Interner Health Check

Wieso MTI diesen Service bietet:

Die meisten Organisationen sind sich der Gefahren bewusst, die durch externe Bedrohungen für ihre Geräte und Dienstleistungen entstehen. Allerdings ist auch die interne Infrastruktur erheblichen Bedrohungen ausgesetzt, sei es absichtlich oder versehentlich, von Benutzern innerhalb der Perimeterverteidigungen, sowohl physisch als auch logisch.

Während viele Cyberbedrohungen remote aktiviert werden, besteht auch die Gefahr, von innen kompromittiert zu werden. Diese Bedrohung kann von einem unbefugten Benutzer mit physischem Zugang, einem autorisierten Benutzer auf der Suche nach erweiterten Berechtigungen, einem erfolgreichen Remote-Angriff, der tiefer in die Umgebung eindringt, oder böswilligem Zugriff wie einem Ransomware-Angriff ausgehen. Daher ist es entscheidend, dass die Sicherheitsvorkehrungen für interne Geräte stark genug sind, um diesen Angriffen standzuhalten.

Der Service

Unser Service wurde entwickelt, um die Sicherheit Ihres internen Netzwerks zu stärken, indem er Schwachstellen identifiziert, bei denen Geräte oder Dienstleistungen von einem Angreifer kompromittiert oder gefährdet werden könnten. Unsere Palette von Tests und Bewertungen bietet einen Überblick über den Zustand Ihres internen Netzwerks mit Nachweisen von Schwachstellen, die behoben werden müssen.

Unser umfassender Bericht identifiziert nicht nur potenzielle Schwachstellen, sondern bietet auch praktische Lösungen zu ihrer Behebung, um eine sichere Umgebung für Ihre Organisation zu gewährleisten. Sie können diese Empfehlungen eigenständig umsetzen oder unser professionelles Service-Team in Anspruch nehmen, das auf 35 Jahre Erfahrung zurückgreift, um die Probleme effizient und wirksam für Sie zu lösen.

Stufe 1: Was wir testen:

Unsere Penetrationstests für interne Netzwerke umfassen drei Hauptbereiche:

Interner Penetrationstest: Dieser Bestandteil zielt darauf ab, Schwachstellen zu identifizieren, die ausgenutzt werden könnten, falls ein Angreifer Zugang zum internen Firmennetzwerk erhält.

Interner Penetrationstest:

Dieser Bestandteil zielt darauf ab, Schwachstellen zu identifizieren, die ausgenutzt werden könnten, falls ein Angreifer Zugang zum internen Firmennetzwerk erhält.

Domain-Kompromissbewertung:

Dieser Bestandteil versucht, die Active Directory-Domäne(n) zu kompromittieren, um vollen Zugriff auf alle Hosts und Daten in der Domäne zu erlangen. Dies dient dazu, einen umfassenderen Überblick über die gesamte Umgebung zu bieten.

Passwortüberprüfungen:

Die Passwortüberprüfungen extrahieren die verschlüsselte Passwortdatei für die Active Directory-Domäne, trennen Benutzer in Domänenadministratoren und Standardbenutzer auf und versuchen, alle Passwörter zu entschlüsseln.

Stufe 2: Was die Tests ausmacht:

Unsere Tests sind darauf ausgelegt, ein klares Bild der Schwachstellen und Stärken in Ihrem internen Netzwerk zu liefern.

Interner Penetrationstest: Identifiziert typischerweise Probleme wie fehlende Betriebssystem-Patches, Schwächen bei Drittanbieter-Patches (Java, Flash, etc.), unsichere Betriebssystemrichtlinien, schwache Zugangsdaten, unsichere Verschlüsselungsstandards, nicht unterstützte Software, inkorrekte Active Directory-Konfiguration und unsichere Arbeitspraktiken von Benutzern und IT-Personal.

Domain-Kompromissbewertung: Die Tests variieren je nach Hosts, Diensten und Software im Netzwerk. Typischerweise werden Domänen durch verschiedene Probleme kompromittiert, darunter fehlende Betriebssystem-Patches, schwache Zugangsdaten für Benutzer und Domänenadmins, schwache Passwortrichtlinien, unsichere Passwortverschlüsselung, schwache Service-Berechtigungen und Standardzugangsdaten.

Passwortüberprüfungen: Liefern Details zu allen geknackten Passwörtern sowie gängigen Konventionen. Alle Benutzerkonten mit schwachen Verschlüsselungsstandards und Konten, bei denen Passwörter auf "Niemals ablaufen" eingestellt sind, werden aufgelistet.

Kontaktieren Sie MTI
T: +49 (0) 6122 9950
E: deinfo@mti.com
W: de.mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Stufe 3: Reporting

Ein formaler Ergebnisbericht zu den Testphasen wird die Zielsetzung der Sicherheitsbewertung, den Umfang, die Zusammenfassung der Ergebnisse, die Risikobewertung, die CVSS-Bewertung, die Beschreibung der Schwachstellen, Empfehlungen und Kontaktdaten für den Kunden und das Testteam sowie Zertifizierungen der CHECK/ CREST/ Cyber-Scheme-Berater umfassen.

Schwachstellenregister

Zur Unterstützung bei der Behebung und Verfolgung der Compliance wird MTI ein Excel-basiertes Schwachstellenregister bereitstellen, das alle während manueller Tests gefundenen Probleme auflistet, zusammen mit den CVSS-Bewertungen in einem sortierbaren und bearbeitbaren Format. Aufgrund der üblicherweise gefundenen Vielzahl von Problemen umfasst dies nicht die während automatisierter Tests entdeckten Probleme.

Ergebnisse & Vorteile:

Unser interne Health Check liefert die folgenden Ergebnisse:

- Bietet eine gründliche Untersuchung und Prüfung der internen Infrastruktur.
- Erläutert Probleme, die eine Bedrohung für die Integrität der Unternehmensinfrastruktur darstellen.
- Skizziert, wo Elemente des Netzwerks korrekt und sicher konfiguriert sind.
- Bietet Sicherheit, indem Schwachstellen entdeckt und aufgezeigt werden, wie sie behoben werden können.

Warum MTI?

MTI ist lebenslanges Mitglied des globalen Cyber-Sicherheitsverbands CREST und führt seit mehr als 20 Jahren Penetrationstests an internen Infrastrukturen durch. Als eines der ersten Unternehmen, das diesen Service anbietet, haben wir ein umfangreiches Wissen und Fähigkeiten in den Taktiken entwickelt, die von bösartigen Benutzern angewendet werden, um Zugang zu Unternehmensnetzwerken zu erhalten. Dies ermöglicht es uns, Risiken für das Geschäft zu identifizieren und Maßnahmen zur Behebung dieser Risiken zu skizzieren.

Wenn gewünscht, kann unser erfahrenes professionelles Dienstleistungsteam diese Maßnahmen schnell und effektiv umsetzen, um eine robuste Sicherheit für Ihre Organisation zu gewährleisten.

Ergebnisse des Dienstes

Der interne Health Check bietet:

- Einen formellen Bericht, der einen Überblick über das Netzwerk und vorgeschlagene Maßnahmen zur Verbesserung bietet
- Einen Bericht, der zur Rechtfertigung von Ausgaben zur Verbesserung der Infrastruktursicherheit verwendet werden kann
- Eine Skizzierung Ihres Wegs zu einer sichereren Umgebung
- Einen Bericht, der bei Akkreditierungsstellen eingereicht werden kann
- Einen Bericht, der Ihr Engagement für Sicherheit gegenüber internen und externen Kunden demonstriert.

Berichte werden innerhalb von 10 Arbeitstagen nach Abschluss aller Tests geliefert. Nach Abschluss der Testarbeiten wird jeder Bericht unabhängig von einem Mitglied des technischen Teams auf technische Genauigkeit und Lesbarkeit des Berichts überprüft.

Kontaktieren Sie MTI
T: +49 (0) 6122 9950
E: deinfo@mti.com
W: de.mti.com