



CUSTOMER SUCCESS

Your Success
is our Priority

O365 Security Testing

Introduction

When deploying Office 365, default security controls are applied. StarLink's O365 Security testing service is designed to identify any security gaps or vulnerabilities that exist so that O365 can be configured securely in the context of, and explicitly for, the security requirements of individual organisations.

The StarLink Security Test Methodology

StarLink believe that O365 security testing is only beneficial when analysed within the context of each organisation's policies, controls and network structure. StarLink also understand that the security skills and resourcing required to determine the underlying cause of reported vulnerabilities are not always available inside of the organisations that are being tested. Based on this assumption, StarLink include concise remediation advice for each vulnerability uncovered and are happy to discuss each of our findings to ensure that each client receives best value from the Penetration Testing service.

Management Reporting

Following the testing a report is provided which includes; details of all security vulnerabilities discovered and how these vulnerabilities could be combined to achieve a compromise of the system, within the context of business. This debrief is primarily given in a management context, however, where required the consultant will provide a detailed technical insight of the vulnerabilities.

Why StarLink?

StarLink's Information Security Team have vast experience of helping organisations assess the business risks associated with cyber threats and security breaches through the use of best practice information security policies, procedures and expert services.

Our consultants include:

- Cyber Essentials Certified Assessors
- ISO 27001 Auditors (information security standard)
- ISO 22301 Auditors (business continuity standard)
- Certified Ethical Hackers (CEH)



STARLINK PROFESSIONAL SERVICES

O365 Security Testing Deliverables

The default deliverables from StarLink O365 Security Testing are detailed below. Additional requirements can be catered for on request.

Scope of O365 Security Testing Service

The scope of each test will depend on the client's objectives for carrying out the test and in the context of each organisation. The typical scope for the O365 Security Assessment service is shown below:

Web Application Testing

Office 365 applications are tested using the OWASP security risks to ensure that web based configuration is optimal and proper security measures have been applied. OWASP top 10 is a list of the most generous web vulnerabilities and methods to remediate these flaws.

O365 Configuration & Security Checks

- Ensure User and Administrator permissions are applied correctly
- Mobile Devices and Sync'd content offline configuration
- Security Auditing
- External Sharing
- MFA and Cloud App Security checks
- Secure email flow and mailbox auditing
- DLP and customer lockbox
- Office Messaging Encryption (OME)
- Office ATP Email Testing
- Azure Security Center & Penetration Testing
- Audit Controls against NIST_800, ISO27001 & ISO27018

Timescales

There is typically a two week lead time from the initial enquiry, through to delivering the Penetration Testing Service. The report is normally delivered within 5 working days of the tests being completed

Other Services

StarLink's Information Security practice offer a number of valuable certification and enablement services including:

- Cyber Essentials Enablement
- ISO 27001 Auditing
- ISO 22301 Auditing
- Information Security Reviews*



— with —

STARLINK
TRUSTED SECURITY ADVISOR

2 Arlington Square, Bracknell, RG121WA

Tel: +44 1344 747341 | Email: uk@starlinkme.net

www.starlink.uk.com