TLP: WHITE

OFFICE 365 SECURITY RECOMMENDATIONS FOR SMB

IstroSec

Date: 28. 3. 2023 | Project: Office 365 Recommendations | Version 1.0

Černyševského 10 | 851 01 Bratislava | info@istrosec.com | www.istrosec.com

CONTENTS

INTRODUCTION

Office 365 is a common target to attackers because it is a popular cloud-based platform that is used by many organizations. Remote work popularized cloud platforms and enterprises began to rely more on cloud solutions, such as Office 365. Office 365 is a large, complex system that is constantly evolving, making it difficult to secure and manage.

Common attacks against Office 365 include phishing attacks, where attackers use malicious emails to trick users into revealing sensitive information or downloading malicious software, or brute force, where attackers use automated tools to guess passwords and gain access to accounts.

After gaining an initial access to the systems, attackers can deploy a wide range of payloads, including BEC, data exfiltration, malware or various destructive attacks.

This guide goes in-depth into defending the Office 365 using built-in security features and policies and describe ways to detect security incidents within the system and respond to them using built-in tools and policies.

OFFICE 365 HARDENING

Create a break glass account

A break glass account is an emergency account that is used to access critical systems or data when all other access methods have failed. It is important because it provides a secure way to access critical systems or data in the event of an emergency, such as a security breach.

The following statements should be true of the break glass account:

- It should have the highest, global administrator role.
- It should be excluded from security policies, such as MFA requirements or other conditional access policies.
- The account should be used only for emergencies and disaster recovery purposes.
- It should be protected with a strong and unique password.
- The password should be only stored offline and physically protected from unauthorized access.
- Any login or activity related to the break glass account should be monitored.

How to create a break glass account:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Under Manage, select Users.
- Click on New user and Create new user.
- Give the account a User name.
- Give the account a Name.
- Create a long, complex, and unique password for the account.
- Under Roles, assign the Global Administrator role.
- Under Usage location, select the appropriate location.
- Create.

References:

https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

Enable multifactor authentication

Multifactor authentication (MFA) in Office 365 is a security feature that requires users to provide more than one form of authentication to access their Office 365 account. This can include a combination of something the user knows (such as a password), something the user has (such as a phone or security token), or something the user is (such as a fingerprint or facial recognition). MFA helps protect user accounts from unauthorized access, even if a user's password is compromised.

We recommend enabling MFA for all user accounts, with only the exception of a break glass account or service accounts. In environments, where globally enabling MFA is not possible, we recommend deploying MFA at least to privileged and sensitive accounts (administrator accounts, financial & HR departments, C-level executives..).

To enable multifactor authentication for administrators, use the Microsoft 365 Admin Center:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Select Security then, under Protect, select Conditional Access.
- Click New policy.
- Go to Assignments > Users and groups > Include > Select users and groups > check Directory roles.
- At a minimum, select the following roles: Billing admin, Conditional Access admin, Exchange admin, Global admin, Helpdesk admin, Security admin, SharePoint admin, and User admin.
- Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and do not exclude any apps).
- Under Access controls > Grant > select Grant access > check Require multifactor authentication (and nothing else).
- Leave all other conditions blank.
- Make sure the policy is enabled.
- Create.

Warning: Do not lock yourself out. Never apply Conditional Access policies to all admin accounts. Make sure you exclude a break glass account.

References:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Make sure only strong types of MFA are allowed

While MFA provides a strong account protection, it is still vulnerable to phishing. MFA can be phished because it relies on the user to provide the correct credentials. Attackers can use social engineering techniques to trick users into providing their credentials, including verification codes from SMS or codes from authenticator apps.

We recommend the use of strong types of MFA, such as FIDO2 security keys. FIDO2 keys are resistant to social engineering attacks and cannot be bypassed by phishing sites. Additionally, FIDO2 allows password less authentication – making the sign-in experience safer and more intuitive for users.

If FIDO2 keys are unattainable due to the initial cost (about 100€ per user), or other reasons, we recommend using the Microsoft Authenticator option with number matching and geographic location prompt as the next-best option. With number matching and geographic location prompt enabled, the user is shown a prompt with the location of the sign-in and must enter a code from the Authenticator app.

To add FIDO2 keys into user account:

- Navigate to: https://mysignins.microsoft.com/security-info
- Click Add sign-in method.
- Select Security key and click on Add.
- Follow instructions to add a security key, repeat the process for a backup key.
- Make sure two keys are added and visible.

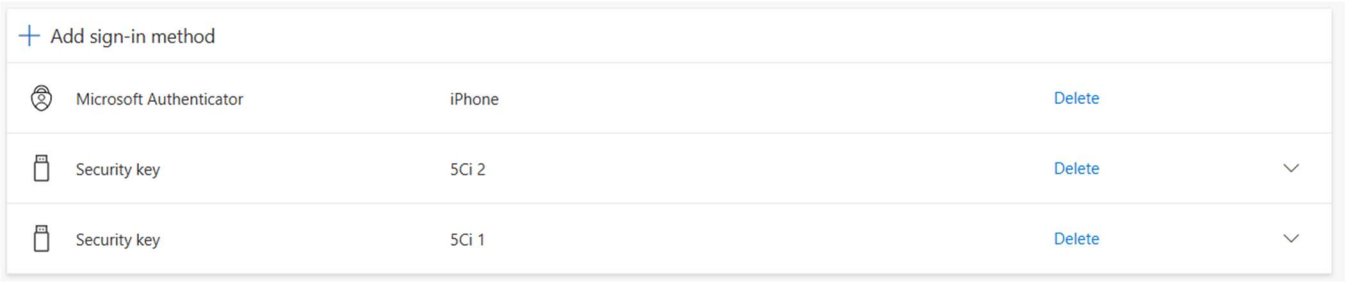

Image 1. Security Info screen with two keys and Authenticator app

To enforce FIDO2 (make sure users added FIDO2 keys prior to enforcement, otherwise they will be locked out):

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Select Security then, under Protect, select Conditional Access.
- Click New policy.
- Go to Assignments > Users and groups > Include > Select users and groups.
- Select groups and user accounts with FIDO2 security keys.
- Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and do not exclude any apps).
- Under Access controls > Grant > select Grant access > check Require authentication strength > Select phishing-resistant MFA.
- Leave all other conditions blank.
- Make sure the policy is enabled.
- Create.

Warning: Do not lock yourself out. Never apply Conditional Access policies to all admin accounts. Make sure you exclude a break glass account.

To enable number matching and geographic location prompt in Microsoft Authenticator:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Select Security then, under Manage, select Authentication methods.
- Select Policies, Under Manage.
- Click on Microsoft Authenticator.
- On the Enable and Target tab, Enable the policy and include users.
- On the Configure tab, enable Allow use of the Microsoft Authenticator OTP.
- Under Require number matching for push notifications, select Enabled.
- Under Show geographic location in push and password less notifications, select Enabled.
- Click on Save.

References:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths

Make sure modern authentication is enabled

Modern authentication in Exchange Online is a more secure authentication process that uses multi-factor authentication (MFA) and token-based authentication. It supports the use of security tokens, certificates, and other authentication methods to verify user identity. This authentication process is more secure than legacy authentication because it allows the use of multiple factors to authenticate a user, making it more difficult for attackers to gain access to user accounts. Additionally, modern authentication provides better protection against phishing attacks and other malicious activities. It also provides better visibility into user activity, allowing administrators to better monitor and control access to their Exchange Online environment.

Modern authentication should be enabled for most tenants, however, you should make sure that it is enabled in your environment.

To verify whether modern authentication is enabled:

- Install the Exchange Online PowerShell per documentation: https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-and-maintain-the-exchange-online-powershell-module
- Load the module and connect with a global admin account per documentation: https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps
- Run the following command:

```
Get-OrganizationConfig | Format-Table Name,OAuth* -Auto
```

- Output should be True if modern authentication is enabled.

To enable modern authentication in your tenant:

- Install the Exchange Online PowerShell per documentation: https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-and-maintain-the-exchange-online-powershell-module
- Load the module and connect with a global admin account per documentation: https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps
- Run the following command:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

References:

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

Disable legacy authentication

Legacy authentication is an authentication protocol that is vulnerable to brute force attacks, phishing, and other security threats. Disabling legacy authentication in Office 365 helps to protect your organization from these threats by ensuring that only modern authentication protocols are used. Modern authentication protocols are more secure and provide additional features such as multi-factor authentication, which adds an extra layer of security to your organization's data.

When disabled, legacy authentication protocols such as POP, IMAP, SMTP, and Exchange ActiveSync (EAS) will stop working. You can exclude certain user accounts or groups from the policy to maintain compatibility with legacy services.

To verify whether legacy authentication is actively used inside your organization:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Select Sign-in logs under Monitoring.
- Click on Add filters.
- Add a filter named Client app.
- Under Legacy Authentication Clients, check every option.
- Click on Apply.

To disable legacy authentication:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Select Security then, under Protect, select Conditional Access.
- Click New policy.
- Go to Assignments > Users and groups > Include > Select users and groups > check Directory roles.
- Include all Users and, if necessary, exclude certain accounts or groups.
- Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and do not exclude any apps).
- Under Conditions, click on Not configured under Client apps.
- Check Exchange ActiveSync clients and Other clients. Leave Browser and mobile apps and desktop clients **unchecked**.
- Under Access controls > Grant > select Block access
- Leave all other conditions blank.
- Make sure the policy is enabled.
- Create.

Warning: Do not lock yourself out. Never apply Conditional Access policies to all admin accounts. Make sure you exclude a break glass account.

References:

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

Block PowerShell access to users

Blocking PowerShell access to users in Azure AD and Office 365 can help protect your organization from malicious actors who may attempt to use PowerShell to gain access to sensitive data or to perform malicious activities. PowerShell consoles can be used by unprivileged user accounts to enumerate users, groups, and applications.

By blocking access to PowerShell, you can help ensure that only authorized users are able to perform these tasks. Additionally, blocking PowerShell access can help reduce the risk of malicious actors using PowerShell to gain access to sensitive data or to perform malicious activities.

To block PowerShell access, you should use a script provided by Microsoft: https://learn.microsoft.com/en-us/schooldatasync/blocking-powershell-for-edu

Follow the documentation closely and make sure to exclude administrator accounts from the policies.

References:

https://learn.microsoft.com/en-us/powershell/module/azuread/?view=azureadps-2.0

https://learn.microsoft.com/en-us/schooldatasync/blocking-powershell-for-edu

Block access to management portals for non-privileged users

By default, Azure AD allows access to the Azure Portal and PowerShell administrative consoles even to non-privileged users. Blocking access to admin portals in Azure AD is important for security reasons. It helps to protect your organization's data and resources from unauthorized access. It also helps to ensure that only authorized users can access sensitive information, such as list of users, including their properties and roles.

To block access to management portals:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Select Security then, under Protect, select Conditional Access.
- Click New policy.
- Go to Assignments > Users and groups > Include > All users.
- **Important:** Go to the Exclude tab, check Directory roles, and select privileged roles used in your organization, included but not limited to the Global Administrator.
- Go to Cloud apps or actions > Cloud apps > Include > Select apps > Select Microsoft Azure Management from the list.
- Under Access controls > Grant > select Block access.
- Leave all other conditions blank.
- Make sure the policy is enabled.
- Double-check whether administrator accounts, including the break glass account are excluded from the policy.
- Create.

Warning: Do not lock yourself out. Never apply Conditional Access policies to all admin accounts. Make sure you exclude a break glass account.

Audit accounts with privileged roles

Any role assignments should follow the principle of least privilege (POLP). POLP is a security concept that requires users to be given only the minimum level of access rights and privileges necessary to perform their job functions. This means that users should not be given any more access than is absolutely necessary to do their job, and should not have access to sensitive information or resources that are not relevant to their job. This helps to reduce the risk of data breaches, malicious activity, and other security issues.

Additionally, any privileged role assignment should be documented, approved, and removed after it’s no longer necessary.

To export the list of privileged role assignments:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Under Manage, select Roles and administrators.
- Select Download assignments.
- Click on Start.

Tenants with Microsoft 365 E5, Microsoft 365 E5 Security, Microsoft 365 F5 Security, Microsoft 365 A5 Security or Microsoft 365 A5, can utilize Privileged Identity Management (PIM). It provides a comprehensive set of features to help organizations manage, monitor, and secure privileged access to resources in the cloud. It also helps organizations to reduce the risk of privilege abuse and accidental or malicious misuse of privileged accounts by providing just-in-time and time-bound privileged access.

It also provides a single view of privileged access across the organization, enabling organizations to quickly identify and respond to potential threats.

For more information about PIM, see Microsoft documentation: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

References:

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Limit guest access

By default, guest user account can see memberships of all non-hidden groups within the Azure AD. This allows guest users to enumerate other users within the Azure AD tenant.

We recommend limiting the guest access to hide group membership information.

To hide group membership information from guests:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Under Manage, select Users.
- Under Manage, select User settings.
- Under External users, click on Manage external collaboration settings.
- Under Guest user access restriction, choose Guest user access is restricted to properties and memberships of their own directory objects.
- Save.

References:

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions

Enable Common Attachment Filter

Attackers may use malicious attachments to deliver malware, such as viruses, ransomware, and Trojans, to a user's computer. Attackers may also use malicious attachments to steal sensitive information, such as passwords, credit card numbers, and other personal data.

Common attachment filter in Office 365 is designed to protect users from malicious attachments. The filter detects suspicious file types, such as executable files, and block them from being downloaded. Additionally, the filters can be configured to block certain file types, such as .exe files, from being sent from the user's account.

Common attachment filter is harder to bypass by attackers, because it relies on „magic bytes", instead on just the file extension itself. This means that the filter can detect executable files in archives or files that lack their file extension.

To enable the common attachment filter:

- Log in to https://security.microsoft.com as a Global Administrator.
- Navigate to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware.
- Click on the Default policy.
- Scroll down and click on the Edit protection settings.
- Check the Enable the common attachment filter option.
- Click on Select file types.
- Add the following types:
    - apk,app,application,appx,bat,chm,cmd,com,dll,dmg,docx,elf,exe,gadget,hta,img,inf,iso,jar,js,jse,kext,lib,library,lnk,lsp,msi,msix,pif,pkg,ppkg,pptm,ps1,py,reg,scr,vb,vbe,vbs,vhd,vhdx,vsmacros,ws,wsc,wsf,wsh,xlsmm
- Save.

References:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide

Make sure Zero-Hour Purge is enabled

The zero-hour auto purge feature in Office 365 is a security feature that automatically deletes malicious files and e-mails from a user's mailbox within an hour of detection. This feature helps protect users from malicious content, such as phishing emails, ransomware, and other malicious attachments. The zero-hour auto purge feature scans all incoming emails and attachments for malicious content and deletes any malicious files it finds. This helps protect users from malicious content that may have been sent to them, as well as from malicious content that may have been sent to other users in their organization.

To verify whether Zero-Hour Purge for malware is enabled:

- Log in to https://security.microsoft.com as a Global Administrator.
- Navigate to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware.
- Select the Default policy.
- Scroll down and click on the Edit protection settings.
- Make sure Enable zero-hour auto purge for malware (Recommended) is enabled.

To verify whether Zero-Hour Purge for phishing is enabled:

- Log in to https://security.microsoft.com as a Global Administrator.
- Navigate to Email & Collaboration > Policies & Rules > Threat policies > Anti-Spam.
- Select the Anti-spam inbound policy (Default).
- Click on Edit actions.
- Make sure Enable zero-hour auto purge (ZAP) is enabled for both spam and anti-phishing messages.

References:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Enable Safe Links and Safe Attachments

The Safe Links feature in Office 365 is a security feature that helps protect users from malicious links in emails. It works by scanning links in emails for malicious content and replacing them with a safe link. When a user clicks on the safe link, they are taken to a Microsoft-hosted page that checks the link for malicious content. If the link is found to be malicious, the user is blocked from accessing the content. This helps protect users from malicious websites, phishing attempts, and other malicious content.

The Safe Attachments feature in Office 365 is a security feature designed to protect users from malicious email attachments. It works by scanning all incoming email attachments for malicious content and blocking any attachments that are deemed to be a threat.

Both features are limited to users with Office 365 E5, Microsoft 365 Business Premium, Microsoft 365 F5 Security, Microsoft 365 E5 Security, Microsoft 365 E5, Microsoft 365 A5 Security and Microsoft 365 A5 licenses.

To enable Safe Links:

- Log in to https://security.microsoft.com as a Global Administrator.
- Navigate to Email & Collaboration > Policies & Rules > Threat policies > Safe Links.
- Click on Create.
- Name your Policy.
- Include all users by adding your domains.
- Enable the feature for both messages and Microsoft Teams.
- Make sure Apply real-time URL scanning for suspicious links and Wait for URL scanning to complete before delivering the message are both enabled.
- Review the policy and submit.

To enable Safe Attachments:

- Log in to https://security.microsoft.com as a Global Administrator.
- Navigate to Email & Collaboration > Policies & Rules > Threat policies > Safe attachments.
- Click on Create.
- Name your Policy.
- Include all users by adding your domains.
- Under the Safe Attachments unknown malware response select Block.
- Review the policy and submit.

References:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-about?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-about?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-policies-configure?view=o365-worldwide

Set phishing e-mails to be quarantined

Quarantine is a feature in Office 365 that allows administrators to manage the flow of incoming emails. It can be used to identify and contain suspicious emails that may contain malicious content or spam. Quarantined emails are held in a secure location and can be released or deleted by the administrator and are invisible to users.

By default, only high confidence phishing e-mails are quarantined. Other phishing e-mails are moved to the spam folder and are visible to user. We recommend quarantining all phishing e-mails to prevent users manipulating with potentially malicious e-mails.

To quarantine all phishing emails:

- Log in to https://security.microsoft.com as a Global Administrator.
- Navigate to Email & Collaboration > Policies & Rules > Threat policies > Anti-Spam.
- Select the Anti-spam inbound policy (Default).
- Make sure that both phishing and high confidence phishing messages are set to Quarantine message.
- Save.

References:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-policies-configure?view=o365-worldwide

Configure self-service password reset is set to require at least two methods

Self-service password reset (SSPR) in Azure AD is a feature that allows users to reset their own passwords without the need for IT support. It allows users to reset their passwords by providing answers to security questions, using a one-time code sent to their registered phone number or email address, or using a third-party authentication provider.

When set to one, an attacker with the knowledge of just one method, such as a security code from SMS or e-mail, or a security question, can perform account takeover. We recommend setting the number of required methods to at least two.

To set the number of required methods to two:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Under Manage, select Users.
- Under Manage, select Password reset.

- Under Manage, select Authentication methods.
- Set Number of methods required to reset to 2.
- Select intended methods.
- Save.

References:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Enable notifications for users and admins on password reset

We recommend keeping notifications for password reset enabled for both users and admins. If enabled, users will get a notification when their own password has been reset via the Self-Service Password Reset.

If enabled for admins, global administrators will receive an e-mail when other administrator reset their own password. This can be an indicator of malicious activity and should be investigated.

To enable notifications for both admins and users:

- Log in to https://portal.azure.com as a Global Administrator.
- Search for Azure Active Directory.
- Under Manage, select Users.
- Under Manage, select Password reset.
- Under Manage, select Notifications.
- Enable Notify users on password resets and Notify all admins when other admins reset their password.
- Save.

Ensure DKIM, DMARC and SPF are enabled

DKIM, DMARC and SPF help protect against email spoofing and phishing attacks. DKIM (DomainKeys Identified Mail) is an email authentication protocol that uses digital signatures to verify the authenticity of emails. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps protect against phishing attacks by verifying the sender's identity. SPF (Sender Policy Framework) is an email authentication protocol that helps protect against spoofing attacks by verifying the sender's IP address. Together, these protocols help ensure that emails sent from a domain are legitimate and not spoofed or phished.

To verify whether SPF is enabled:

- Run the following command in CMD (replace domain1.com with your custom domain):

  nslookup -type=txt domain1.com

- Ensure that the value contains: include:spf.protection.outlook.com

To enable SPF:

- Follow the steps in Microsoft documentation: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-spf-configure?view=o365-worldwide

To verify whether DKIM is enabled:

- Log in to https://security.microsoft.com/dkimv2 as a Global Administrator.
- Click on the domain you with to verify.
- Verify whether Sign messages for this domain with DKIM signatures is enabled.

To enable DKIM:

- Log in to https://security.microsoft.com/dkimv2 as a Global Administrator.
- Click on the domain you with to configure.
- Click on Create DKIM keys.
- Publish the CNAME records to your DNS service provider.
- Return to https://security.microsoft.com/dkimv2 and click on Sign messages for this domain with DKIM signatures.

To verify whether DMARC is enabled:

- Run the following command in CMD (replace domain1.com with your custom domain):

  nslookup -type=txt _dmarc.domain1.com

- Ensure that a policy exists that starts with v=DMARC1.

To enable DMARC:

- Follow the steps in Microsoft documentation: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dmarc-configure?view=o365-worldwide#step-4-form-the-dmarc-txt-record-for-your-domain

References:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-spf-configure?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dkim-configure?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dmarc-configure?view=o365-worldwide

OFFICE 365 MONITORING

Security monitoring is important because it helps organizations detect and respond to cyber threats in a timely manner. Monitoring for any suspicious activity should be done on a regular basis, ideally every day. It is important to monitor for any suspicious activity or changes in the system, as well as to ensure that all security measures are up to date and effective.

This chapter contains a guide to implement an effective monitoring inside Office 365 / Azure AD for SMBs.

Monitor access to management consoles

Attackers can abuse management consoles in Azure AD and Office 365 by gaining unauthorized access to the consoles, manipulating settings, and deleting or modifying data. Even if access to management consoles is restricted by security policies, you should monitor for any failed attempts.

Suspicious sign-ins to management consoles can be monitored using the Sign-In logs in Azure AD:

- Log in to https://portal.azure.com as a Global Administrator, Security Administrator or Security reader.
- Search for Azure Active Directory.
- Under Monitoring, select Sign-in logs.
- Click on Add filters and add a filter names Application.
- Monitor the following application names:
    - Azure Portal
    - Microsoft Azure CLI
    - Azure Active Directory PowerShell
    - Microsoft Azure PowerShell
    - Graph Explorer
    - Azure DevOps
    - ACOM Azure Website
- Any attempted logins should be investigated.

Even with access to management portals blocked with CA, login attempts should be investigated in-depth. We recommend examining the Authentication Details and Conditional Access tab. Usually, conditional access policies are only validated if provided a correct password. This means that login attempts to management portals that had been blocked by CA means a potential attacker activity.

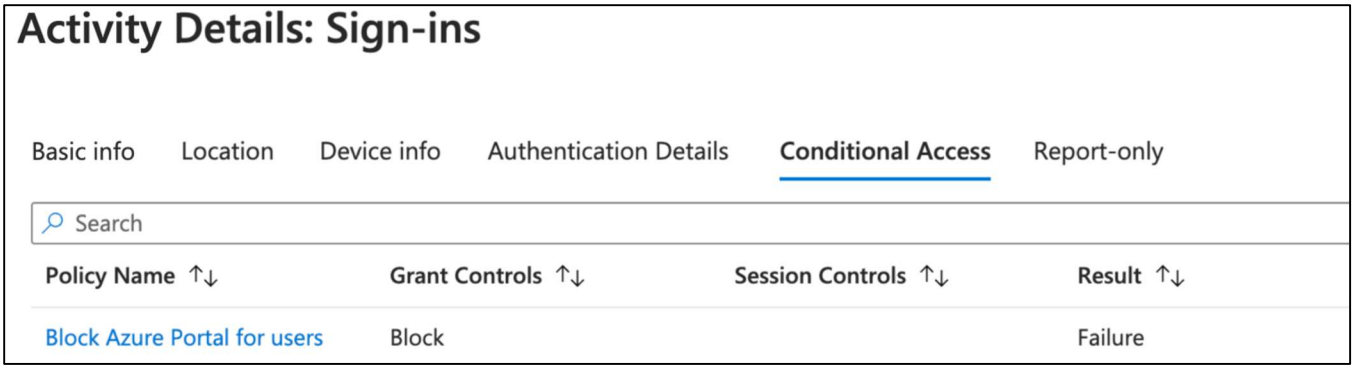

Image 2. Access to Azure Portal blocked by conditional access. Still, the account is likely compromised.

References:

References:

https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Monitor access from unusual/untrusted countries

Any logins from unusual countries, or untrusted countries should be verified. We recommend contacting the user, or their supervisor, and verifying whether the activity is legitimate or not.

Suspicious sign-ins can be monitored using the Sign-In logs in Azure AD:

- Log in to https://portal.azure.com as a Global Administrator, Security Administrator or Security reader.
- Search for Azure Active Directory.
- Under Monitoring, select Sign-in logs.
- Click on Download and download the data in CSV format.
- Filter out usual locations, such as your local ISP, or the company' IP, in spreadsheet editor.

References:

https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Investigate Office 365 Cloud Apps Security Apps alerts

Office 365 Cloud Apps Security is a cloud-based security solution that provides advanced security and compliance capabilities for Office 365. It helps organizations protect their data and users from threats, detect malicious activity, and enforce compliance policies. Office 365 Cloud Apps Security can help your organization automatically detect suspicious user activities, such us impossible travel, unusual sign-ins, or a potential ransomware activity.

Office 365 Cloud Apps Security is available at https://portal.cloudappsecurity.com/.

You need at least Office 365 E5, Microsoft 365 E5, or Microsoft 365 A3 license to utilize Cloud App Security.

References:

https://learn.microsoft.com/en-us/defender-cloud-apps/

Monitor for credential leaks

Credential leak monitoring is the process of actively monitoring the internet for leaked or stolen credentials. This includes monitoring websites, dark web forums, and other sources of leaked information. The goal of credential leak monitoring is to detect and respond to any unauthorized access to sensitive data, such as usernames, passwords, and other confidential information. This helps organizations protect their data and reduce the risk of a data breach.

You can use services, such as have i been pwned, to get leak notifications for your domain.

RESPONDING TO ACCOUNT COMPROMISE

Revoke access

It is important to quickly revoke access to compromised accounts to protect the security of the system and the data stored within it. By quickly revoking access, the attacker's access is limited, and the risk of further damage is minimized.

When responding to a serious cybersecurity incident, we recommend contacting a company specializing in incident response. IstroSec specialists are experienced in dealing with BEC incident both within client's on-premise infrastructure and cloud (Office 365, Gmail, webmail accounts). They know the tactics, techniques and procedures employed by attackers and have the knowledge necessary to mount a quick, effective and complex reaction.

In case you have been targeted by BEC, or other cybersecurity incident, contact us 24/7 on phone number +421 917 699 002 or by sending an email to incident@istrosec.com

Revoke user access in cloud-only environments (GUI):

- Disable the user in Azure A:
  - Log in to https://portal.azure.com as a Global Administrator or Security Administrator.
  - Search for Azure Active Directory.
  - Under Manage, select Users.
  - Search for the user you wish to disable.
  - Click on Edit properties.
  - Choose the Settings tab.
  - Uncheck Account enabled.
  - Save.
- Revoke the user's Azure AD tokens:
  - Log in to https://portal.azure.com as a Global Administrator or Security Administrator.
  - Search for Azure Active Directory.
  - Under Manage, select Users.
  - Search for the user.
  - Click on Revoke sessions.
- Disable user's devices:
  - Log in to https://portal.azure.com as a Global Administrator or Security Administrator.
  - Search for Azure Active Directory.
  - Under Manage, select Users.
  - Search for the user.
  - Select users' devices and click on Disable.

Revoke user access in hybrid environments:

- Disable the user in on-prem Active Directory:

  Disable-ADAccount -Identity johndoe

- Reset the user's password **twice** in on-prem Active Directory (replace newPassword with a new password of choice):

  Set-ADAccountPassword -Identity johndoe -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "newPassword" -Force)

  Set-ADAccountPassword -Identity johndoe -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "newPassword" -Force)

- Disable the user in Azure AD:
  Set-AzureADUser -ObjectId johndoe@contoso.com -AccountEnabled $false

- Revoke the user's Azure AD tokens:
  Revoke-AzureADUserAllRefreshToken -ObjectId johndoe@contoso.com

- Disable user's devices:
  Get-AzureADUserRegisteredDevice -ObjectId johndoe@contoso.com | Set-AzureADDevice -AccountEnabled $false

References:

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access

LIMITED LIABILITY STATEMENT

Recommendations included in this document are provided as-is. Author does not take responsibility of any inconvenience or business impact caused by inappropriate deployment or enforcement of provided security measures. Adequacy and suitability of individual settings must be assessed by administrator or other relevant employee with deeper knowledge of business and user requirements.