Microsoft 365 Security Recommendations

Owner: Service Manager

Introduction: Below is a list of best practice changes we recommend that all clients make to their Microsoft 365 tenant to improve the security of their accounts and data.

Contents

Below is a list of settings that we recommend changing for all companies using Microsoft 365.

These setting ensure that our customers can comfortably operate their business without the looming threat of a security breach and data loss.

Email Security

- **Raise the level of protection against malware in mail**
  - WHAT - This setting enabled the “Common Attachment Types Filter” in the Anti-Malware setting to block a range of malicious file types sent as attachments.
  - WHY - Blocking potentially malicious attachments from being sent through emails can help to eliminate malware that may pass through the antivirus scanners
  - IMPACT - Users may not be able to receive some attachments, however these attachments are typically not files used in a law firm.

- **Protect against ransomware / reference**
  - WHAT - This change extends on the common attachments filter by creating a series of custom rules that warns or block additional file types when they are sent as attachments in emails.
  - WHY - Blocking potentially malicious attachments from being sent through emails can help to eliminate malware that may pass through the antivirus scanners
  - IMPACT - The files that are blocked are regularly used to send malware and would not typically be sent in a business environment (for example executables). Files that may contain malware but may also be legitimate are set to warn only.

- **Stop auto-forwarding for email**
    - WHAT - The ability for users to forward their email account to external recipients is disabled.
    - WHY - When an account is compromised often the offender will set up auto forwarding to allow them to gain access to the account even if the password is changed.
    - IMPACT - There should be no user impact in most situations as users can still forward their emails to internal recipients. There are potential issues where external applications or vendors use the email forwarding option to receive legitimate emails.

User Identity Protection

- **Enable users to reset their own password**
    - WHAT - When users sign in they are prompted for additional account details (secondary email, mobile number etc) to enable them to verify their own identity if they forget their password.
    - WHY - This allows users to get back into their account quickly or outside of business hours. It also standardises the verification of identity methods.
    - IMPACT - If you are in a hybrid mode or syncing users passwords from on premise active directory then an Azure AD Premium license is required.

- **Set password to never expire**
    - WHAT - Disable the password expiration policy so that users passwords do not expire every 90 days.
    - WHY - Research suggests that requiring users to regularly change their passwords results in them choosing easy passwords or re-using passwords across multiple systems making the passwords easy to guess by hackers.
    - IMPACT - This policy should only be implemented with MFA or security defaults enabled. The only impact to this policy is that users will not be required to change their passwords every 90 days and can instead choose a complex password that is also easy to remember.

- **Enforce multi-factor authentication (MFA)**
    - WHAT - Enable the Microsoft Security Defaults which enforced users to setup MFA using their smartphone. When a user logs into a new device or accesses a privileged service they will be prompted to approve the request on their phone.
    - WHY - Microsoft research suggests that enabling MFA can block over 99.9% of account compromise attacks and using the Security Defaults is the easiest way for organisations to implement MFA. For more complex environments Conditional Access can be used instead of Security Defaults which allows additional customisation.
    - IMPACT - MFA is a lot easier than you think. Users will be required to setup the Microsoft Authenticator application on their smartphone and link it to their account. When they login to a new devoice they will need to approve their login on their smartphone so they will need to keep their smartphone handy. Security Defaults also blocks legacy applications that cannot authenticate with a modern authentication protocol. This may impact some old systems that rely on IMAP or POP3 access to mailboxes.

- **Use dedicated admin accounts**
    - WHAT - Dedicated admin accounts should be used for access to the Microsoft 365 admin portal and the accounts should only be used when specifically required. Where we maintain an a Global Admin account for a customers tenant the customer still controls and manages their own admin account.
    - WHY - Dedicated admin accounts should be used that are also not used to run applications or browse the internet. This minimises the impact of a hacker getting access to the admin credentials if a computer is compromised.
    - IMPACT - There is minimal impact to users. A user with admin access needs to authenticate with a different username and password when admin access is required.

SharePoint Online

- **Set external sharing level to new and existing guests**
    - WHAT - This setting disabled the option Users can share files and folders using links that don't require sign-in
    - WHY - This prevents users from sharing files externally without any sign in.
    - IMPACT - Files can still be shared with other firms but the recipients need to sign in or provide a verification code for access.

- **Limit sharing of individual sites**
    - WHAT - Store confidential files in their own sites and then restrict sharing of those sites to prevent files being shared externally. For sites that are not restricted set the site sharing so that the entire site can only be shared by the site owner.
    - WHY - This prevents users from accidentally sharing confidential files externally.
    - IMPACT - Files is confidential sites can only be shared with internal staff.