an IT service provider like us to develop an effective and practical zero trust strategy.

Contact us to secure your business's future through **ZERO TRUST NOW.**

ACCi we've got it covered

www.acci.com

205-987-8711