IMPROVING SECURITY FOR MICROSOFT 365®

Mitigating Business Email Compromise (BEC) Issues Related to Insecure Microsoft 365® Environments

Cyber criminals are increasingly using weak Microsoft 365® (formerly called Office 365) security configurations to obtain/falsify the credentials of legitimate organizational users, and then use them to ill effect via ***Business Email Compromise*** (or "BEC") attacks.

BEC attacks tend to involve various types of fraudulent activity, and often include wire fraud where employees are convinced (by email impersonators) to send funds to the bank account of the attacker. These types of incidents represent a continuing source of monetary loss for the victimized companies, as well as their cyber insurance carriers.

Organizations can use the recommendations in this Advisory to harden their Office 365 platform services for improved resistance to BEC attacks.

When your organization moves its traditional in-house IT applications (including email) to a commercial cloud-hosted offering, you need to be keenly aware of the new "division of labor" that exists between your IT administrators and the application-=hosting vendor regarding who is responsible for implementing effective cybersecurity practices. ***A primary responsibility that remains with your team is the proper configuration of end-user account protections and access control requirements.***

Microsoft 365 ("M365") is a popular platform of hosted office applications used by business organizations of all sizes. Microsoft offers a wide range of security configuration options designed to enhance the protection and privacy of company data. Unfortunately, a sizeable percentage of M365 corporate clients fail to properly configure these additional protections.

The frequency and severity of data breaches for companies using M365 have recently become so serious that the U.S. government has issued specific guidance to encourage companies to strengthen their M365 configurations. In direct response to the recent work-from-home trend spawned by the COVID-19 pandemic, the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security has now published eight (8) detailed recommendations. For the full article, please see: https://www.us-cert.gov/ncas/alerts/aa20-120a.

This Advisory provides highlights from the CISA recommendations, along with important additional suggestions from other industry sources.

For Network and System Administrators

1. ***Require Multi-Factor Authentication (MFA) for Administrator Accounts:*** Azure Active Directory Global Administrator accounts are the means by which employee email accounts are migrated from on-premise mail servers to M365. These are ***highly-privileged*** Admin accounts, and the M365 client/tenant ***must turn on multi-factor authentication*** as one of the very first tasks after creating these accounts.

2. ***Assign "Sub" Administrator Roles via "Least Privilege" Principles:*** Role-based access control (RBAC) allows you to allocate narrowly-defined privileges for accounts rather than relying upon the Global Administrator accounts described in (1) above. Make use of temporary and restricted access whenever possible and reevaluate on a day-to-day basis.

3. ***Enable Unified Audit Log (UAL) for All M365 Services:*** The UAL facility allows for collection of a broad variety of event records across most M365 services. The UAL facility should be fully enabled. and event records should be preserved for future examination for at least 90 days.

4. ***Enable Important Mail-Centric Security Features:*** Within the context of your M365 implementation, make sure to configure these three impactful features: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC). These features help guard against fraudulent attempts to manipulate email headers and content.

5. ***Incorporate Microsoft's Secure Score Tool:*** Microsoft understands that clients may not fully implement their recommended security capabilities initially. They created the Microsoft Secure Score tool to encourage clients to see how they measure up against contemporary security expectations. In sharing with clients their current levels of protection, Microsoft continues to offer appropriate suggestions to help clients advance along a cybersecurity "maturity curve." Organizational clients would be well advised to enable the Secure Score tool and take notice of the suggestions provided.

6. ***Learn How to Map Microsoft UAL Alerts Against Your Existing SIEM Platform Messages:*** You may rely upon a commercial security information and event management (SIEM) platform as your "eyes and ears" to watch for suspicious activity patterns involving your IT assets. Microsoft's UAL alerts can add to your overall perspective and understanding in this area – and so it is vital that you incorporate UAL alerts into your overall SIEM-centric approach to detecting suspicious activities.

7. ***Ensure That You Have Maximized the Use of Email Blocking for Anti-Phishing/Anti-Spoofing Threats:*** As an additional layer of protection, Administrators should evaluate and implement contemporary solutions (beyond the native capabilities included within M365) that can also block incoming anti-phishing/anti-spoofing threats.

8. ***Eliminate Unnecessary Services at Your Firewall, Especially Microsoft's Remote Desktop Protocol (RDP) Service:*** Beyond the M365 context, it is important to ensure that your perimeter firewalls are tightened as much as possible. As a key example, the public-facing availability of Microsoft's Remote Desktop Protocol (RDP) is no longer considered a prudent practice. People who need access to RDP as part of a necessary business requirement should do so by way of a secure VPN connection.

For (or On Behalf of) End Users:

1. ***Require Multi-Factor Authentication (MFA) for All Users:*** MFA is the leading tool in repelling the efforts of malicious actors who are attempting to gain access to employee accounts so that they can launch their attacks under the guise of "legitimate" users.

2. ***Disable Legacy Protocol Authentication Where Possible:*** Over several decades, users have relied upon older POP3, IMAP, and SMTP-based protocols for sending/receiving their email. To the extent possible, these older methods of mail transport should be eliminated in favor of more contemporary Azure Active Directory ("AD") authentication methods.

3. ***Enable "Suspicious Activity" Alerts:*** Additional logging of user activity within M365's Security Compliance Center can help investigators' efforts to identify malicious attempts to compromise the environment through review of logins from unusual locations and for email-sent volumes that exceed normal thresholds.

4. ***Prohibit the Automatic Forwarding of Email to External Addresses:*** Allowing employees to automatically forward their company email to external (and usually personal) accounts has never been a good idea. In the present environment, that practice becomes even more dangerous and should be eliminated.

5. ***Add an "External Source Email" Banner for Incoming Emails Originating from Outside the Organization:*** Alerting your employees that individual pieces of email arrived in their inbox from outside the company helps them focus on the trustworthiness of the named senders and the associated contents.

Don’t Forget the Non-Technical Practices!

Reducing the risk of Business Email Compromise should not rely solely upon technology-based protections. Old-fashioned common sense and reasonable business procedures still play a very important role in keeping cyber losses to a minimum. When a non-trivial amount of money is involved in a requested transaction, employees should pick up the phone and call the requester to verify the transfer request.

Email communications should never be considered 100% trustworthy – even with the benefit of Microsoft 365’s powerful security features and related network security components. A healthy sense of skepticism when conducting business in the electronic age will pay dividends.

Thank you very much for your attention to this NetDiligence Security/Privacy Advisory, and please do not hesitate to reach out to us (at management@netdiligence.com) for further advice and assistance with your cyber risk management efforts!