Microsoft 365 Security Deep Dive

Overview

The adoption of Microsoft 365 presents an opportunity for increased creativity, productivity, collaboration, and connectivity for many businesses. Whilst Microsoft 365 can drive innovation and competitive advantage, it is crucial to prioritise the security of your Microsoft 365 tenancy to ensure the protection of confidential, customer, personal, and intellectual information stored in the service.

Given that the Notifiable data breaches report (January to June 2022) published by the Office of the Australian Information Commissioner (OAIC), reported that 25% of cyber incidents in the country arise from stolen or compromised credentials and an additional 26% from phishing attacks, it is crucial to safeguard your Microsoft 365 tenancy with a security review.

Highlights

- **Prioritise** security enhancements
- **Increase** security awareness
- **Minimise** threats
- **Follow** security best practices
- **Improve** your security posture

Safeguard your Microsoft 365 tenancy

The Missing Link's Microsoft 365 Security Deep Dive has been created by our Microsoft 365 Subject Matter Experts (SMEs) utilising their extensive experience of best practice security controls and configurations of Microsoft 365 services.

By carrying out a proactive review, businesses can mitigate security risks caused by common misconfigurations or lacking security controls in Microsoft 365.

Review Approach

The Missing Link's Microsoft 365 Security Deep Dive evaluates the configuration of the following 6 core products:

- Microsoft Entra ID
- Microsoft Purview
- Microsoft Intune
- Microsoft 365 Defender
- Microsoft SharePoint
- Microsoft Teams

Timeline

The Microsoft 365 Security Deep Dive typically takes 2 weeks to complete, broken into the below 3 phases:

Configuration Review

Remote review of Microsoft 365 configurations and settings

Reporting

Creation of report that details findings and recommenations to improve security posture

Presentation

Meeting with SME to present and discuss findings and recommendations

themissinglink®

Deliverables

The Missing Link's SMEs will provide a detailed report that includes the following:

- A summary of all key findings prioritised by severity
- A detailed breakdown of the existing Microsoft 365 security configuration
- A detailed analysis of sensitive data types, over-shared data, external sharing links and shadow users
- Review of Microsoft 365 licensing
- Recommendations to enhance security posture of Microsoft 365 tenancy

Next Steps

Reach out to your Account Manager at The Missing Link to learn more about our Microsoft 365 Security Deep Dive or send an email to contactus@themissinglink.com.au.

Terms and Conditions

- All services are delivered under The Missing Link's standard Terms and Conditions that are freely available from The Missing Link website at http://www.themissinglink.com.au/terms-and-conditions or by emailing your Account Manager. Please ensure you have read and agreed to these before accepting any statements of work or quotations for these services.
- All activities are completed remotely.
- Presentation of findings and recommendations will be done remotely via Microsoft Teams.
- The Missing Link's Microsoft 365 Security Deep Dive includes the review of a single Microsoft 365 tenancy. A review of multiple tenancies can be provided on request.
- The Missing Link's Microsoft 365 Security Deep Dive will reduce the risk of your Microsoft 365 tenancy being compromised by implementing best practices, but it does not provide guarantees that comprises won't happen.
- The security of the Microsoft 365 tenancy remains the responsibility of the Client.
- The above terms and conditions are advisory only. A full list of our terms and conditions, assumptions and exclusions can be provided on request.