MICROSOFT AZURE PENETRATION TESTING

Our Azure Penetration testing service identifies cloud misconfigurations and other security issues on your Microsoft Azure infrastructure and provides actionable recommendations to improve your Azure cloud security posture.

External Azure Pentesting

In an external Azure pentest, we emulate an external attacker to:

Identification of
Cloud Assets

Scanning Cloud Assets for
Misconfiguration and
Vulnerabilities

Risk Analysis on
Vulnerabilities Found

MDS (MAUREEN DATA SYSTEMS) utilizes specialized cloud pentesting tools and manual security testing to reveal security issues in your public facing Azure services.

Cloud Security Assessment

Scanning internet-facing cloud resources is a high priority, but a complete cloud security assessment which evaluates the security posture of your Microsoft Azure infrastructure, requires the following steps:

1. Discovery of all internet-facing assets a hacker could find as potential vector into your Azure account

2. Identification of attack surfaces exposed by cloud services and Active Directory (AD) integration

3. Identification of known and common vulnerabilities on internet-facing assets and web applications.

4. Identification of vulnerabilities that can be exploited to increase privileges and gain unauthorized access to other systems, applications, and sensitive data.

5. Verification of findings using manual Azure penetration testing techniques and expert interpretation.

6. Actionable guidance for the remediation of verified vulnerabilities.

Internal Network Pentesting

Testing internal cloud resources from another resource such as a Virtual Machine (VM) enables MDS to emulate an attacker that has gained unauthorized access in your Azure environment.

MDS emulates an insider attacker by acquiring ordinary users' organizational profiles to escalate privileges and access restricted resources in Azure through its management portal or command line interface.

Configurations Review

Our Azure security experts evaluate the configurations of your Azure infrastructure, by performing a comprehensive assessment which adheres to Microsoft cloud security best practices and industry standards such as CIS (Center for Internet Security) Controls. MDS configuration assessment, provides tailored recommendations and actions which will improve the overall security of your Azure tenant and allow your business to broaden your cloud adoption efforts safely.