THE
NATIONAL LAW REVIEW

US Government Recommends Office 365 Security Advice including the use of MFA (Multi-Factor Authentication)!

FOLEY & LARDNER LLP

Article By
Peter Vogel
Foley & Lardner LLP
Legal News Alert

- Communications, Media & Internet
- Administrative & Regulatory

- All Federal

Friday, May 24, 2019

Bleepingcomputer.com reported that the "Cybersecurity and Infrastructure Security Agency (CISA) issued a set of best practices designed to help organizations to mitigate risks and vulnerabilities associated with migrating their email services to Microsoft Office 365." The May 13, 2019 report entitled "U.S. Govt Issues Microsoft Office 365 Security Best Practices" included these following examples of Microsoft Office 365 configuration vulnerabilities in its AR19-133A analysis report from CISA:

Multi-factor authentication for administrator accounts not enabled by default: Azure Active Directory (AD) Global Administrators in an O365 environment have the highest level of administrator privileges at the tenant level. Multi-factor authentication (MFA) is not enabled by default for these accounts.

Mailbox auditing disabled: O365 mailbox auditing logs actions that mailbox owners, delegates, and administrators perform. Microsoft did not enable auditing by default in O365 prior to January 2019. Customers who procured their O365 environment before 2019 had to explicitly enable mailbox auditing.

Password sync enabled: Azure AD Connect integrates on-premises environments with Azure AD when customers migrate to O365. If this option is enabled, the password from on-premises overwrites the password in Azure AD. In this particular

situation, if the on-premises AD identity is compromised, then an attacker could move laterally to the cloud when the sync occurs.

Authentication unsupported by legacy protocols: Azure AD is the authentication method that O365 uses to authenticate with Exchange Online, which provides email services. There are a number of protocols associated with Exchange Online authentication that do not support modern authentication methods with MFA features. Taking this step will greatly reduce the attack surface for organizations.

Given the widespread use of Office365 this is critical advice!

Source URL: https://www.natlawreview.com/article/us-government-recommends-office-365-security-advice-including-use-mfa-multi-factor