CYBERSECURITY ADVISORY

Microsoft Office 365 Security Recommendations

Last Revised: April 29, 2020 **Alert Code:** AA20-120A

Summary

As organizations adapt or change their enterprise collaboration capabilities to meet "telework" requirements, many organizations are migrating to Microsoft Office 365 (O365) and other cloud collaboration services. Due to the speed of these deployments, organizations may not be fully considering the security configurations of these platforms.

This Alert is an update to the Cybersecurity and Infrastructure Security Agency's May 2019 Analysis Report, AR19-133A: Microsoft Office 365 Security Observations <https://www.us-cert.gov/ncas/analysis-reports/ar19-133a>, and reiterates the recommendations related to O365 for organizations to review and ensure their newly adopted environment is configured to protect, detect, and respond against would be attackers of O365.

Technical Details

Since October 2018, the Cybersecurity and Infrastructure Security Agency (CISA) has conducted several engagements with customers who have migrated to cloud-based collaboration solutions like O365. In recent weeks, organizations have been forced to change their collaboration methods to support a full “work from home” workforce.

O365 provides cloud-based email capabilities, as well as chat and video capabilities using Microsoft Teams. While the abrupt shift to work-from-home may necessitate rapid deployment of cloud collaboration services, such as O365, hasty deployment can lead to oversights in security configurations and undermine a sound O365-specific security strategy.

CISA continues to see instances where entities are not implementing best security practices in regard to their O365 implementation, resulting in increased vulnerability to adversary attacks.

Mitigations

The following list contains recommended configurations when deploying O365:

Enable multi-factor authentication for administrator accounts: Azure Active Directory (AD) Global Administrators in an O365 environment have the highest level of administrato privileges at the tenant level. This is equivalent to the Domain Administrator in an on-premises AD environment. The Azure AD Global Administrators are the first accounts created so that administrators can begin configuring their tenant and eventually migrate their users. Multi-factor authentication (MFA) is not enabled by default for these accounts. Microsoft has moved towards a “Secure by default” model, but even this must be enabled by the customer. The new feature, called “Security Defaults,”[1] <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults> assists with enforcing administrators’ usage of MFA. These accounts are internet accessible because they are hosted in the cloud. If not immediately secured, an attacker can compromise these cloud-based accounts and maintain persistence as a customer migrates users to O365.

Assign Administrator roles using Role-based Access Control (RBAC): Given its high level of default privilege, you should only use the Global Administrator account when absolutely necessary. Instead, using Azure AD's numerous other built-in administrator roles instead of the Global Administrator account can limit assigning of overly permissive privileges to legitimate administrators.[2] <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles> Practicing the principle of "Least Privilege" can greatly reduce the impact if an administrator account is compromised.[3] Always assign administrators only the minimum permissions they need to do conduct their tasks.

Enable Unified Audit Log (UAL): O365 has a logging capability called the Unified Audit Log that contains events from Exchange Online, SharePoint Online, OneDrive, Azure AD, Microsoft Teams, PowerBI, and other O365 services.[4] An administrator must enable the Unified Audit Log in the Security and Compliance Center before queries can be run. Enabling UAL allows administrators the ability to investigate and search for actions within O365 that could be potentially malicious or not within organizational policy.

Enable multi-factor authentication for all users: Though normal users in an O365 environment do not have elevated permissions, they still have access to data that could be harmful to an organization if accessed by an unauthorized entity. Also, threat actors compromise normal user accounts in order to send phishing emails and attack other organizations using the apps and services the compromised user has access to.

Disable legacy protocol authentication when appropriate: Azure AD is the authentication method that O365 uses to authenticate with Exchange Online, which provides email services. There are a number of legacy protocols associated with Exchange Online that do not support MFA features. These protocols include Post Office Protocol (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transport Protocol (SMTP). Legacy protocols are often used with older email clients, which do not support modern authentication. Legacy protocols can be disabled at the tenant level or at the user level. However, should an organization require older email clients as a business necessity, these protocols will presumably not be disabled. This leaves email accounts accessible through

the internet with only the username and password as the primary authentication method. One approach to mitigate this issue is to inventory users who still require the use of a legacy email client and legacy email protocols and only grant access to those protocols for those select users. Using Azure AD Conditional Access policies can help limit the number of users who have the ability to use legacy protocol authentication methods. Taking this step will greatly reduce an organization's attack surface.[5] <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

Enable alerts for suspicious activity: Enabling logging of activity within an Azure/0365 environment can greatly increase the owner's effectiveness of identifying malicious activity occurring within their environment and enabling alerts will serve to enhance that. Creating and enabling alerts within the Security and Compliance Center to notify administrators of abnormal events will reduce the time needed to effectively identify and mitigate malicious activity.[6] At a minimum, CISA recommends enabling alerts for logins from suspicious locations and for accounts exceeding sent email thresholds.

Incorporate Microsoft Secure Score: Microsoft provides a built-in tool to measure an organization's security posture with respect to its O365 services and offer enhancement recommendations.[7] These recommendations provided by Microsoft Secure Score do NOT encompass all possible security configurations, but organizations should still consider using Microsoft Secure Score because O365 service offerings frequently change. Using Microsoft Secure Score will help provide organizations a centralized dashboard for tracking and prioritizing security and compliance changes within O365.

Integrate Logs with your existing SIEM tool: Even with robust logging enabled via the UAL, it is critical to integrate and correlate your O365 logs with your other log management and monitoring solutions. This will ensure that you can detect anomalous activity in your environment and correlate it with any potential anomalous activity in O365.[8]

Solution Summary

CISA encourages organizations to implement an organizational cloud strategy to protect their infrastructure assets by defending against attacks related to their O365 transition and better securing O365 services.[9] Specifically, CISA recommends that administrators implement the following mitigations and best practices:

- Use multi-factor authentication. This is the best mitigation technique to protect against credential theft for O365 administrators and users.
- Protect Global Admins from compromise and use the principle of “Least Privilege.”
- Enable unified audit logging in the Security and Compliance Center.
- Enable Alerting capabilities.
- Integrate with organizational SIEM solutions.
- Disable legacy email protocols, if not required, or limit their use to specific users.

References

[1] Azure AD Security Defaults <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

[2] Azure AD Administrator roles <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

[3] Protect Global Admins

[4] Unified audit log

[5] Block Office 365 Legacy Email Authentication Protocols <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

[6] Alert policies in the security and compliance center

[7] Microsoft Secure Score

[8] SIEM integration with Office 365 Advanced Threat Protection

[9] Microsoft 365 security best practices

Revisions

April 29, 2020: Initial Version

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

Give Feedback