mcrIT Microsoft 365 Security Assessment

Problem Statement

Malicious actors and campaigns target your critical business data. Often organisations consider firewalls as sufficient protection, but often the threat is hidden within the email, a shared link or file, an USB drive or a visitor accessing your WiFi.

Regardless of whether your vital IT are onsite or in the cloud security requires constant monitoring and management to ensure your staff can use the tools and systems in order to perform their tasks consistently, reliably and securely.

So do you know your security posture?:

- Do you have controls in place for Acceptable Use of EndPoint devices?
- Do you have a Zero Trust approach to Security?
- When did you last review your SharePoint Permissions?
- When did you last review your SharePoint Guests, their access and if they have Multifactor Authentication (MFA) Enabled?
- How much time to you spend reviewing your security of your data?
- Do you know where your data is stored and how to recover it?
- How much do you estimate it costs your business if your IT is offline?
- Do you hold backup copies of your emails, shared files and CRM information held in M365 or SaaS platforms?
- Do you have a current view of your IT and Network health, including capacity, maintenance, licencing, performance and availability?

Why use a mcrIT M365 Security Review?

Security is an everyday maintenance activity, and often users think they are working in a secure environment when the security of the business data is at risk from many factors. A Health check will provide:

- Understanding of the security profile, in line with the ASD Essential Eight
- Risk awareness of the M365 environment and end user and company data security.
- Identification of budget and priority actions to remediate and protect the environment.
- Security Awareness - Phishing education for endpoint users

What is Involved?

Our Microsoft Security Engineer will access your M365 tenant (using a read-only access provided by you for the duration of the assessment). There is a 50-point checklist.

The engineer will assess:

- User and Admin accounts in use, the licences used, including Guest and shared accounts
- Identity Management, including conditional Access controls, including Multi-factor authentication
- Document and data management (SharePoint, OneDrive and Email security controls)

What do you get?

mcrIT will provide a Security report that provides:

- An executive summary of the assessment
- A link to the online detailed assessment including the priority of the results
- Information on each check and the recommended action
- A walk-through of the key findings via Teams Meeting
- An estimate of cost to remediate the agreed action items

What does it cost?

The M365 Security Assessment has a value of $5,000.

Any agreed remediation projects will be scoped separately, or you may elect to implement the remediation actions yourselves.

mcr IT