Zero Trust Concept – M365 E5

Zero trust is a modern security approach to protect and secure employee and customer data by verifying access requests throughout the network infrastructure. It can be seen as a very explicit way to defend organization resources. Today, it is commonly used because of remote work. Organizations have addressed remote work by creating new security standards, however it could be difficult to manage end to end encryption, VPN configuration, and creating a seamless experience for remote workers to access applications and resources remotely. Instead, by using the Zero trust security model in Microsoft 365, administrators can ensure that devices, users, files and applications can be accessed from any location. The purpose of Zero trust is to check these requests. If configured properly, zero trust will use all available data points, and all compliance and security policies put in place to ensure that an actual employee is trying to access the organization's resources instead of a threat actor. Zero trust is also commonly mistaken as an easy way to protect organization information. However, zero trust relies on the security tools provided in M365. Some of the key security components in the zero trust security strategy / model within M365 include checking Identity (Ensuring the right user is accessing organization resources. Endpoints (This provides insight into the end user device, whether it's a threat actor, a jailbroken phone, a phone with sideloaded applications, or a regular employee trying to access organization resources.) [1.] Application protection policies, compliance policies, device profile policies can all monitor and determine whether users have permissions to access certain applications. These users can be monitored, and further configuration can be made to limit or expand the amount of resources or applications the user has over the organization's network. Another way zero trust defends the organization is by using data labels. Data labels are intended to classify different types of data based on their sensitivity. This is also a valuable tool to ensure that data is encrypted and not accessed by anyone other than those with permissions. Building a zero trust network infrastructure is evidently a significant security strategy for organizations that use cloud based networks like M365. From sharing resources, accessing applications, sending emails or having sensitive data at bay. [3.] Committing to a zero trust strategy for the network infrastructure will prevent malicious attacks, detect anomalies, and will use every resource possible to identify malicious sign ins.

References

[1]

BrendaCarter, “Zero Trust deployment plan with Microsoft 365,” *Microsoft.com*, Apr. 09, 2024. https://learn.microsoft.com/en-us/microsoft-365/security/microsoft-365-zero-trust?view=o365-worldwide#step-5-protect-and-govern-sensitive-data (accessed Jun. 15, 2024).

[2]
chrisda, “Zero Trust identity and device access configurations - Microsoft 365 for enterprise,” *Microsoft.com*, May 14, 2024. https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-identity-device-access-policies-overview?view=o365-worldwide (accessed Jun. 15, 2024).

[3]
cabailey, “Secure data with Zero Trust,” *Microsoft.com*, Apr. 30, 2024. https://learn.microsoft.com/en-us/security/zero-trust/deploy/data (accessed Jun. 15, 2024).