PUBLICATION

Department of Homeland Security Issues Report on Microsoft Office 365

Authors: Alisa L. Chestler
May 15, 2019

Organizations and their legal departments continue to deal with the repercussions of email compromises. Regardless of whether your organization is considering migration of email services to Microsoft Office 365 (O365) or other cloud services, you must be aware of certain vulnerabilities and risks that are inherent to the use of email. While there are benefits to maintaining email services in the cloud, there are also risks when an organization does not adequately monitor security configurations in place during and after the migrations.

On May 13, 2019, the Cybersecurity and Infrastructure Security Agency (CISA) component of the U.S. Department of Homeland Security (DHS) issued an Analysis Report (AR19-133A) which highlights certain security risks associated with email migration to the cloud and recommendations for mitigating the risks. Specifically, CISA describes the following risks of which organizations and their third-party vendors should be aware and should address proactively:

1. **Multi-factor authentication (MFA) is not enabled by default for administrator accounts**. MFA must be enabled proactively and failing to do so can leave these accounts with the highest level of privileges exposed to Internet access. Note, we recommend all users have MFA enabled, as the requirement is one of the better defenses and the use of MFA is not as onerous as users anticipate.

2. **Relevant mailbox auditing logs may not be enabled**. While Microsoft enabled audit logs by default in January 2019, organizations whose environments were established before this date must have explicitly enabled the mailbox auditing. Further, unified audit logs, which often provide detailed logging for events in various components of the tenant, still must be enabled proactively by an administrator. This is a very important tool for organizations to utilize when an event has occurred; it can be the best evidence that the event did not result in an actual "breach."

3. **Password syncs from the on-premises environment may expose cloud environment**. When migrating to O365, there is an authentication option in Azure AD involving a "Password Sync," which overwrites the password for the cloud environment with the on-premises environment password. Thus, if the credentials for an on-premises account were compromised prior to the migration, the intruder could move laterally to the O365 account after the sync.

4. **Outdated protocols (POP3, IMAP, and SMTP) may be used with older email accounts that do not support modern authentication with MFA**. These outdated protocols should be disabled, if not required, or limited to specific users.

Without careful attention to security configurations prior to and during an email migration, organizations can open themselves up to additional risk of a data breach. If a data breach occurs, organizations may be required to disclose the incident to individuals, regulators, and/or the media, and may face lawsuits and/or regulatory fines and penalties. Although the DHS Analysis Report is focused on risks related to email migrations, organizations should assess their security configurations presently. These considerations can improve an organization's security posture even when a migration is not contemplated.

We also encourage our clients to document how the organization addresses these considerations in a written information security program, as many states require such documentation for organizations that maintain personal information on a resident of their state, regardless of whether the organization has a presence in the state or not. We further encourage clients who use third-party vendors for cloud migration services to address these considerations and ensure adequate security is included as an obligation of the vendor in the vendor contract.

If you have any questions regarding these issues or any other cybersecurity or data privacy-related matters, please contact Alisa Chestler or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.