Securing Exchange Online

About this document

Preamble

Email poses an increasingly attractive vector for criminals to exploit. Most inboxes contain some form of confidential information, whether it is chatter about new products, sensitive information between C-suite members or vendor payment authorization emails from the finance department. Unauthorized access into email servers/inboxes is known as Business Email Compromise and is one of the most financially damaging online crimes.

Microsoft Office 365 usage is accelerating at an ever-increasing pace and adoption shows no signs of slowing. With the impending expiry of Exchange 2010 extended support, the need to provide email to the remote workforce during the COVID-19 pandemic, or the simple allure of no longer needing to manage email servers; more businesses are moving their email services to Exchange Online in the Microsoft Office 365 suite.

The shared security model adopted by most cloud service shifts a portion of securing data to the customer. Microsoft is no different in this respect, and they have published their security support matrix here: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. In this model, Microsoft will protect the platform by securing access to the physical components, making sure the underlying operating systems and applications have the latest patches, and providing the customer the ability to apply additional data and configuration controls. The customer is then responsible for managing identity, defining access to data, and maintaining configuration of the service to meet the security needs of their organization.

The base configuration of Exchange Online is set to allow quick onboarding of customers with minimal barriers to the smooth migration of email into the service. The configuration does require tweaks to in order to make it more secure. I aim to cover some of the more effective tweaks in this document and point the reader to the right documentation to secure their Exchange tenant.

Targeted readers

The information in this document is for all administrators and engineers that are responsible for securing Exchange Online. While somewhat technical in nature, each headline in this document can be used by non-technical people as a conversation starter with their technology team.

Not Included

Exchange Online has many settings and features. Some are large enough to merit a separate document on their own, and others are accessible only through scripting/coding. With this in mind, the following topics are not addressed in this document: Data Loss Prevention (DLP), Digital Rights Management (DRM), Advanced Threat Protection (ATP) and Advanced Message Encryption. The Outlook client can also be secured with policies, but this is also not addressed in this document.

Securing Identity

Account takeover is one of the most common forms of breach in Office 365. Malicious actors commonly take advantage of reused passwords that are leaked in breaches, and short, easy to guess passwords are easily broken by password spraying attacks. Criminals find this vector one of the easiest to exploit, so here are some ways to make it harder for them to succeed.

Identity source. The following four authentication methods are available:

- Cloud only
- Directory sync with password hash
- Directory sync with pass through authentication
- Directory sync with Active Directory Federation Services

Most businesses migrate from an on premise Exchange system into Exchange Online and will already have Microsoft Active Directory (AD) in place. Part of the migration process is to synchronize identities from Active Directory into Azure AD for use in Office 365. To use Azure AD connect to synchronize identities, you can have any Azure AD level license https://azure.microsoft.com/en-us/pricing/details/active-directory/ and you will can download it from the AAD blade in the Azure portal. I also recommend deploying the additional Azure AD Connect Health agent to your on-premise Domain Controllers to monitor the overall health of your replications to the cloud https://portal.azure.com/#blade/Microsoft_Azure_ADHybridHealth/AadHealthMenuBlade/overview.
Microsoft has published this handy guide to help the implementer decide which path is better for their organization https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#decision-tree

Azure AD has a number of features you can use to detect and block risky login. Many of the premium features require the password hash to be synchronized into Azure AD and work best when business users log in with the Microsoft Azure authentication portal. As Active Directory Federation does not synchronize the hash to Azure AD, many of the protections offered with Azure AD identity are not available with this authentication method.

Multifactor Authentication (MFA). There are two forms of MFA supported in Office 365:

- Office 365 MFA: this is managed through the Office 365 Admin portal, and is available to any consumer of the service.
- Azure Active Directory (Azure AD) MFA: this is managed through the Azure AD blade in the Azure Portal, and offers tight integration into other security services.

Both types support application based push notifications (Approve / Deny), text message (SMS) and voice based One-time Passcodes (OTP). While the consensus in the security community is that SMS and voice based OTP are not secure, the use of any MFA will raise security significantly, and having some form of MFA is better than having none at all. Where possible, use application based push notifications as a second factor.

Microsoft outline the pros and cons of each service in this document. They also include links to further documentation on how to enable each type of MFA. https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication

The Azure AD version of MFA offers extra protection when you include the use of Conditional Access (Azure P1 license) or Risk Based Conditional Access (Azure P2 license).

Conditional Access. Configuring conditional access specifies the conditions that must be satisfied before allowing use of the service.

While it can be somewhat tricky to do the initial configuration, it is worth the time as you can require a combination of conditions be present like: Trusted IP addresses, AD domain joined / Intune Compliant, type of app (legacy, browser, compliant app), MFA, Device type (Android, Windows, iOS), users/groups.

To make it easier to implement new policies, Microsoft added a “Report Only” toggle that allows you to test out your policies before enforcing them. There is also a “What if” feature that allows you to validate some combinations of conditions without needing to build the policy first.

More information on how to put together a Conditional Access policy is located here: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

Azure AD Identity Protection. Requiring a Premium Azure AD license (P1 or P2), this service adds additional reporting of risky logins, which can help raise awareness of potentially compromised logins.
Here is a guide on how to turn this feature on: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications

Azure AD Password Protection. You can use this feature to restrict the use of easy to guess passwords along with their common letter substitutions. If you have P1 or P2 premium licensing, you can also extend this protection into your on premise Active Directory domain by installing an agent on your domain controllers. With the additional license, you also gain the ability to upload a custom word list for blocking commonly guessed passwords.
Here is the Microsoft document on this feature: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

Limit Global / Exchange Administrators. Criminals that attack Azure AD / Exchange online tenants are themselves very competent Azure Administrators. Limit the exposure by reducing the number of accounts in privileged roles (like the Global / Exchange Administrator roles) by using Privileged Identity Management (Azure P2), or by moving accounts into lower privileged groups (like Global Reader).
Make sure that any accounts that remain in those roles have MFA enabled. A “break-glass” administrator account should not have MFA enabled, and needs to have a long and complex password stored in a physical safe.

Securing Exchange Online

Exchange Online contains many different vectors of attack. Examples can include group spam, persistent access for email account compromise, all the way to the spoofing of your CEOs email address. Here are some ways to increase security in Exchange Online.

Disable third party app integration. Allowing end users to approve the use of Office 365 apps potentially allows malicious persistent access to their email mailbox. Use the following document to turn this feature off to mitigate this risk. https://docs.microsoft.com/en-us/microsoft-365/admin/misc/integrated-apps?view=o365-worldwide#turning-user-consent-on-or-off

If you have had this feature enabled in your tenant for a while, an Administrator should review the list of applications that have already been granted access in Azure AD, and remove any that do not have a valid business justification. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide#steps-for-using-the-azure-active-directory-portal

Disable auto-forwarding email. If a criminal gains access to a user's mailbox, they can configure auto-forwarding rules to redirect email from the users inbox to a criminally controlled outside email address. Well-meaning employees, who may set up forwarding of company data into personal email services while trying to increase convenience of use. Exploited more often in business email compromise attacks, auto-forwarding allows the criminal to exfiltrate sensitive data, mask their presence, and maintain some level of persistence after credentials are changed.

Three ways to mitigate this attack are outlined in this article: https://techcommunity.microsoft.com/t5/exchange-team-blog/the-many-ways-to-block-automatic-email-forwarding-in-exchange/ba-p/607579

Enable notifications. Email alerts can be set up to trigger when risky activity is detected. Go to https://protection.office.com/alertpolicies and at minimum, enable the following rules:

- Creation of forwarding/redirect rule
- Impossible travel activity
- Elevation of Exchange admin privilege
- Users targeted by phish campaigns
- Phish (High Confidence) Detected during delivery

You can see alerts that were triggered by going to https://protection.office.com/viewalerts, but note that more detail on each event is actually located in the Cloud App Security portal https://portal.cloudappsecurity.com/#/alerts

Mark external emails with a banner. You can add text to an email if the sender originates from outside of your organization. This is useful to highlight inbound messages from external senders, especially spoofed emails from “the CEO”.

The basic steps to enable this feature are:

- In the Exchange admin center, navigate to Mail Flow and create a new rule called "External Mail Warning”.
- Set the rule as follows:
  - Set "Apply this rule if..." > The sender is located... > Outside the organization
  - Click “More Options…. at the bottom of the rule dialog
  - Set “Do the following...” > Prepend the disclaimer... > Add text (or HTML if you want it to stand out).
  - Set “Choose a mode for this rule” > Enforced.

Disable Legacy Authentication. Basic Authentication (aka Legacy Authentication) is used by older applications like Outlook 2010 and earlier versions of Exchange Online PowerShell, and older protocols like POP3 and IMAP. This type of authentication attracts password spraying and credential stuffing attacks because MFA is not inserted as a further barrier.

First, you need to turn on Modern Authentication, and then monitor Azure AD Sign In blade for legacy “Client Apps”. Once you have migrated the users of those legacy applications to their modern counterparts, you can either use Conditional Access to block access to legacy applications, disable use of specific protocols, or disable basic authentication for Exchange Online altogether.

Enable Modern Authentication: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online

Monitoring Sign-Ins for Legacy app authentication: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/new-tools-to-block-legacy-authentication-in-your-organization/ba-p/1225302

Block Legacy authentication by app with Conditional Access: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication
OR:
Disable Legacy Authentication: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online
OR:

Disable individual protocols on individual mailboxes:
https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/pop3-and-imap4/enable-or-disable-pop3-or-imap4-access

Disable app passwords. App passwords allow a user to create one or more passwords for use with non-browser applications that do not support Modern Authentication. Leaving this setting enabled is risky. Criminals use this feature to maintain persistent connectivity on compromised email accounts, and app passwords are not subject to the expiry policies applied to Azure AD or Active Directory on premise.

The feature can be disabled from either the Azure or Office 365 Admin portal:

Azure Portal:

- Go to https://portal.azure.com
- Click on blade Azure Active Directory
- Navigate to Users > All users
- Click Multi-Factor Authentication
- Click "service settings"
- Under app passwords, select "Do not allow users to create app passwords to sign in to non-browser apps"

Office 365 Portal:

- Go to https://admin.microsoft.com
- Click on Settings > Org settings
- Locate and click Multi-factor authentication, then Configure multi-factor authentication
- Click "service settings"
- Under app passwords, select "Do not allow users to create app passwords to sign in to non-browser apps

Enable Mobile Device quarantine. While Intune and Conditional Access offer a seamless way to control access to email on a mobile device, they are only available for tenants licensed with P1 and P2, or have an enterprise mobility license. Exchange Online has a feature that allows you to quarantine mobile device connections to Exchange.

To enable the feature, open the Exchange admin center, navigate to Mobile, and create a rule to cover the device types you want to control.

Enable Mailbox Level auditing. Mailbox auditing keeps a 90-day log of connections to mailboxes and the actions performed. Use this document to learn how to turn on auditing: https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019#enable-or-disable-mailbox-audit-logging

Enable Sender Policy Framework (SPF). SPF helps email administrators by reducing spoofed emails for their email domains. The key to enabling this feature is knowing about all email sources that could send email for your domain. Examples include internal email servers that send to outside recipients, Office 365, your marketing email provider and antispam solutions.

Once you have collected this information, you can use online SPF generators to create the record, and then you can apply the suggested TXT record change to your public DNS zone.

Note: If you maintain a split DNS zone (same domain name maintained internally and externally on different DNS servers), you will need to make sure both zones are updated with the TXT record.

Enable Domain Keys (DKIM) and DMARC. DKIM provides a way to verify the sender of the email. The sender does not have to match the From information, it's more about the server responsible for sending the email.

Like with SPF, you need to find all sources of emails from your domains, make sure they support DKIM, turn on the feature and publish the signature generated by DKIM for that mail source into the relevant DNS TXT record. Each mail source will have its own signature, and you will have one DNS record per mail source. If the mail sources support it, you can import a single signature in the TXT record.

DMARC allows other email systems to validate that the signature matches the one advertised for the originating mail server, and take the action prescribed in the DNS DMARC record.

DKIM: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide

DMARC: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide

Limit Calendar Sharing. If anonymous calendar sharing is enabled, your users can share the full details of their calendars with external, unauthenticated users. Calendars contain enough information to help attackers understand organizational relationships, gather information intended for internal parties, and determine when specific users may be travelling or more vulnerable to an attack.

To disable anonymous sharing:

- Go to the Services and Add-ins https://portal.office.com/adminportal/home?switchtomodern=true#/Settings/ServicesAndAddIns
- Click on Calendar
- Uncheck “Let your users share their calendar with people outside of your organizations who have Office 365 or Exchange”.

Restrict email from outside senders to sensitive groups. Criminals can distribute malicious emails to your employees via the use email Groups. Your sensitive groups should be set to block mail originating outside of your organization. Pay particular attention to groups that have less characters in the user part of the email address (before the @ symbol). There is a good chance that spam engines already found them by cycling through letter combinations.

- In the Exchange admin center, navigate to Recipients and then Groups.
- Open each sensitive group, click on "delivery management" and select "Only senders inside my organization"

Last thoughts

Some features require more work to configure properly, while other features may cause varying amounts of change in end user workflow. With this in mind, here is my list of quick wins to increase Exchange Online security:

- Enable MFA. Available in some form, regardless of the level you have purchased, it requires initial configuration, needs end user setup and introduces friction into the email login workflow. The security gained from this feature makes it well worth the effort, and end-users will eventually become accustomed to MFA use.
- Disable third party app integration. No complex configuration required, and most users will not know that the feature exists.
- Disable auto-forwarding email. This is very easy to do and shuts down a very commonly used method of persistence and data exfiltration.

- Enable notifications. Configured correctly, you will get alerts when a compromise is detected. You can then follow up with the appropriate incident response.
- Mark external emails with a banner. Providing visibility to end users will enable them to more easily identify spoofed emails from “their CEO”.
- Above all, please communicate with your email users and listen to what they have to say! Announcing service adjustments ahead of time will allow them time to wrap their minds around the changes coming at them, and it is better to have them as champions rather than an insider threat. Ultimately, they are your last line of defense, so treat them fairly and keep them up to date with what you are doing to keep them and their email safe!

Implementing the features and controls listed in this document will help your organization raise the bar against criminals seeking access to the sensitive data in your email environment. I hope this document helps you to increase the security of your Microsoft Exchange Online tenant.

I would like to thank Jim, Ryan, Evan, Kenni and the 7MS Slack Blueteam members for all of their valuable contributions to this document.

Finally, you should be able to find an updated copy of this document at the following link:
https://github.com/systeminsecure/public_documents/blob/master/Securing%20Exchange%20Online.pdf