

Penetration Testing

Beim Penetration Testing prüfen unsere zertifizierten IT-Sicherheitsexperten, wie gut Ihre Systeme gegen digitale Angriffe geschützt sind. Dazu werden kontrollierte Hackerangriffe simuliert – natürlich ohne Schaden anzurichten. Ziel ist es, Schwachstellen und Angriffspfade frühzeitig zu er-

kennen und zu beheben, bevor echte Angreifer sie ausnutzen können. Damit die Tests möglichst realistisch und wirkungsvoll sind, werden sie individuell auf Ihr Unternehmen abgestimmt. So lassen sich aktuelle und zukünftige Bedrohungen gezielt nachstellen und bewerten.

	Interner Penetration Test	Externer Penetration Test	Application Penetration Test	Fokussierter Penetration Test
Worüber gibt der Test Auskunft?	Können Mitarbeiter oder unbefugte Dritte aus dem Unternehmen heraus Schaden anrichten?	Kann jemand von außen – über das Internet – in das Unternehmen eindringen?	Ist es möglich, in ausgewählte Anwendungen wie z.B. einzelne Programme oder Apps einzudringen?	Können Teilbereiche eines Unternehmens übernommen werden?
Was wird geprüft?	Interne Netzwerke, Programme, Passwörter und Geräte	Öffentlich erreichbare Webseiten und Programme	Applikationen mit oder ohne Zugangsdaten sowie – sofern gewünscht – der Programmcode	Einzelne, ausgewählte Komponenten wie Computer und Server, Active Directory oder Cloud-Systeme
Wann ist der Test sinnvoll?	Um zu prüfen, wie gut das interne Netzwerk geschützt ist	Um öffentlich zugängliche Systeme optimal abzusichern	Um potenzielle Sicherheitslücken in neu entwickelten Programmen oder Apps auszuschließen	Um wichtige Systemänderungen auf potenzielle Sicherheitslücken zu prüfen
Dauer	Ab 8 Arbeitstagen	Ab 5 Arbeitstagen	Ab 5 Arbeitstagen	Ab 5 Arbeitstagen

Sie wollen wissen, wie gut Ihre Systeme wirklich geschützt sind? Wir liefern die Antwort!

Kontaktieren Sie uns für Ihr unverbindliches Angebot: