Internal Health Check

A RICOH Company

Why MTI offers this service

Most organisations understand the dangers posed by external threats to their equipment and services but internal infrastructure is also subject to significant threats, either malicious or accidental, from users located physically or logically within the perimeter defences.

While many cyber threats are activated remotely, organisations also face the danger of being compromised from within. The threat could come from an unauthorised user with physical access to the environment, an authorised user seeking to gain elevated privileges, a successful remote attack attempting to penetrate further into the environment, or malicious access such as a Ransomware attack. It's vital that the security of internal equipment is robust enough to withstand these types of attack.

The Service

Our service is designed to help strengthen the security of your internal network by identifying vulnerabilities where equipment or services could be compromised or breached by an attacker. Our range of tests and reviews provides an overview of the state of your internal network with evidence of the vulnerabilities and weaknesses that need to be addressed.

Our comprehensive report not only identifies potential vulnerabilities but also provides practical solutions to remediate them, ensuring a secure environment for your organisation. You can implement these recommendations on your own or entrust our professional services team, backed by 30 years of expertise, to efficiently and effectively resolve the issues for you.

Stage 1: What we test

Our penetration testing for internal networks covers three main areas.

Internal penetration test: this component seeks to identify vulnerabilities that could be exploited if an attacker gains access to the internal corporate network.

Domain compromise assessment: this component attempts to compromise the Active Directory Domain(s) to gain full access to all hosts and data on the Domain. This serves to provide a larger overview of the environment as a whole.

Password reviews: The password reviews extract the encrypted password file for the Active Directory Domain, separate users into Domain Administrator and standard users and attempt to crack all the passwords.

Stage 2: What the tests identify

Our tests are designed to provide a clear picture of the vulnerabilities and strengths in your internal network.

Internal penetration test: This test usually finds issues in a range of areas including missing operating system patches, missing third party patches (Java, Flash, etc), weak policies applied to operating systems, weak or default credentials, weak encryption standards, unsupported software, incorrect Active Director configuration and insecure working practises by users and IT staff.

Domain compromise assessment: Tests differ depending on the hosts, services and software on the network. Typically we compromise a Domain via a number of issues including missing operating system patches, weak user and domain admin credentials, weak password policies, weak password encryption, weak service permissions and default credentials.

Password reviews: The tests provide detail on all cracked passwords, along with any common conventions used for the passwords. All user accounts associated with passwords stored with weak encryption standards will be listed along with all accounts which have passwords set to not expire.

Stage 3: Reporting

A formal results report on the testing phases will include the Security Assessment's objective, scope, executive summary of findings, risk grading, CVSS scoring, vulnerability description, recommendations, and contact details for the customer and test team, as well as CHECK/CREST/Cyber Scheme consultants' certifications.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Vulnerability Register

To aid with remediation and compliance tracking, MTI will provide an Excel-based Vulnerability Register listing all issues found during manual testing, along with the CVSS scores in a sortable and editable format. Due to the volume of issues usually found, this does not include issues discovered during automated testing.

Outcomes & Benefits:

Our internal health check delivers the following outcomes:

- Provides a thorough examination and test of the internal infrastructure.
- Details issues that comprise a threat to the integrity of the company infrastructure.
- Outlines where elements of the network are configured correctly and securely.
- Provides peace of mind by discovering vulnerabilities and outlining how they can be addressed.

Deliverables of the service

The internal health check service provides:

- A formal report that presents an overview of the network and suggested remediation steps for improvement.
- A report that can be used to justify expenditure to improve infrastructure defences.
- An outline of your path to a more secure environment.
- ·A report which can be submitted to accreditation bodies.
- ·A report which demonstrates your commitment to security to your internal and external customers.

Reports are delivered within 10 working days after completion of all testing. After completion of the testing work, each report is independently reviewed by a member of the technical team to assess technical accuracy and readability of the report.

Why MTI?

MTI is a lifelong member of global cyber security body, CREST, and has been conducting penetration testing on internal infrastructure for more than 20 years. As one of the first companies to provide this service, we have developed a wealth of knowledge and skills in the tactics used by malicious users to gain access to corporate networks. This enables us to identify risks to the business and outline remediation measures to counter those risks.

If you require, our accomplished professional services operation can swiftly and effectively implement these measures, ensuring robust protection for your organisation.

> "Engaging and working with MTI performing our recurring penetration testing was a very smooth experience. The team quickly understood our specific needs, the technical environment, and any specific test scenarios we requested. Good feedback from the consultants during the actual penetration test and a very professional report with vulnerabilities in order of priority and suggested corrective measures. All in all a job well done."
>
> Michael Zetterlund
> Chief Product Officer
> Ariane Systems

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation