

Externer Health Check

Um in der modernen Ära sicher zu agieren, ist es unerlässlich, dass sämtliche Organisationen sicherstellen, dass ihre Internetgrenzen vor externen Bedrohungen geschützt und abgesichert sind. Alle Komponenten der Netzwerkinfrastruktur, die dem Internet ausgesetzt sind, unterliegen ständigen Überprüfungen durch Opportunisten, Ransomware-Banden und kriminelle Organisationen. Um die Integrität der internen Infrastruktur zu gewährleisten, bedarf es einer regelmäßigen Überprüfung und Behebung von Problemen an allen internetexponierten Geräten.



Unser Service

Unser Service ist darauf ausgerichtet, die Sicherheit Ihrer nach außen gerichteten Infrastruktur zu stärken und potenzielle Schwachstellen zu identifizieren, an denen Ausrüstung oder Dienste durch einen Angreifer kompromittiert oder durchbrochen werden könnten. Unsere umfangreiche Palette von Tests und Überprüfungen bietet einen ganzheitlichen Überblick über den Zustand Ihres externen Netzwerks sowie klare Hinweise auf Schwachstellen und Schwächen, die behoben werden sollten.

Unser Bericht enthält detaillierte Empfehlungen zur Behebung dieser Schwachstellen und liefert einen klaren Leitfaden, um Ihre Umgebung zu sichern. Sie haben die Möglichkeit, die Schwachstellen eigenständig zu beheben oder von unserem professionellen Service-Team mit über 35 Jahren Erfahrung zu profitieren, das die Probleme in Ihrem Auftrag lösen kann.

Stufe 1

Was wir testen:

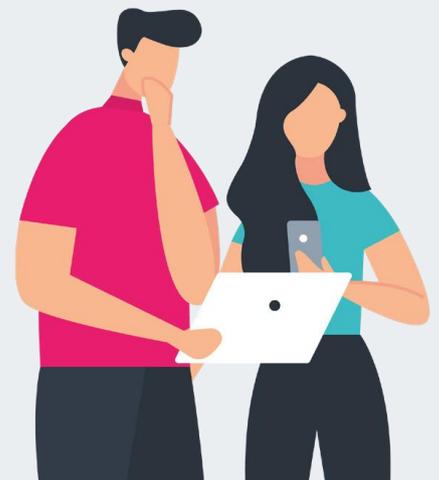
Unsere Penetrationstests für nach außen gerichtete Netzwerke erstrecken sich über verschiedene Bereiche.

Manueller Penetrationstest: Zur Identifizierung von Schwachstellen und Risiken, die durch Ihr Internet-Gateway freigelegt werden, führen wir einen gründlichen manuellen Penetrationstest durch. Dies gewährleistet ein umfassendes Bild aller Systeme, die dem Internet zugänglich sind.

Tools-basierte Schwachstellenanalyse und manuelle Überprüfung: Zur Sicherstellung einer hochwertigen Dienstleistung kombinieren wir zwei Methoden – eine tools-basierte Schwachstellenanalyse und maßgeschneiderte manuelle Überprüfung. Dadurch stellen wir sicher, dass alle identifizierten Probleme eingehend untersucht werden und falsch positive Ergebnisse ausgeschlossen sind.

Umfassender Service: Jeder dem Internet ausgesetzte Dienst wird auf bekannte Schwachstellen, Konfigurationsfehler, fehlende Patches, veraltete Software, Standardpasswörter, erratbare Passwörter und viele andere Probleme hin überprüft.

Fortgeschrittene Tests: Mit unseren erstklassigen Penetrationstest-Tools und Exploit-Frameworks führen wir gründliche Tests an Systemen durch, um sie auf die neuesten bekannten Bedrohungen und Schwächen zu überprüfen. Dadurch identifizieren wir sowohl bekannte als auch unbekannte Schwachstellen. Wenn zutreffend, werden sowohl bekannte als auch unbekannte Schwachstellen ausgenutzt, einschließlich Tests auf Schwachstellen, bevor ein Hersteller einen Patch veröffentlicht hat. Dies ermöglicht uns, zu prüfen, ob ein umfassender Ansatz verfolgt wurde, um sicherzustellen, dass zusätzliche Schutzmaßnahmen vorhanden sind.



Stufe 2

Die nächsten Schritte:

Im Folgenden führen wir Tests auf Netzwerkebene durch, um Schwachstellen in Router-Filtering, Firewall-Filtering, Betriebssystemen, Serveranwendungssoftware, Konfigurationsfehlern, Webservern, Webanwendungen und Maildiensten zu identifizieren. Potenziell ausnutzbare Schwachstellen werden erörtert und – nach Zustimmung – ausgenutzt, um deren Umfang zu überprüfen.

Unsere eigenen Textwerkzeuge und Skripte ermöglichen effiziente Tests zahlreicher Hosts, wobei hohe Standards eingehalten und Kosten minimiert werden.



Stufe 3 Reporting

Der formale Bericht über die Testphasen wird die Zielsetzung der Sicherheitsbewertung, den Umfang, die Zusammenfassung der Ergebnisse, die Risikobewertung, die CVSS-Bewertung, die Beschreibung der Schwachstellen, Empfehlungen sowie die Kontaktdaten für den Kunden und das Testteam enthalten. Zudem werden Zertifizierungen von CHECK/CREST/Cyber Scheme-Beratern aufgeführt.

Schwachstellenregister: Um bei der Behebung und Überwachung der Compliance zu unterstützen, wird MTI ein auf Excel basierendes Schwachstellenregister bereitstellen. Dieses enthält alle bei manuellen Tests gefundenen Probleme, einschließlich der CVSS-Bewertungen, in einem sortierbaren und bearbeitbaren Format. Aufgrund der üblicherweise großen Anzahl von Problemen umfasst dies jedoch nicht die während automatisierter Tests entdeckten Schwachstellen.



Deliverables

Der externe Gesundheitscheck-Service umfasst:

- Einen formellen Bericht, der einen Überblick über die dem Internet zugängliche Infrastruktur bietet und zeigt, was getan werden muss
- Einen Aktionsplan, der die empfohlenen Schritte zur Behebung darlegt und die Etappen detailliert beschreibt, um Ihren Fortschritt bei der Behebung nachzuverfolgen
- Einen Bericht, der dazu verwendet werden kann, Ausgaben zur Verbesserung der Verteidigung gegenüber anderen Teilen des Unternehmens zu rechtfertigen
- Eine Skizzierung Ihres Wegs zu einer sichereren Umgebung. Die Berichte werden nach Abschluss aller Tests geliefert. Wir werden uns bemühen, die Berichte so schnell wie möglich zu veröffentlichen und sie zu beschleunigen, wenn kritische Fristen eingehalten werden müssen, sofern im Voraus über den Beginn der Arbeiten informiert wird. Berichte werden nach Abschluss aller Tests geliefert. Wir werden uns bemühen, die Berichte so schnell wie möglich zu veröffentlichen und sie zu beschleunigen, wenn kritische Fristen eingehalten werden müssen, vorausgesetzt, dass im Vorfeld über den Beginn der Arbeiten informiert wird

Wieso MTI?

MTI ist lebenslanges Mitglied der globalen Cybersecurity-Organisation CREST und führt seit 20 Jahren Penetrationstests an Internet-gerichteter Infrastruktur durch. Als eines der ersten Unternehmen, das diesen Service anbietet, haben wir ein umfangreiches Wissen und Fähigkeiten in den Taktiken entwickelt, die von böswilligen Benutzern verwendet werden, um Zugang zu Unternehmensnetzwerken zu erhalten. Dies ermöglicht es uns, Risiken für das Unternehmen zu identifizieren und Maßnahmen zur Behebung dieser Risiken zu skizzieren.

Bei Bedarf können Sie von unserer Expertise profitieren, um die erforderlichen Maßnahmen zur Behebung über unseren professionellen Service umzusetzen.

Ergebnisse & Vorteile

Unser externer Gesundheitscheck liefert die folgenden Ergebnisse:

- Bietet eine gründliche Prüfung und Test der dem Internet zugänglichen Infrastruktur
- Erkennt 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

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