Interested in learning more about security?

SANS Institute InfoSec Reading Room

Migration to Office 365, a Case Study on Security and Administration in the Non-profit Sector

A non-profit serves a mixed community of staff and volunteers. Its email archiving and spam filter services were going to reach the end of life in January 2017. Generous charity pricing for Office 365 from Microsoft was an incentive to move away from the existing hosted Exchange platform. The company needed to develop a strategy for migration to Microsoft Office 365. It had to upgrade Microsoft Office software as well as migrate email. How could it accomplish the transition as well as maintain or improve security?

Migration to Office 365, a Case Study on Security and Administration in the Non-profit Sector

GIAC (GCWN) Gold Certification

Author: Richard Snow, rich@bnc-consulting.com
Advisor: Christopher Walker, CISSP, GSEC, GCED, GCWN, GCUX, GWEB, C|CISO
Accepted: February 26, 2017

Abstract

A non-profit serves a mixed community of staff and volunteers. Its email archiving and spam filter services were going to reach the end of life in January 2017. Generous charity pricing for Office 365 from Microsoft was an incentive to move away from the existing hosted Exchange platform. The company needed to develop a strategy for migration to Microsoft Office 365. It had to upgrade Microsoft Office software as well as migrate email. How could it accomplish the transition as well as maintain or improve security?

Information was gathered from sources including Microsoft, the non-profit community, and a trusted VAR. All concerns were diagrammed in a team meeting and tied to specific technology and actors. The migration was completed in September 2016. Security was strengthened by implementing a uniform password policy and directory synchronization. The company reduced costs and unified the administration of mobile and local users through the project, but it also increased complexity and required new administrative procedures. As a result of the successful upgrade, the company is now well positioned to take advantage of future opportunities to securely host applications on the Microsoft Azure cloud.

1. Introduction

Non-profit companies come in all shapes and sizes (Salamon, 1999). The company is a mid-sized non-profit with a mixed user base and a large outdoor campus. Many computer users are barely computer literate, but there are office workers and some sophisticated CAD, Finance and GIS applications in use. There has been a big increase in Mobile access for staff working on the grounds. The company's line of business applications rely on Microsoft Office, and it has been using hosted Exchange at MindShift.com. To maintain the best security and operability posture, it will need to upgrade from the Office 2007 suite and redesign its Exchange infrastructure.

2. Business Concerns Driving the Upgrade

2.1. Platform

The company used Microsoft Windows 7 SP1 with Office Professional Plus (Windows 7 Technical Library Roadmap, 2009; Shinder, 2007) against a hosted Exchange provider and a hosted SPAM filter and archive. Microsoft Access is required to service line of business applications. Extended support for Office 2007 ends in 2017 (Search product lifecycle, 2017) and version upgrades are made every 5 years to reduce file incompatibilities.

2.2. Upgrade Incentive

Microsoft offers an exceptional non-profit discount on Microsoft Office 365 (Office 365 Nonprofit plans and pricing, n.d.). The company pays more per user for a hosted Exchange subscription than the non-profit cost for Office 365 E3. Could they leverage the upgrade incentive while maintaining robust security protections?

Richard L. Snow, rich@bnc-consulting.com

2.3. Upgrade Deadline

The company was using McAfee SaaS to filter and archive email. McAfee was acquired and the product line was to be closed out in January 2017. The company wanted to migrate its email archive and find a new filtering service. Microsoft offers an archiving service and a SPAM filter that was considered among the options.

Microsoft Office 365 comes in all the colors of the rainbow. The company had to choose the appropriate licensing for Office and whether to use Microsoft's filtering (Office 365 - Advanced Email Threat Protection, n.d.) and archiving service (Microsoft Exchange Email Archiving Solutions, n.d.), or use a third party for filtering and archiving.

It also had to decide where to deploy subscription-based licensing and where to install stand-alone software packages. As the staff have email accounts, they would be subscribers; volunteers would use shared computers with standard software licensing.

3. Cyber security concerns in meeting the business requirement

Office 2016 uses a new deployment packaging method called "Click-to-Run". The frequency of software updates is controlled when configuring a local deployment repository, or in the portal when deploying from the web. At the time of the project, there was no Office package customization tool, but enterprise management of the software was available through Group Policy and Administrative Templates. For security purposes, the Office applications do not allow full functionality for files loaded from the network or for older file types. These security settings are found the Trust Center for each application and may be set through a GPO.

In a 2003 project at the company, Microsoft Exchange 5.5 was found to have very limited spam filtering. At that time, there were few after-market products for a small business. In 2016 there was a bewildering array of options to sanitize the flow of email. In that time terminology has changed, but the demarcation points are the same: Cloud or

Premise server solutions, and Endpoint filtering solutions - often the only line of defense for consumers and small businesses.

One of the key tenets of the SANS GIAC training is a "Defense in Depth" (McGuinness, 2001) approach, sometimes referred to as a "belt and suspenders" approach to security, where multiple layers of defense are deployed throughout the IT infrastructure. In this context relying on systems all sourced from one vendor, a monoculture, could be a liability. But a positive effect of unifying these systems is that authentication can flow through from the end user's Windows O/S login to the security infrastructure. In practice Defense in Depth is accomplished at the company when the mail flow is sanitized at the server, filtered at the LAN perimeter and again inspected by the endpoint AV stack.

Microsoft offered two email security options at the time of implementation, Office 365 - Advanced Email Threat Protection (Office 365 - Advanced Email Threat Protection, n.d.), and Exchange Online Protection (Email Security - Microsoft Exchange Online Protection, n.d.), the latter formerly known as Forefront Online Protection for Exchange. Rather than use a traditional three-year product cycle, with Office 365 Microsoft has committed to a continual development process. New products and feature sets are being released frequently and this is particularly true in the security and administration of Office 365.

To maintain the company's security posture, it would need to replace the McAfee SaaS platform for email filtering and archiving. Can it maintain the current feature set at a reasonable price? Can it address new threats as they become prevalent?

A recent phishing incident demonstrated the importance of greater prevention around email spoofing. The head of HR received a forged request for W2 forms from her boss. She asked IT about this email before replying to it, a result that was largely due to training. Unfortunately, the volume and targeting of phishing emails are increasing rapidly.

Implementations of SMTP email do not prevent a user from sending mail under a forged identity. Email spoofing can be prevented by not allowing any unauthorized server

to deliver mail to the company for its domain, but that would break legitimate uses of the user's email identity unless a comprehensive whitelist were maintained.

Many service providers use this feature to send legitimate messages with the identity of the client. Mailing list servers like Constant Contact, MailChimp, and MailMan; as well as web applications and equipment notifications from network devices all send email under the user's identity. These are legitimate uses of the ability to send messages with a forged sender address.

Some specific requirements:

- Filtering Spam messages
- Blocking executable attachment types
- Addressing malicious links in messages
- Ability to filter message content for compliance with PCI DSS and Massachusetts law 201 CMR 17.00 protections on private information
- Ensuring encryption of messages with sensitive content

To comply with privacy protections and best practices, the company will encrypt any private information that is transferred over the internet. MA 201 CMR 17.00 (201 CMR 17.00) defines this "personal information" as information that contains financial account codes associated with individuals' names. In practice, the company does not handle some of the most sensitive customer account information – social security numbers, but all organizations must safeguard employee data. Those who accept credit card payments must safeguard financial information.

The simplest way to ensure information privacy would be to encrypt email, but email security is hard to guarantee from sender to receiver. The message transport may utilize encryption such as STARTTLS, but this does not guarantee encryption from end to end. In 2015 a study found that information privacy faces several obstacles due to the nature of the SMTP protocol and its extensions:

"Unfortunately, in the protocol's current form, mail providers cannot fail closed in the absence of STARTTLS until there is near total deployment of the extension, and

until organizations deploy valid certificates, relays will be unable to automatically authenticate destination servers." (Durumeric, et al., 2015)

Phishing attacks due to mail spoofing are increasingly common and cannot be adequately controlled through authentication. This same study (Durumeric, et al., 2015) found that additional measures that have been implemented to provide authentication including DKIM and SPF are not universal and have significant challenges with shared infrastructure, such as found in cloud services like Office 365.

Even if STARTTLS were universal, encryption of the message in transit does not address what occurs once the message is received at a service provider. In a cloud-based system, the security of these messages at rest on the server is handled by a third-party unknown to the sender, and possibly the recipient.

4. Cyber Security Design and Implementation Issues

4.1. Mitigation of Incidents via the Email Infrastructure

End to end encryption is necessary to allow business communication containing private information. But STARTTLS cannot be relied upon for end to end encryption at present. Various solutions have grown up around this issue. Commonly used email encryption systems such as PGP and S/MIME are available but require technical skill of both sender and recipient - who must be using compatible applications to communicate effectively. (Why No One Uses Encrypted Email Messages, n.d.)

File sharing sites such as Box and OneDrive (and many, many others) allow the user to send a link to a password protected secure site, rather than send an unencrypted attachment.

The user could be trained to encrypt an attachment containing private information before sending. Microsoft Office applications can securely encrypt a document before it is sent as an attachment. After encrypting the document, the user can separately communicate a password to the recipient. In practice, some users are likely to send an encrypted file attachment in an email containing the password – rather than using a separate communication with the password – thus defeating the purpose of encrypting the

file attachment. To ensure security, the human element must be considered as well as the technical design!

Secure file sharing is improving quickly and the company considered OneDrive for Business to replace other file sharing methods. A drawback of OneDrive for Business is its heritage in the Groove product, which is focused towards file synchronization. File synchronization prompts are confusing to users who simply want to share an occasional file or folder. Consider the case of an international traveler whose equipment may be inspected by customs officials… It may not be appropriate to synchronize files on a laptop rather than work with them remotely.

A filtering system to handle SPAM and malicious attachments was required. A method to neutralize malicious links would be very helpful, but this falls under the action of the receiving endpoint when a web page is launched. Security systems that replace web links in an email with a sanitized link often break the links they replace. These systems may have no knowledge of valid UNC paths. The vulnerability lies in the web browser, modifying (and potentially breaking) the email message does not address a general vulnerability of the browser.

Filtering web access at the internet connection as well as through antivirus and anti-malware software on the endpoint addresses malicious links received in an email message, but the increasing rate of change in malicious web links makes this a hit or miss proposition.

5. Policies Implemented to support the design

The company requires the ability to send and receive HTML email. Outlook does not display images in an email by default - preventing an attack vector for malware and message tracking by the sender. But unless a group policy is applied, this is under the discretion of the user. The company chose to allow the user to select when to enable graphics on a message by message basis. Graphics in an email are required, but they are not required for every message. Training will include an explanation of why these graphics are not always displayed.

Richard L. Snow, rich@bnc-consulting.com

Choosing where to filter and archive messages is also a policy decision. Office 365 has various levels of security filtering available, and the product feature set has been changing rapidly. The Microsoft antivirus solution Security Essentials had a poor track record. The underlying AV signatures were reported to be the same as those used in Forefront so the company explored alternative filtering offers. A requirement for archiving was to eliminate the need to store large quantities of email, allowing the user to reduce their mailbox size. User access to Microsoft's built-in archiving system was deemed to be too difficult at the time of implementation. Many alternative filtering and archiving systems are on the market. Mimecast, Proofpoint, EdgeWave, and Microsoft were evaluated based on price, feature set and the history of reliability. EdgeWave won out based on price and reliability.

Since the implementation in September 2016, Microsoft has continued to change their anti-malware feature sets and now utilize malware signatures from multiple 'best of breed' providers. (Anti-malware protection FAQ: Exchange Online Help, 2016) Company requirements around archiving are changing at the same time, and using the Microsoft inbuilt archive capability may meet the need in the future.

Maintaining a separate filtering infrastructure increases the complexity of the configuration and administrative tasks. For small sites, the simplest way to handle user accounts at an external spam filtering provider is to manually maintain the list of users. Each email enabled user needs an independent entry for their mailbox and aliases. This is an extra step when Onboarding new employees.

Testing mail-flow is complicated by the routing through the external provider. Likewise, an external archiving service is also isolated from the Active Directory authentication infrastructure. Message archives store the messages in .EML format, which is not a Microsoft format. These messages can be read with some Outlook versions. Moving data from one archive service to another can be time-consuming and expensive, and the archive must be encrypted in transit.

Using Microsoft for spam filtering and archiving where possible simplified administration and provided a single point of contact for tech support, and it would also allow better reporting and auditing of user accounts.

Richard L. Snow, rich@bnc-consulting.com

Mobile devices will now come under the Windows password policy when accessing Office applications. The company has a 90-day password expiration and requires complex passwords 8 characters or longer.

6. Technical features to improve prevention, detection of issues and recovery of infrastructure

6.1. Redundancy

Provisioning an external archiving system and mail filtering system provides some opportunities for redundancy if Microsoft servers are offline. The EdgeWave product set allows web-based email access during outages. The archive allows access to deleted messages and accounts and is valuable for forensic and compliance research.

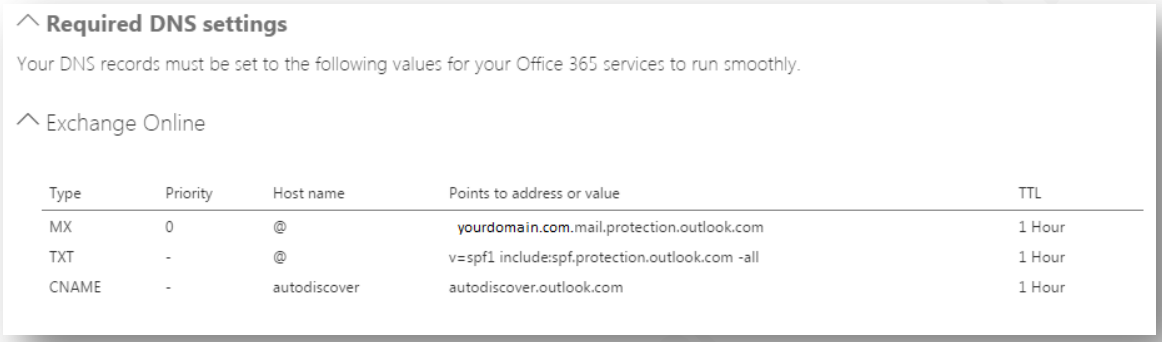
6.2. Backup Concerns

Office 365 uses replication technology rather than traditional backup and restore to prevent data loss (Backing up email in Exchange Online: Exchange Online Help, 2016). Each organization will need to decide if they are comfortable with this backup method.

In 2015 Microsoft changed the retention policy for deleted items and they are now stored “indefinitely”. The retention period can be adjusted through changing the default “MRM” retention policy (Redmond, 2015). This is critical to understand for compliance purposes if the organization has mandated a limit to email retention for legal purposes!

6.3. DNS

Email for the domain is directed to the third-party filtering company by setting the MX record for the domain. The Office 365 admin center provides a list of DNS records required for the service. (Note: there are several records to be managed here depending on what services you are implementing.)



Required DNS settings

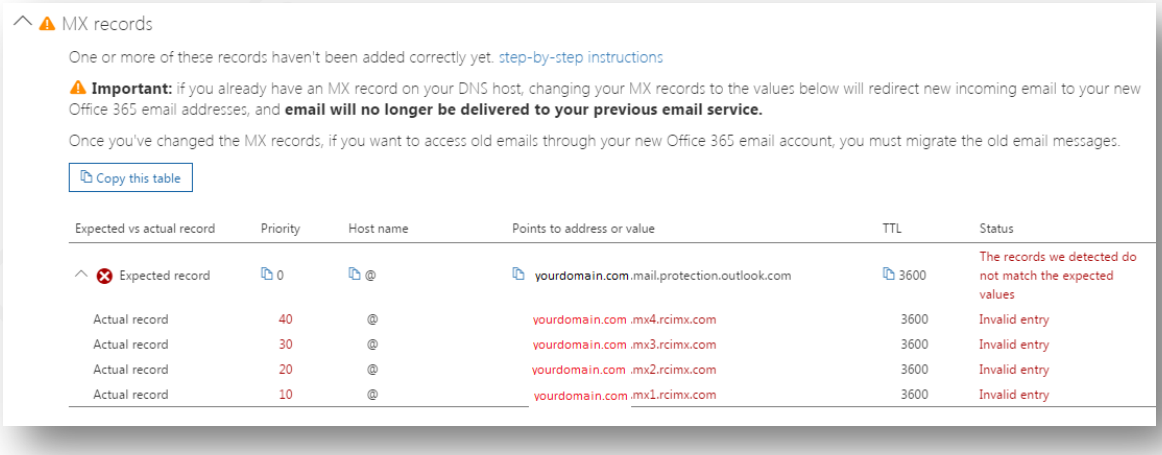
Your DNS records must be set to the following values for your Office 365 services to run smoothly.

Exchange Online

Type	Priority	Host name	Points to address or value	TTL
MX	0	@	yourdomain.com.mail.protection.outlook.com	1 Hour
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour

Figure 1- Exchange DNS Settings for Office 365

Microsoft's DNS checker will show an error when the MX records are directed to an external provider. Once mail flow has been set up and tested – this error can be ignored. Microsoft even provides a button to 'ignore' the errors!



MX records

One or more of these records haven't been added correctly yet. step-by-step instructions

Important: if you already have an MX record on your DNS host, changing your MX records to the values below will redirect new incoming email to your new Office 365 email addresses, and **email will no longer be delivered to your previous email service.**

Once you've changed the MX records, if you want to access old emails through your new Office 365 email account, you must migrate the old email messages.

Copy this table

Expected vs actual record	Priority	Host name	Points to address or value	TTL	Status
Expected record	0	@	yourdomain.com.mail.protection.outlook.com	3600	The records we detected do not match the expected values
Actual record	40	@	yourdomain.com .mx4.rcimx.com	3600	Invalid entry
Actual record	30	@	yourdomain.com .mx3.rcimx.com	3600	Invalid entry
Actual record	20	@	yourdomain.com .mx2.rcimx.com	3600	Invalid entry
Actual record	10	@	yourdomain.com .mx1.rcimx.com	3600	Invalid entry

Figure 2- DNS Checker with an external mail exchanger

An Exchange connector can be configured to use a third-party filter on outbound messages as well.

6.4. Azure AD Connect

Office 365 includes licenses for MS Office software as well as hosting services. The Office suite is available on a subscription basis as well as in a traditional license SKU. When the user signs into the subscription version of Office programs, their email

address and password are required. This can be an account managed in the Office portal or it could be an account synchronized with an AD domain.

Active Directory Federation Service (ADFS) could be implemented to synchronize an on-premise domain with the cloud, but it requires additional server infrastructure. A simpler service, Azure AD Connect can be used to provide synchronization. Often this is configured for one-way synchronization of accounts to Azure, and Office 365. A static password is no longer used for hosted email accounts – the user's AD account and password are used. The same credentials are used to log on to the domain as for applications on the user's mobile device. Self-service password reset is possible through Azure AD premium where two-way synchronization is enabled.

6.5. Password Policy

If password policies are enabled in the domain such as password expiration and complexity, these can mostly be mirrored in Office 365. One thing to note is that there are different restrictions on characters that are allowed in passwords and the length of passwords in Azure AD. In a Windows domain, a password can contain a space but this is not allowed in Azure AD. Azure AD also restricts password length to 16 characters (Password policies and restrictions in Azure Active Directory | Microsoft Docs, 2015). This sometimes shows up when the user's account will not synchronize to Office 365!

The company decided that by synchronizing passwords with AD, the users could tolerate a password change every 90 days because they no longer must remember a separate password for their email account.

6.6. Local Administration

Directory synchronization controls where the account is managed. If the account is synchronized from AD, then management is done through the familiar tools in the Windows domain environment. Auditing of windows logins is available through the domain controller, but there is no native auditing and reporting on user file access.

The AD Connector can be set to synchronize a particular OU. The company has a Staff OU that syncs users with subscriptions. Distribution Groups from AD are used to

control mailing lists in Office 365. It is also possible to add accounts directly in the Office 365 portal, which are managed online through the portal.

Contact information in each synced user's account will be populated in the GAL. In ADUC the "Advanced Features" view needs to be enabled in order to use the attribute editor under each user account. SMTP addresses are entered under the proxyAddress attribute:

- Main address: SMTP:user@domain.com;
- Aliases: smtp:alias@somedomain.com

The company's administrators spent some quality time cleaning up and reorganizing entries in Active Directory. These were made consistent and correct before they were synchronized to Azure AD. During the process of installing Azure AD Connect, there are options to scan and clean up directory entries, such as IDFix, which are very helpful.

6.7. Reporting

Office 365 has an expansive reports area, with an overall usage display featuring Email, OneDrive, SharePoint and Skype for Business activity, along with Office Activations.

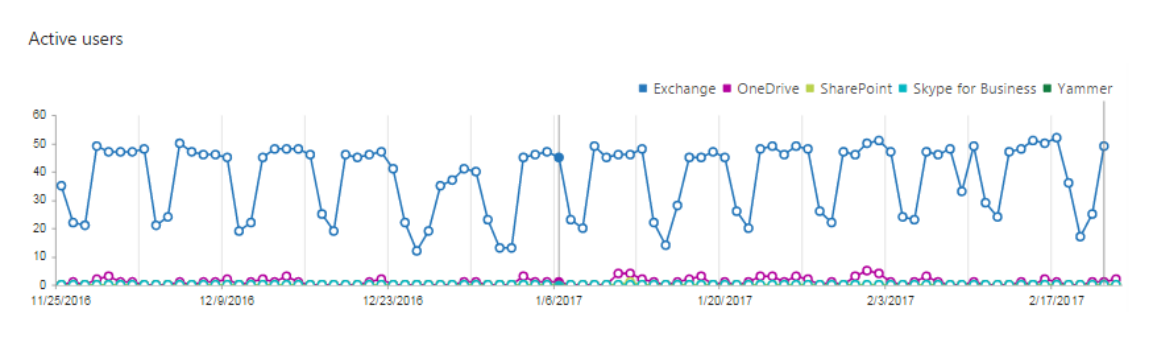


Figure 3- Usage Report from the Office Administrative Center

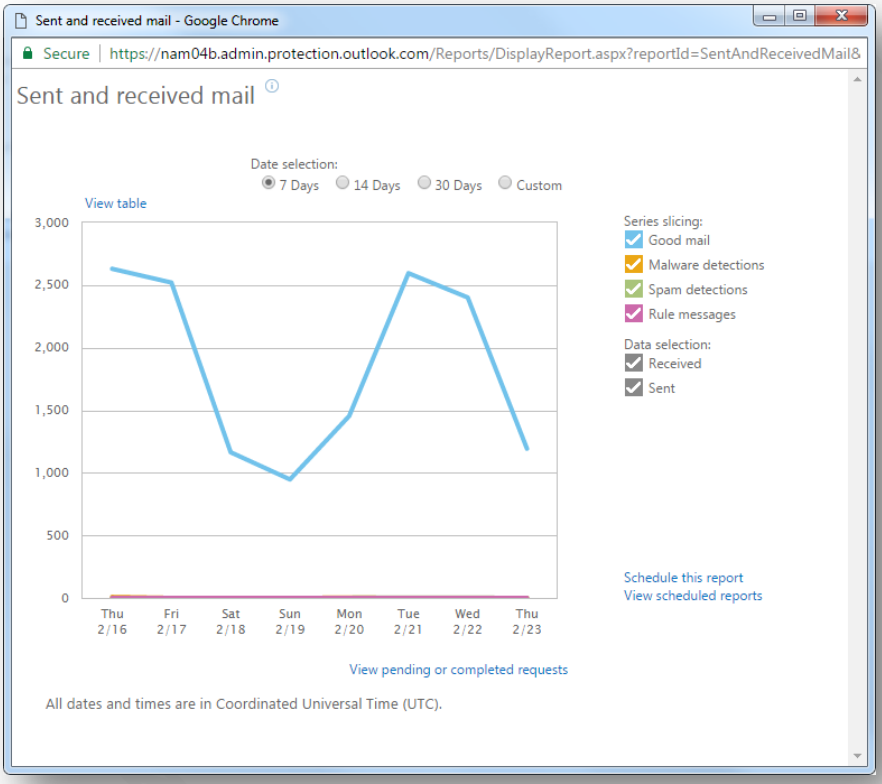


Figure 4- Sent and Received Mail from the Security & Compliance Reports

The "Sent and received mail report" shown above does not show spam and malware detections. With Microsoft's filtering system they would be shown conveniently in this report.

For mail debugging purposes, there is a detailed message trace feature in Exchange. In the Security & compliance tab, there are 17 reports in the areas of Auditing, Protection, Rules and Data Loss Prevention (DLP). Under the Azure administrative center, there are 20 reports regarding users accessing the services integrated with Azure AD, including auditing login information and detecting anomalies such as sign-ins from multiple geographies and sign-ins after multiple failures.

Richard L. Snow, rich@bnc-consulting.com

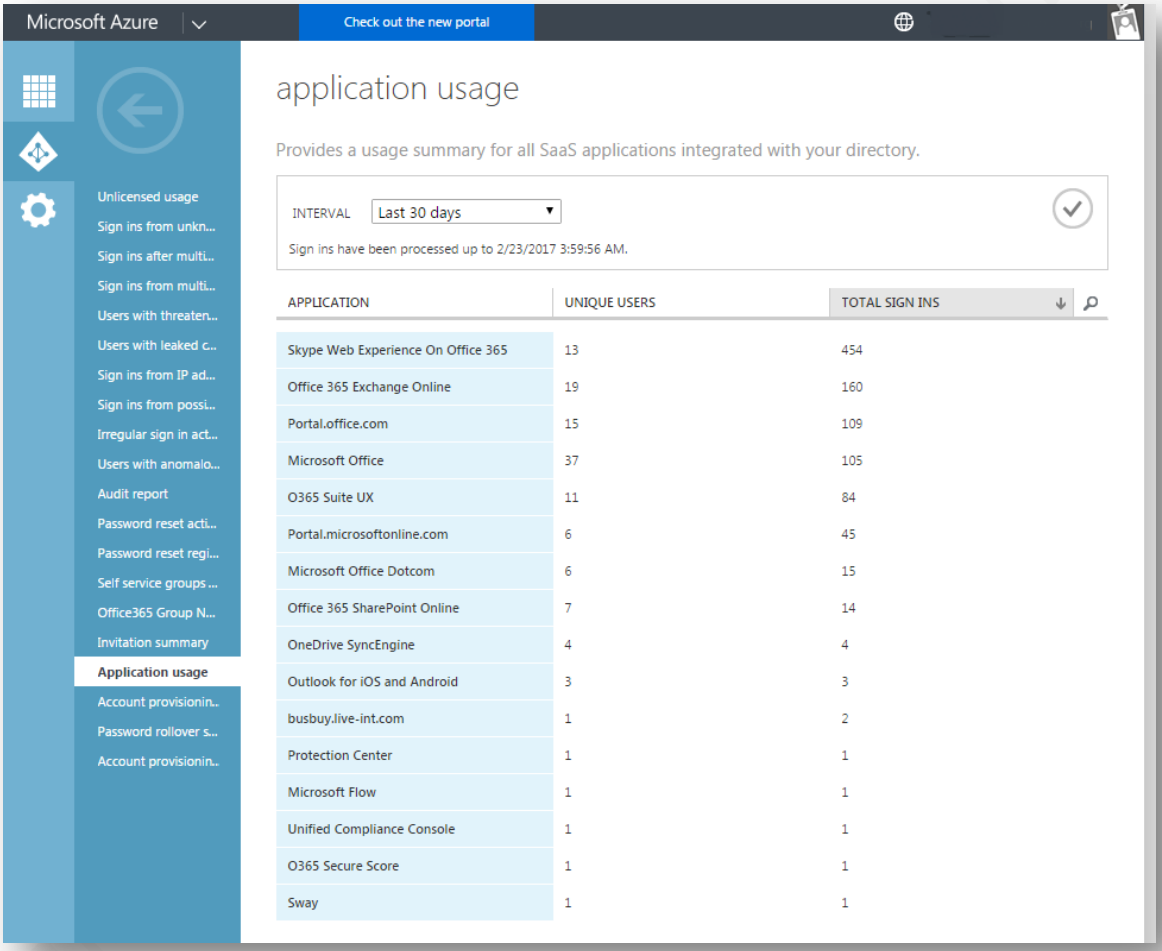


Figure 5- Reports in the Azure Administrative Center

Detailed information regarding directory synchronization is shown in the Office portal. This is handy when debugging password synchronization, and creating new users. Finally, there is a dashboard showing the service status of the Microsoft servers in the local region to help understand service outages.

These are just a few of the reporting options that are available in the product. Reporting is greatly advanced over the legacy deployment of Exchange, SharePoint and Active Directory.

Richard L. Snow, rich@bnc-consulting.com

7. Cyber Security Lessons Learned

7.1. Security vs. Useability

During the conversion into Office 365, the company needed to manually configure and test the user's desktop applications. This required that resetting all passwords, reconfiguring the user's profile, and ideally setting the password to require a reset.

The company did not require a password reset. Users received a new password when they came in for their first day with Office 365. Logging on, logging into the Office applications and learning to activate the Office suite presented a challenge to many users. If a password reset had been required there would have been confusion due to the time it takes for the password to synchronize from AD to the cloud. On this first day with Office 365, the user needs to authenticate both to AD and the cloud in a matter of minutes. All the user's passwords were reset in 90 days as a matter of course.

Older versions of Microsoft Office had to be removed from the systems before installing Office 2016. Even after removing the older apps, many systems do not save the user's Office activation from day to day. After much exploration, it seems that completely rebuilding the machine is the best solution for the worst cases. Also, the newer "Click to run" applications are not compatible with Microsoft's EMET security tool. Where EMET had been installed it was best to wipe and reload the system.

Mail relaying is required for internal servers and devices to send outbound mail. Best practice requires using a secure connection and password authentication to smtp.office365.com:587. Some applications do not provide SMTP AUTH or encryption, in which case an SSL tunnel application such as stunnel may be used as a mail proxy.

7.2. Leverage your relationships

Service providers were essential to the success of the project. The company relied on an engineer with its local VAR who understood the interactions of the different parts of Office 365. AD sync and the Office installation was completed before implementing the email mail flow. The newer versions of Office are much easier to configure with Exchange online.

Richard L. Snow, rich@bnc-consulting.com

Microsoft does not provide automated migration tools to migrate from a hosted Exchange provider. But the legacy hosting provider MindShift agreed to develop a custom migration project plan. MindShift was losing business to Microsoft, but they were willing to perform the migration. It never hurts to ask!

7.3. Greater Administrative Access

Moving from a dedicated Exchange server to a tenant in a hosting environment often results in a loss of administrative privilege. The company has a tenant environment within Office 365 which offers greater administrative control through Powershell. In the legacy hosted environment, the company's access is limited to basic user administration.

One example of administrative access through Powershell is shared calendar information. By default, the company shares full calendar information. The default in Office 365 and Exchange 2016 is to share the free/busy information but not the calendar entry detail. The permissions for user calendars can be changed through Powershell scripting by the administrator.

A similar issue arose regarding the board of Trustees. These important users require the ability to read attachments, but they are not using a Microsoft system. The most consistent way to deliver attachments to external users is to turn off TNEF formatting. This is best accomplished through Powershell.

7.4. Mobile Device Security

As a non-profit organization with limited use of private information, the company considered MDM systems and found them to be overly complicated and expensive. Through Office 365 it now has greater visibility into users' activity. And it can enact basic policies through ActiveSync such as locking or wiping a device that may be lost.

A full MDM system may be employed to provide further management of mobile devices and to segment work-related data from personal data. Microsoft offerings in this area have the advantage of access to the authentication mechanism in Azure AD and can extend other infrastructure investments such as SCCM. Microsoft InTune provides remote management of mobile devices, but it also has capability beyond smartphones and tablets to manage laptops and remote desktops.

Richard L. Snow, rich@bnc-consulting.com

7.5. Third party vendors

Where the security of company information is required, it is important to certify cloud vendors as a matter of due diligence. At a small company, best practice requires examining security certifications in place before engaging with a cloud vendor. Larger companies may have the clout and budget to audit cloud vendors, and to negotiate contractual terms.

The company has an information security program following best practice recommendations from the ISO/IEC 27002 standard, and it complies with PCI DSS 3.2 and MA 201 CMR 17. (ISO/IEC 27002; PCI DSS Quick Reference Guide, 2016; 201 CMR 17.00)

ISO 27002 and PCI DSS 3.2 include controls for supplier relationships. These standards are designed to be implemented appropriately with regard to the scale and nature of the business.

The company evaluates and maintains documentation of security certifications and practices of third party vendors who may handle personal or sensitive information. Microsoft publishes extensive guidance on the security controls and SLAs in place for Office 365. (Microsoft Office 365 security, n.d.) (Top 10 lists, n.d.) (Online Services Consolidated SLA, 2017)

Cloud applications are in some measure designed to replace or evade the control of an IT or compliance group within a company – the so-called "shadow IT" effect, so it is crucial to work with staff to ensure that sensitive information is handled properly by cloud vendors.

8. Conclusion

It's helpful to recall the old saw that the best firewall is an air gap. To meet current business needs, we do not have the luxury of an air gap between the internet and our most sensitive information. Just the opposite, applications now reach through the company's primitive filters to provide the services that the community is clamoring for, and potentially to expose sensitive information. The coming deployment of IPV6 may

obsolete NAT altogether or tunnel through IPV4 with technology such as Microsoft's Teredo. Look Ma, no air gap!

There are limited personnel resources available to the company to monitor and manage internal servers. The company must explore the cost advantage of moving at least some services to a cloud provider, along with the benefits of new workflows that are enabled by mobile and remote access. Mobile applications will take advantage of extending user authentication to the cloud provider to enable future hosted services such as a GIS Map.

Well-defined administrative practices and SLAs (Online Services Consolidated SLA, 2017) are scarce in the non-profit and small business world – but they are available from cloud vendors such as Microsoft at no cost premium. Coupled with additional compliance and DLP reporting, this may balance the discomfort administrators feel when moving applications and file storage out of house.

Richard L. Snow, rich@bnc-consulting.com

References

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH. (n.d.). Retrieved February 26, 2017, from www.mass.gov: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

Anti-malware protection FAQ: Exchange Online Help. (2016, November 11). Retrieved from technet.microsoft.com: https://technet.microsoft.com/en-us/library/jj200664(v=exchg.150).aspx

Backing up email in Exchange Online: Exchange Online Help. (2016, June 23). Retrieved from technet.microsoft.com: https://technet.microsoft.com/en-us/library/dn440734(v=exchg.150).aspx

Durumeric, Z., Adrian, D., Mirian, A., Kasten, J., Bursztein, E., Lidzborski, N., . . . Halderman, J. A. (2015, October). *Neither Snow Nor Rain Nor MITM . . . An Empirical Analysis of Email Delivery Security.* Retrieved from ACM IMC 2015: http://conferences2.sigcomm.org/imc/2015/papers/p27.pdf

Email Security - Microsoft Exchange Online Protection. (n.d.). Retrieved February 1, 2017, from products.office.com: https://products.office.com/en-us/exchange/exchange-email-security-spam-protection

ISO/IEC 27002. (n.d.). Retrieved February 26, 2017, from Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_27002

McGuinness, T. (2001). *Defense in Depth.* Retrieved from SANS.org: https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525

Microsoft Exchange Email Archiving Solutions. (n.d.). Retrieved January 4, 2017, from products.office.com: https://products.office.com/en-us/exchange/microsoft-exchange-online-archiving-email

Microsoft Office 365 security. (n.d.). Retrieved February 26, 2017, from Microsoft Trust Center: https://www.microsoft.com/en-us/trustcenter/security/office365-security

Richard L. Snow, rich@bnc-consulting.com

Office 365 - Advanced Email Threat Protection. (n.d.). Retrieved January 4, 2017, from products.office.com: https://products.office.com/en-us/exchange/online-email-threat-protection

Office 365 Nonprofit plans and pricing. (n.d.). Retrieved February 24, 2017, from products.office.com: https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing

Online Services Consolidated SLA. (2017, January). Retrieved from microsoftvolumelicensing.com: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=11675

Password policies and restrictions in Azure Active Directory | Microsoft Docs. (2015, February 5). Retrieved from docs.microsoft.com: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-policy

PCI DSS Quick Reference Guide. (2016, May). Retrieved from www.pcisecuritystandards.org: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1488155774124

Redmond, T. (2015, February 19). *Compliance and hybrid problems loom as Microsoft plans to keep every deleted item in Exchange Online | Tony Redmond's Exchange Unwashed Blog*. Retrieved from Windows IT Pro: http://windowsitpro.com/blog/compliance-and-hybrid-problems-exchange-online-keeps-every-deleted-item

Salamon, L. M. (1999). *Global civil society - Dimensions of the nonprofit sector*. Baltimore, MD: The Johns Hopkins Center for Civil Society Studies.

Search product lifecycle. (2017, February 24). Retrieved from Microsoft.com: https://support.microsoft.com/en-us/lifecycle/search/8753

Shinder, D. (2007, May 7). *Which edition of Office 2007 is right for you?* Retrieved from TechRepublic: http://www.techrepublic.com/article/which-edition-of-office-2007-is-right-for-you/

Richard L. Snow, rich@bnc-consulting.com

Top 10 lists. (n.d.). Retrieved February 26, 2017, from products.office.com: https://products.office.com/en-us/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy

Why No One Uses Encrypted Email Messages. (n.d.). Retrieved February 23, 2017, from How-To Geek: https://www.howtogeek.com/187961/why-no-one-uses-encrypted-email-messages/

Windows 7 Technical Library Roadmap. (2009, October 21). Retrieved January 4, 2017, from Microsoft Technet: https://technet.microsoft.com/library/dd349342(v=ws.10).aspx

Richard L. Snow, rich@bnc-consulting.com

Last Updated: March 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Boston Spring 2018	OnlineMAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced