

AGILER

CYBERSICHERHEITS- SCHNELLTEST



Haben Sie auch ein mulmiges Gefühl zum Status Quo Ihrer IT-Sicherheit? Werden Sie vielleicht sogar schon angegriffen und Sie wissen es noch gar nicht, weil die Angreifer sehr vorsichtig vorgehen, um nicht aufzufallen? Und kennen Sie alle möglichen Schwachstellen und Einfallstore für Angreifer in Ihrer IT-Umgebung?

Ziel unseres agilen Cybersicherheits-Schnelltests ist es, Ihnen kostengünstig und schnell einen ersten Überblick über die Cybersicherheit Ihrer Infrastruktur an die Hand zu geben. Darin enthalten sind Handlungsmaßnahmen sowie Empfehlungen zur Steigerung Ihrer IT-Sicherheit. Dieser Schnelltest besteht aus drei Phasen und kann sowohl für extern erreichbare Systeme als auch für interne Systeme und Netzwerke durchgeführt werden.

ABLAUF

Phase 1 „Screening“: Überblick verschaffen und Angriffspunkte verifizieren

- Erste Sichtung vorhandener Netzwerkpläne und IT-Unterlagen
- Festlegung der zu prüfenden Systeme
- Identifizierung erster Angriffspunkte auf Grundlage der gesichteten Dokumente

Phase 2 „Schwachstellenanalyse“: Analyse und Verifizierung

- Überprüfung der ausgewählten Systeme auf offene Ports und Dienste (Port-Scan)
- Einsatz eines automatischen Schwachstellenscanners, der die Systeme auf bekannte Schwachstellen, Fehlkonfigurationen und Sicherheitsprobleme untersucht
- Verifizierung der identifizierten Schwachstellen

Phase 3 „Auswertung und Report“: Zusammenfassung mit ersten Hinweisen zur Verbesserung

- Kurze Zusammenfassung der Phasen 1 und 2
- Unsere IT-Sicherheitsexperten erläutern die Schnelltest-Ergebnisse und besprechen das mögliche weitere Vorgehen bei Bedarf
- Bereitstellung einer Schnelltest-Auswertung als Zusammenfassung der Testergebnisse

BEWERTUNGSGRUNDLAGE UND RISIKOKLASSIFIZIERUNG

Die festgestellten Risiken werden vier Kategorien zugeordnet (Hohes Risiko, Mittleres Risiko, Geringes Risiko, Empfehlung). Die Klassifizierung der festgestellten Risiken erfolgt aus der Perspektive der IT-Sicherheit bezogen auf die Infrastruktur, Systeme, Dienste und Prozesse im Untersuchungsbereich. Für die identifizierten Risiken werden Empfehlungen ausgesprochen, welche die IT-Sicherheit der Infrastruktur, Systeme, Dienste und Prozesse im Geltungsbereich nachhaltig verbessern bzw. optimieren.

ABSCHLUSSBERICHT

Der Abschlussbericht orientiert sich bei der Bewertung der identifizierten Schwachstellen an den jeweiligen Prüfgrundlagen und enthält unter anderem Informationen wie: Prüfgrundlagen, Management-Zusammenfassung (max. 1 DIN A4-Seite), Liste der Risiken (ggf. nach Systemen, Technologien, Abteilungen, etc. gruppiert), Beschreibung der durchgeführten Tätigkeiten, der gefundenen Risiken und der für diese Risiken angemessenen Maßnahmen.

PREIS

Durchführung eines agilen Cybersicherheits-Schnelltest mit Fokus auf die Kernsysteme der internen IT-Infrastruktur (begrenzt auf 25 Systeme, inkl. Schnelltest-Ergebnisbericht)

pauschaler Paketpreis **€ 4.900,- zzgl. MwSt.** (Leistung erfolgt remote, optional vor Ort möglich)

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

Für Fragen oder weitere Informationen:

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

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



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

