

MICROSOFT 365 SECURITY ANALYSIS

Analysis and assessment of the security posture in a Microsoft 365 environment



Improsec delivers an independent security analysis and assessment, providing management and the IT security organization with a clear overview of the basic security controls implemented in Microsoft 365 compared to vendor best practices.

Value

- Analysis and assessment of the security posture in an Office 365 environment
- An evaluation of asset and resource security misconfigurations
- Manage the risks associated with adoption and utilization of Office 365
- Ensure policies and security controls are implemented according to requirements
- Enhance and improve security to protect the Office 365 environment

Product

The deliverable of the analysis is a written report containing the following:

- A non-technical section with an Executive Summary for management and decision makers
- A technical section including detailed observations and tangible recommendations to strengthen the level of security and recommendations on how hardening can be applied

Method

The security assessment is, among other recognized

resources, based on Cloud Security Alliance's (CSA) "Security Guidance for Critical Areas of Focus in Cloud Computing", and "CIS Microsoft 365 Foundations Benchmark". In addition, Microsoft best practice descriptions, guidelines and whitepapers are used in conjunction with the above benchmarking framework, combined with our personal expertise, and tailored to your specific setup and configuration of the deployed Microsoft 365 environment.

- The assessment includes evaluation of:
 - Service misconfigurations (OneDrive, SharePoint, Exchange etc.)
 - Access controls and user permissions (internal / external)
 - Protection of information and data in shared storage solutions
 - Logging, monitoring, and alerting
 - Utilization and configuration of security solutions
 - Collaboration settings and configuration
 - Proper modern security perimeter usage (Conditional Access)
 - Utilization of least privilege targeting security principals

Involvement

The delivery requires minimal involvement of your technical staff.