GIBRALTAR®
DRIVING DIGITAL TRANSFORMATION

Top 10 Action Items to Improve the Security Posture of Your Microsoft 365 Environments

Companies are seeing ransomware on the rise like never before, with a 300% increase in just one year - and small- to medium-scale businesses bear the greatest risk. Fortunately, experienced security experts at Gibraltar have devised ten critical tips to keep Microsoft 365 environments safe from cyber-attack during this turbulent time of hybrid workforces and rapid advancement in technology.

Action Item #1: Multi-Factor Authentication

Strengthen the security of your Microsoft 365 accounts with Multi-factor Authentication. By verifying and confirming a secondary form of identification in addition to your username & password, MFA serves as an added layer of protection against unauthorized access to confidential data. Protect yourself - it's easy and essential.

- **Offer Acceptance and Negotiation**

Action Item #2: Configure Strong Password and Password Expiration Policies

Many people believe their password is safe as long as they're not leaving their credentials written down somewhere. Unfortunately, that couldn't be further from the truth. Microsoft 365 accounts are being hacked by a method called password spraying, a high-volume attack in which the person carrying out a cyber-attack takes one (often weak or common) password and tests it against as many accounts as they can.

- **Set strong password parameters and strict expiration policies.**

Action Item #3: Separate Global Admin Accounts from End User Accounts

Each individual on your team should have their own credentials based on the information and authorizations they should need to execute their own job function. However, disjoining your admin and end user accounts specifically help limit the amount of access a hacker has even if they do breach your Microsoft 365 environment.

- **Separate all administrative accounts from end-user accounts.**

Action Item #4: Implement Conditional Access Policies

Conditional access policies help ensure safe sign-ins by verifying the location and device of the user before granting access. Your conditional access policy may do one or all of the following:

1. Block unsupported locations
2. Block unsupported devices
3. Restrict access to critical data to only LAN

- **Implement conditional access policies based on your team's needs.**

Action Item #5: Configure Audit Log and Alert Policy

The built in audit log and alert settings are a feature we highly recommend taking advantage of. Alert policies can detect suspicious and unusual activity in your Microsoft 365 environment, such as a file shared with a user outside of your organization, or 1000 files downloaded within a 5-minute time frame. These logs and the alerts that they generate are a great added layer of protection in monitoring and securing your data.

- **Fine-tune your audit log and alert settings**

Action Item #6: Block Legacy Authentication

"Legacy authentication" is a term Microsoft sometimes uses to describe basic authentication, as opposed to the term "modern authentication" which provides more security and capabilities. The trouble is, only modern authentication can support multi-factor authentication, as we discussed earlier as a vital security measure. With legacy authentication, MFA can't be effectively enforced, which leaves your data vulnerable to an attack.

- **Block Legacy Authentication**

Action Item #7: Block Sign in for Shared Mailboxes

A shared mailbox is a mailbox that is shared by a group of designated users in Microsoft 365 based on the permissions granted. When you create a shared mailbox in Exchange Online, a password is generated for the mailbox at the back end. This password can then be used as valid credentials for access to the shared mailbox, leaving it at risk for an attack. Luckily, this shared mailbox can be limited to permissions use only while effectively blocking that automated password.

- **Block Shared Mailbox Sign-In**

Action Item #8: Configure SPF, DKIM, and DMARC for Anti Spoofing Email

Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC), are considered by many to be the three pillars of email authentication. These three criteria help limit the chances that an unauthorized sender can access your domain without your consent.

- **Configure SPF, DKIM, and DMARC to Stop Email Spoofing**

Action Item #9: Disable Forwarding to Remote Domains

Although there are legitimate reasons to utilize auto-forwarding of business email, most of the time the most secure option is to disable the function altogether. Hackers, using phishing attacks to gain access to a user's mailbox, can use auto-forwarding settings to forward emails to an outside address. This method ensures that through only one entrance to your system, they can continue to receive your most sensitive information, delivered directly to their inbox.

- **Disable Forwarding to Remote Domains**

Action Item #10: Revisit OneDrive/SharePoint External Collaboration and Governance Settings

OneDrive and SharePoint are excellent tools for collaborating with your team, especially for remote or hybrid companies. However, hackers are easily taking advantage of a lack of governance settings in your environment. By limiting access to specific users, you can ensure that your information isn't accidentally shared with an unauthorized account, but also limit the potential access points for someone attempting to hack your system.

- **Secure External Collaboration Settings**

Next Steps

To learn more about protecting your Microsoft 365 environment from cyber-attack, book a call with the Gibraltar Microsoft Professional Services Team at **GibraltarSolutions.com**.