bsi.

Inspiring trust for a more resilient world.

Security considerations of moving to Office 365

Areas to examine to mitigate the migration risks

Introduction

As the momentum of data movement from on-premises to cloud continues to build, it is imperative for system administrators, managers and data owners to ensure that they adapt a strong security aligned approach to this migration process and recognize the subtle but significant differences between the two environments.

An O365 migration presents data owners with an ideal opportunity to clear down their on-premises data stores where possible, ensuring compliance with existing archive or data deletion policies that will result in a reduced data volume size and corresponding data transit time.

In this paper, we examine a number of areas that data owners should consider when planning an O365 migration.

Elements to consider

Geographical

Geographical considerations can play a part both in the method for data transit and the physical residency of the data.

From a privacy perspective, it is recommended that data owners adapt a Privacy by Design (PbD) mind-set especially in light of the upcoming EU General Data Protection Regulations (GDPR) which mandates this requirement in Article 25 of the regulation. Irrespective of the British exit from the EU and the corresponding impact on British companies and their O365 data, the timing of the Article 50 exit means that they remain subject to EU law until Friday the 29th March 2019 well after the GDPR enforcement date of 25th May 2018.

Data Loss Prevention (DLP)

In today's challenging world of cyber security and the seemingly endless daily newsfeed of security breaches and data losses, data owners need to consider the "not if, but when we are breached" approach and adapt their policies, procedures and technology accordingly.

In order to minimize both the risk of a security breach occurring and the corresponding fall out, such as reputational damage, regulatory fines and financial losses via stock movements there are a number of functional components that should be utilized.

Data Loss Prevention (DLP) is available both natively in O365 and also by a number of cloud based vendors. By defining specific data types and configuring policies, rules and actions combined with reporting, the potential for accidental or deliberate disclosure of information can be minimized.

eDiscovery

There are many use cases today that require companies to have eDiscovery functionality and these include regulatory investigations, criminal fraud investigations, commercial disputes and now with GDPR being implemented, the right to be forgotten (Article 17).

O365 has this functionality available via the Security and Compliance Center. Included in this feature set is the ability

to preserve information via case management holds, thus preventing data loss.

For those companies who find themselves in a position of extensive legal engagement, the advanced eDiscovery engine provides machine learning, predictive coding, data de-duplication, re-constructing email threads and text analytics.

Data governance

From a governance perspective, data owners will need to ensure that irrespective of the location of their data, that the appropriate controls are in place to meet any industry requirements they may need to adhere to, such as PCI-DSS or ISO27001. Within the Security and Compliance Center, Microsoft's data governance functionality allows you to control the data lifecycle of your files and email via classifications, policies and actions. Audit trails are also essential where you have a need to have visibility in user behaviour, perhaps in specific sensitive business functions. Microsoft offers the unified audit log which enables system owners to review user or admin activity across a range of the O365 offerings. This feature is not enabled by default and can be enabled by clicking the Start recording user and admin activity on the Audit log search page in the Security and Compliance Center. For Exchange online, mailbox audit logging can be enabled by using PowerShell commands after connecting to your Exchange Online organization.

Alternatively, you can enable mailbox auditing for all mailboxes in your organization.

Service uptime and incident management

Another governance aspect to consider when moving to O365 is the obligations on behalf of the Cloud Service Provider (CSP). In Microsoft's case they provide three bands of service credits where uptime is (a) less than 99.9% (25%), (b) less than 99% (50%) and (c) less than 95% (100%). On the face of it these credits look reasonable from a business uptime perspective but we must analyse the appropriate time involved. Point (a) or 'three nines' equates to allowable downtime of 8.76 hours per year or 43.8 minutes per month. Point (b) or 'two nine's' equates to allowable downtime of 3.65 days or 7.2 hours per month whilst Point (c) or 'one and a half nines' equates to allowable downtime of 18.25 days per year or 36 hours per month. Obviously options b & c are not to be considered for those companies that require uptime and stability and one might argue that on-premises availability numbers are lower than option a.

One of the key elements to incident management is communications and stakeholder management. There is a human element to this discussion and users do take comfort when an IT department issue a communication that a service is currently down and they are working to resolve it. It is however another matter when the communication for the same issue but for a corresponding cloud based service is that a call has been logged with the CSP and are awaiting feedback. Microsoft have exceeded these SLA's and in 2016 averaged 99.98% uptime equating to 105 minutes downtime in the year. The problem data owners need to address is there is no control when those 105 minutes occur. To treat this risk, organizations should consider transferring this risk via the use of cyber insurance. There are currently nearly 100 companies operating in the cyber insurance space and the use of service outage contracts and provider data loss policies are widespread.

Malware

Recently threats that were prevalent but reasonably manageable such as phishing and ransomware have become more advanced and persistent. The move from on-premises to O365 does provide users with additional functionality such as the Threat management dashboard which has features such as URL detonation which examines suspicious links and dynamic delivery which provide malware scanning on email attachments. These built in functions should be combined with 3rd party vendor solutions to provide defence in depth capabilities for your organization. Similarly no one can dispute the numbers of users or volume of data residing within O365 and this gives Microsoft great leverage which they use in the form of their Security Intelligence reports and dashboard to provide users with deep analysis and metrics of threats, their origination, their targets within your organization and the actions that were taken to nullify them.

Identity and Access Management (IAM)

Identity management is a key stepping stone to securing the end user element and Microsoft do provide two-factor authentication. In line with best practices it is preferable to separate security capabilities when possible and thus the use of a 3rd party multi-factor authentication should be under consideration when designing the security model for your O365 environment.

Encryption

The ability to encrypt O365 email data is important and email message encryption can be applied or removed within the Exchange admin center. Microsoft supports the use of Transport Layer Security (TLS) v.1.0, 1.1 & 1.2 security certificates to encrypt connections between computers. All customer-facing servers negotiate a secure session by using TLS\SSL for data in transit purposes. For messaging data at rest Microsoft employs BitLocker with AES 256-bit encryption. Where the business requires it the ability to encrypt at file level is available and combined with the distribution of files across multiple Azure storage containers with separate credentials provides another layer of protection.

The security strengths of Office 365

Security monitoring

An aspect that many businesses' query is who watches the watchers? Where data has been uploaded to a cloud provider such as Microsoft, who monitors what Microsoft themselves are doing?

The vast majority of operational actions are completed using automated service tools and Microsoft minimize human interaction with client data. In the rare case such as a troubleshooting ticket that an engineer does need to access data, Microsoft has the Customer Lockbox for O365. This capability give user's explicit control over how their data is handled in this event via multi-level access control approvals. The access is granted on a just in time (JIT) basis and a full audit trail via the Office 365 management activity log is available.

This capability is available to users through the Office 365 access center by placing data access requests through the service overview dashboard.

Business continuity and disaster recovery

Business continuity and disaster recovery are areas where Microsoft's O365 offering is particularly strong. End to end resilience is built into all aspects of the platform from power through disks, networking and site to site replication between geographically dispersed data centers. Nevertheless scenarios should be tested thoroughly and regularly. One area that data owners do have to consider is backups. It needs to be made clear that high levels of resilience do not equate to backups. Offline synchronization, location redundancy, previous versions and time based recycle bins do not assist the recovery of data as required either by the business or external parties. If regulatory authorities or courts request lookups of data related to a legacy legal or commercial matter, companies may struggle to obtain the required data. To bridge this technical gap there are a multitude of 3rd party backup vendors that advocate cloud to cloud or cloud to on-premises backups and data owners need to ascertain if point in time data restoration is a business requirement for their organizations.

Conclusion

In summary, there are several security and governance considerations that data owners need to evaluate as part of any data migration to O365 strategy. Aligning to the business requirements and having the ability to respond to future business requirements is key.

Migration to the cloud does solve a number of challenges specifically in the infrastructure and finance spaces but does not solve all challenges and indeed can introduce a number of new ones. Data owners are advised to recognize this, maximize the security functionality both natively within O365 and with appropriate 3rd party functionality that works to extend Microsoft's capabilities or bridge gaps where they exist. Finally to conduct appropriate security awareness and O365 functionality training for their users which cumulatively will have the effect of reducing risk to their O365 migration.

Digital trust services

Our Digital trust services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Digital Trust strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more

Call UK: +44 345 222 1711

Call IE: +353 1 210 1711

Visit: bsigroup.com/digital-trust