Microsoft 365 Infrastructure Security Best Practices Businesses Operating in the Cloud Should Adopt

Most organizations conduct business in the cloud, tapping into critical benefits such as scalability and accessibility. The rapid move to remote work in 2020 sent organizations scrambling. But now, with the dust settling, they are taking stock of security issues and adjusting strategy accordingly. These Microsoft 365 infrastructure security best practices will help.

Cloud Environment Brings Unique Security Concerns

According to the 2021 State of Cloud Security Report by IDC, 79 percent of businesses reported suffering a cloud data breach in the previous 18 months. While cloud providers list security as one of the key benefits of cloud computing, the true picture involves more complexity.

In the first place, the tidy security perimeter of the traditional on-premises network has disappeared. Every user, every device that connects to cloud data presents a possible doorway for hackers, greatly enlarging the attack surface. If an attacker can compromise a single account from an employee, a vendor or even the IoT, they can potentially access sensitive data.

Secondly, many companies use multiple clouds or a mix of on-premises and cloud networks. Securing a complex hybrid cloud environment necessitates implementing a robust and multifaceted cyber security strategy. This means hiring or partnering with cloud security professionals and carefully implementing tools designed for the hybrid realm.

Thirdly, operating in the cloud means joining forces with cloud providers and understanding the shared responsibility model. Too often, businesses simply send data into the cloud with the assumption that the cloud provider will handle all security. In reality, provider and customer both have security responsibilities.

Finally, remote work and the cloud have significantly increased the use of shadow IT. Any time employees use cloud services and applications not sanctioned by IT, they unwittingly create security gaps. They also increase the risk of data loss and non-compliance.

How Microsoft Protects Your Data

As one of the most popular cloud providers in the world, Microsoft takes its security responsibilities seriously. To protect your Microsoft 365 data, Microsoft implements several key security principles. To begin with, Microsoft engineers have no access to customer data unless the customer specifically requests and approves such access.

Then, when granting access to resources, Microsoft follows the principle of least privilege. That is, the system assumes that any user or service presents a possible threat. Thus, personnel who develop and maintain Microsoft services are granted the minimum amount of resource access necessary to complete the task at hand.

Microsoft isolates resources into segments with clear boundaries. Thus, if a hacker were to compromise one segment, they should not be able to move laterally into another part of the system. To further protect data, Microsoft uses up-to-date encryption protocols to encrypt data both in transit and at rest.

Additionally, Microsoft employs automated security monitoring to detect and even remediate threats. Automated assessments continually search for misconfigured or unpatched services. And security experts constantly conduct simulated attacks and penetration testing to identify vulnerabilities.

Microsoft 365 Infrastructure Security Best Practices to Implement

In addition to providing assurance to their customers, Microsoft security practices offer an example of security habits to adopt. Some of these best practices include the following:

- **Access management** – Even when the cloud provider protects the infrastructure, customer organizations must still secure user accounts and control data access. Consider following the least privilege principle, granting users and services the minimum amount of access they need. Make sure to remove user accounts and access when not needed.
- **Endpoint security** – Implement an endpoint detection and response (EDR) solution such as Microsoft Defender for Endpoint. An EDR will automatically inventory each endpoint, as well as the processes and applications running on the device. By analyzing data from each endpoint, the EDR can quickly respond to potential security threats.
- **Encryption** – Microsoft employs standard encryption for data in their data centers or en route from a user device to the data center. However, additional encryption for highly sensitive data, as well as data shared outside the organization, may prove necessary. Organizations need to take the time to configure encryption controls and policies.
- **Automation** – Automated threat detection and system monitoring are essential to effective security. For instance, security incident and event monitoring (SIEM) automates the process of collecting and analyzing log and event data. This allows companies to detect and respond to threats much earlier.

To improve your cloud infrastructure security posture, consider partnering with a managed services provider such as eMazzanti. With deep expertise in cyber security, as well as Microsoft and other cloud services, our consultants will help your organization implement a cloud security strategy designed to meet your business environment.