PROFESSIONAL LABS: SECURITY

When it comes to the cloud, it's essential to protect your cloud data in whatever form it takes, and wherever it resides. This means protecting it in two states: at rest, and in transit.

- **At rest** includes all containers, storage objects, and data types that are static and exist on physical media.
- **In transit** data is data that is being transferred between programs, components, or locations. This includes transfer across a service bus, over the network, or during the input/output process.

The following are four best practices for managing your data securely in the Azure cloud:

SECURE DATA AT REST

You MUST encrypt data at rest – this is a requirement for maintaining compliance, data privacy, and security.

If you don't encrypt your data at rest, you end up exposed to data-integrity issues. This includes unauthorized agents gaining access to Clear Format-coded data, or stealing data in compromised accounts. Additionally, companies are obligated to demonstrate they are securing their data in order to meet regulatory compliance standards (i.e. HIPAA, PCI).

The best way to accomplish this is by using Azure Disk Encryption, which lets you encrypt both Windows and Linux IaaS VM disks. Disk Encryption combines the industry-standard BitLocker with Linux dm-crypt to provide volume for both OS and data disks. It's important to remember to encrypt drives before writing sensitive data to them, not after.

SECURE DATA IN TRANSIT

Given the nature of the cloud, protecting data in transit is critical to any cybersecurity strategy. Failing to protect data in transit can result in session hijacking, man-in-the-middle attacks, and eavesdropping, all of which represent the first step in attackers gaining access to confidential data.

For securing sensitive data, it usually makes sense to isolate your entire communication channel using a VPN. This can be done with a site-to-site VPN when you want to secure access from multiple workstations to an Azure VM, or with a point-to-site VPN when securing access between an individual workstation and Azure.

For migrating larger datasets over a high-speed WAN link, Azure ExpressRoute can be used alongside SSL/TSL at the application level.

SECURE YOUR WORKSTATIONS

As discussed last week, people form the new data security perimeter. Once an attacker breaches an endpoint, they can steal credentials and gain access to sensitive corporate data. Usually, hackers take advantage of a user's administrator privileges.

For this reason, it's important to ensure you manage with secure workstations. Any subscription administrator or owner should use a secure access or privileged access workstation (PAW), which will ensure safer data and guard against attacks.

SECURE DATA SHARED OUTSIDE YOUR COMPANY

When it comes to data security, you need to consider information such as emails, documents, and sensitive data being shared outside your organization. The best way to do this is by leveraging Azure Information Protection, a cloud-based system for labelling, classifying and protecting emails and documents. Once setup, Azure Information Protection can be given a set of defined rules and conditions and will begin to work automatically.

With Azure Information Protection, classification is always easily identifiable. Labels are included as visual markings in the header or footer, and as a watermark where appropriate. Metadata is made clear in files and email headers to ensure that both your internal team and external solutions such as backup and data loss prevention can act based on data classification.

Information Protection is best paired with Azure Rights Management (Azure RMS). RMS integrates with the entire suite of Microsoft tools, from Office 365 to Azure AD, and protects data using encryption, identify and authorization policies. RMS protects your data independent of where it's located, making it the ideal solution for emails, shared documents and data in-transit.

To best keep your shared data secure, we recommend the following:

1. Deploy Azure Information Protection for your organization.
2. Apply labels that reflect your business requirements, i.e. use a tag named "highly confidential" on all documents and emails that contain top-secret data, to classify and protect your data.

3. Configure usage logging for RMS so that you can monitor how your organization is using the protection service.

Have more questions about security in the cloud? Contact http://prolabs.co.in/contact