What is Microsoft's Role in the Shared Responsibility Model for Data Security?

Migrating to the cloud delivers undeniable business benefits. But it also opens the door to new cyber security risks, and unprepared cloud users may encounter nasty surprises. Understanding Microsoft's role in the shared responsibility model is a critical first step toward safely navigating the cloud.

All too often, organizations shift data and workloads to the cloud, naively assuming the cloud provider will manage all cyber security. They learn lessons the hard way when a hacker accesses sensitive data or a user unwittingly deletes important information.

Think of the cloud as a gated community. A cloud provider such as Microsoft secures the perimeter, in this case the physical infrastructure, the platform, and the applications. But you must secure your own house, including the data and workloads that live in the cloud. The cloud provider offers useful tools, but those tools require proper configuration and implementation.

Cyber Danger in the Clouds

The cloud can be a dangerous place to work, as any system that touches the internet becomes vulnerable to attack. Consider the treasure trove of data moving to and from the cloud in the form of emails or stored documents. Think of all the cloud-based applications that keep businesses humming, from Microsoft Teams to CRM and inventory systems.

Every device that connects to cloud data and applications, from laptops to mobile phones, presents a possible doorway for attackers. If a hacker can compromise just one device or one account, they can gain access to the wider system.

Additionally, the cloud makes it possible for a significant percentage of workers to work remotely at least occasionally. And remote work greatly increases the use of shadow IT. When employees use any applications or cloud services not sanctioned by IT, they unintentionally create security gaps. This increases the risk of data loss and compliance issues.

When organizations work in collaboration with Microsoft and other cloud providers to secure data and systems, they reduce the risks involved.

Securing the Foundation: Microsoft's Role in the Shared Responsibility Model

Microsoft invests heavily in securing its global infrastructure. This includes physical security of data centers and robust security around the hardware and networking equipment that supports Microsoft 365 services. Microsoft also provides some encryption, and it employs continuous monitoring of the underlying platform to detect and remediate threats.

Further, Microsoft uses the principle of least privilege when granting system access to its personnel. That means that Microsoft engineers are granted the minimum access necessary to complete their tasks. They also have no access to customer data unless the customer specifically requests that access.

Another important aspect of Microsoft security involves securing Microsoft 365 applications. As any emerging threats come to light, Microsoft prepares and releases security updates and patches.

Your Data, Your Responsibility

While Microsoft security measures play an important role, these measures alone will not protect your data. For instance, Microsoft 365 applications include sophisticated security options, but those controls require proper configuration. And security patches offer no value if users neglect to install the updates.

The security responsibilities of the customer fall into the following areas:

- Data protection and management – This includes properly categorizing data, setting retention policies, and ensuring additional encryption for highly sensitive data. It also involves defining and enforcing security policies and ensuring regular backups.
- Identity and access management – The organization retains responsibility for securing user accounts and controlling data access. Security experts recommend a zero-trust approach that requires the system to verify every user, device, or workload attempting to access the network.
- Endpoint protection – Every mobile device, laptop, or point-of-sale device that connects to the network creates a possible doorway for hackers. An endpoint detection and response (EDR) solution will automatically inventory and monitor each endpoint. By analyzing data from these devices, the EDR can respond quickly to threats.
- Regulatory compliance – The organization must stay on top of legislation and industry-specific regulations governing data security.

Forging a Powerful Partnership

The beauty of shared responsibility lies in its collaborative nature. Microsoft takes care of the heavy lifting on the infrastructure side, allowing you to focus on securing your data and workloads. To help companies fulfill their side of the arrangement, Microsoft provides robust tools designed to enhance security and compliance.

Working with the data security experts at eMazzanti, organizations gain access to critical expertise and additional tools that enable them to effectively secure vital data assets.