

IT-SCHWACHSTELLENSCAN

Zur Identifizierung der Schwachstellen in einem Netzwerk oder Computersystem können verschiedene Methoden angewendet werden. Eine der Methoden, um potenzielle Gefahren zu erkennen, ist der automatisierte IT-Schwachstellenscan, auch Vulnerability Scan genannt.

Dieser automatisierte Scan wird von einer Software ausgeführt, die auf eine Datenbank mit bekannten Sicherheitslücken zugreift und somit unterschiedliche Gefahren erfassen kann. Der Prozess ermöglicht es, potenzielle Schwachstellen frühzeitig zu erkennen und zu beheben, bevor sie von Angreifern ausgenutzt werden können. Durch regelmäßige Vulnerability Scans der TÜV TRUST IT können Sie Ihre Systeme proaktiv schützen und die Sicherheit Ihrer IT-Infrastruktur verbessern. So tragen Sie wesentlich dazu bei, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Systemen zu gewährleisten.

IT-SCHWACHSTELLENSCAN „PAKET S“

Dieses Paket beinhaltet eine kurze sicherheitstechnische Untersuchung von bis zu 9 Zielsystemen, die durch den Auftraggeber festgelegt werden können. Konkret hierunter befasst sind ein automatisierter tool-gestützter Schwachstellenscan, eine stichprobenartige händische Überprüfung sowie die entsprechende Dokumentation. Der automatisierte Scan untersucht die Systeme auf bekannte Schwachstellen, Fehlkonfigurationen, veraltete Komponenten und weitere mögliche Sicherheitsprobleme. Im Anschluss findet eine stichprobenartige händische Verifizierung statt, durch die Fehlmeldungen, sogenannte False Positives, entfernt werden. Die Ergebnisse werden im Excel-Format dokumentiert und enthalten je identifizierter Schwachstelle eine Beschreibung, eine Risikoklassifizierung sowie daraus abgeleitete Empfehlungen.

IT-SCHWACHSTELLENSCAN „PAKET M“

Das „Paket M“ erweitert den Schwachstellenscan der Stufe „S“ um dediziert manuelle Überprüfungen von bis zu 3 Zielsystemen, die durch den Auftraggeber definiert werden können. Bei diesen manuellen Überprüfungen werden nicht nur False Positives identifiziert, sondern auch separate Prüfroutinen durchlaufen, mittels derer ein größerer Erkenntnisgewinn über das Schadenspotential der gefundenen Schwachstellen erzielt werden kann.

IT-SCHWACHSTELLENSCAN „PAKET L“

Der Schwachstellenscan „L“ ist inhaltlich zum „Paket M“ gleich und ermöglicht die Ausweitung der Dienstleistung auf einen größeren Projektscope. Der Scan darf in diesem Paket bis zu 12 Systeme umfassen und die händische Überprüfung wird für bis zu 6 Systeme, die der Auftraggeber definieren kann, angeboten.

hiermit ebenfalls gebotene gesteigerte Testintensität eröffnet zudem größeren Spielraum für die priorisierte Betrachtung kritischer Systeme.

IT-Schwachstellenscan

„Paket S“

- Auswahl von bis zu 9 Systemen durch den Kunden
- Überprüfung der ausgewählten Systeme auf offene Ports und erreichbare Dienste
- Automatischer Schwachstellenscan, der Systeme auf bekannte Schwachstellen, Fehlkonfigurationen und Sicherheitsprobleme
- Stichprobenartige Verifizierung der identifizierten Schwachstellen
- Bericht mit einer Auflistung der identifizierten Schwachstellen (Beschreibung, Risikoklassifizierung, Empfehlung)

Festpreis: **990,- € netto**

IT-Schwachstellenscan

„Paket M“

- Auswahl von bis zu 9 Systemen durch den Kunden
- Überprüfung der ausgewählten Systeme auf offene Ports und erreichbare Dienste
- Automatischer Schwachstellenscan, der Systeme auf bekannte Schwachstellen, Fehlkonfigurationen und Sicherheitsprobleme
- Verifizierung der identifizierten Schwachstellen
- Zusätzliche manuelle Überprüfungen von bis zu 3 Systemen
- Bericht mit einer Auflistung der identifizierten Schwachstellen (Beschreibung, Risikoklassifizierung, Empfehlung)

Festpreis: **1.990,- € netto**

IT-Schwachstellenscan

„Paket L“

- Stichprobenartige Sichtung vorhandener Netzwerkpläne und IT-Unterlagen
- Auswahl von bis zu 12 Systemen durch den Auditor und Kunden
- Identifizierung erster Angriffspunkte auf Grundlage der gesichteten Dokumente
- Überprüfung der ausgewählten Systeme auf offene Ports und erreichbare Dienste
- Automatischer Schwachstellenscan, der Systeme auf bekannte Schwachstellen, Fehlkonfigurationen und Sicherheitsprobleme
- Verifizierung der identifizierten Schwachstellen
- Zusätzliche manuelle Überprüfungen von bis zu 6 Systemen
- Bericht mit einer Auflistung der identifizierten Schwachstellen (Beschreibung, Risikoklassifizierung, Empfehlung)

Festpreis: **2.990,- € netto**

Erfahren Sie mehr darüber, wie unsere maßgeschneiderten Penetrationstest-Pakete zum Festpreis dazu beitragen können, Ihre IT-Sicherheit zu stärken und Ihnen dabei zu helfen, potenzielle Risiken frühzeitig zu erkennen und zu beheben. Profitieren Sie dabei ebenfalls von unseren Bundle-Paketen:

BUNDLE „PAKET S“

- Bestehend aus IT-Schwachstellenscan „Paket S“ und Phishing-Kampagne „Paket S“
- Festpreis **2.682,- € netto**

BUNDLE „PAKET L“

- Bestehend aus IT-Schwachstellenscan „Paket L“ und Phishing-Kampagne „Paket L“
- Festpreis **7.182,- € netto**

Wir freuen uns auf Ihre Anfrage: vertrieb@tuv-austria.com

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Tel.: +43 (0) 5 0454 - 1000



info@tuv-austria.com
www.it-tuv.com