Automated Penetration Testing

Spüren Sie Schwachstellen im System auf, stärken Sie Ihre Cyber Security und verhindern Sie Cyberattacken

Automated Penetration Testing für digitale Unternehmen

Die vermehrte Nutzung digitaler Technologien und Cloud Services hat die Attack Surface der Unternehmen deutlich vergrößert. Deswegen sollten Organisationen ihre Cyber Security daran anpassen und auf das nächste Level heben.

Eine Methode zur Verbesserung der IT-Sicherheit ist die Identifizierung möglicher Schwachstellen in der IT-Infrastruktur. Angreifer konzentrieren sich auf solche Sicherheitslücken, weil es ihren Job wesentlich vereinfacht. Unternehmen sollten ihre Attack Surface und Cyber Security daher aus der Sicht eines Cyberkriminellen betrachten – und Penetrationstests machen genau das.

Penetrationstests sind simulierte Angriffe auf die IT-Infrastruktur eines Betriebes, etwa das Netzwerk sowie die unterschiedlichen Systeme und Applikationen, um potenzielle Schwachstellen aufzuspüren. Solche Tests manuell durchzuführen, kann sich, speziell für expandierende Unternehmen oder solche mit einer ausgedehnten, komplexen und dynamischen IT-Infrastruktur, jedoch als unzureichend erweisen. Die Lösung sind automatisierte Tests, die den Prozess optimieren und die Effektivität steigern.

Automatische Penetrationstests nehmen weniger Zeit in Anspruch, sind skalierbar, genauer und decken die Gesamtinfrastruktur besser ab. Die Automatisierung ermöglicht Unternehmen, Schwachstellen schneller zu finden, potenziell schädliche Auswirkungen abzuschätzen, Compliance Richtlinien einzuhalten, Kosten zu sparen und Cyber Security proaktiv zu managen.

Durch den Einsatz von Technologien wie künstlicher Intelligenz (KI) und Automatisierung zur Optimierung des Ende-zu-Ende Testprozesses können Organisationen Schwachstellen schneller und kosteneffizienter beseitigen. Auf diese Weise kann ein Unternehmen die Sicherheitsrisiken minimieren, bevor Angreifer sie ausnutzen könnten. Automatische Penetrationstests können somit dazu beitragen, die Folgen von Cyberangriffen zu reduzieren.

Wann ist Automated Penetration Testing sinnvoll?

Automatische Penetrationstests ermöglichen Ihnen und Ihrem Unternehmen:

Proaktiv Schwachstellen zu identifizieren: Finden und beheben Sie Sicherheitslücken in Netzwerken, Systemen und Applikationen und reduzieren Sie die Gefahr von Datenlecks und unberechtigten Zugriffen.

Schnellere und effizientere Tests durchzuführen: Optimieren Sie den Testprozess und sparen Sie wertvolle Zeit und Ressourcen im Vergleich zu manuellen Testmethoden. Tests können öfter und effizienter durchgeführt werden, sodass eine Konstante gebildet werden kann.

Vorteile von Automated Penetration Testing

- **Weiterentwickeltes Scanning:** Schneller und genauer
- **Automatische Reports:** Ergebnisse, die Sie umsetzen können
- **Kontinuierliches Monitoring:** Erkennen von Problemen und reagieren in Echtzeit
- **Integration mit vorhandener IT-Security:** Nur minimale Anpassungen notwendig
- **Testparameter flexibel konfigurierbar:** Individuelle Anforderungen werden umgesetzt

Compliance Richtlinien einzuhalten: Stellen Sie durch regelmäßige Tests Ihrer Cyber Security sicher, dass Ihre Organisation gesetzliche Compliance Anforderungen wie die DSGVO, NIS 2, HIPAA oder PCI DSS einhalten kann und vermeiden Sie die unter Umständen empfindlichen Strafen.

Gesamtabdeckung Ihrer IT-Infrastruktur zu gewährleisten: Stellen Sie umfassende Tests aller potenziellen Attack Surfaces sicher, darunter Netzwerke, Webanwendungen und sämtliche Endpunkte. Finden Sie Sicherheitslücken in Ihrer IT-Landschaft, reduzieren Sie blinde Flecken und verbessern Sie dadurch die Cyber Security Ihres Unternehmens.

Skalierbarkeit: Passen Sie die Testparameter an die spezifischen Anforderungen Ihrer Organisation an. Egal ob Ablaufplanung, Definition des Testumfangs oder Auswahl der Zielsysteme, der Testprozess kann flexibel an die individuellen Anforderungen Ihrer Organisation angepasst werden.

T Systems

Wie wir Sie unterstützen können

Nachdem wir die Zielsetzung mit Ihnen abgeklärt haben, wählen wir einen oder mehrere Bereiche für die Penetrationstests aus, beispielsweise Netzwerksicherheit, Webanwendungen, Sicherheit der Endgeräte usw.

Unsere Testphasen:

Reconnaissance

Automatisierte Tools sammeln Informationen über die ausgewählten Netzwerke, Systeme, Anwendungen, Endpunkte und Schwachstellen

Scannen

Scanning Tools suchen systematisch in der definierten IT-Umgebung nach offenen Ports, schwach gesicherten Services und Sicherheitslücken

Auflisten der Ergebnisse

Automatische Tools berechnen die Systemdetails, beispielsweise den Account der Nutzer, Ressourcen im Netzwerk und Systemkonfiguration, um mögliche spätere Tests noch zielgerichteter durchführen zu können.

Nachsondierung

Sammlung zusätzlicher Informationen, Ausweitung der Berechtigungen und tiefer reichender Zugriff auf fehlerhafte Systeme.

Berichterstattung

Detaillierter Bericht über die Ergebnisse der Tests. Dieser detaillierte Bericht enthält den Schweregrad der identifizierten Probleme, Empfehlungen zur Abhilfe und Priorisierung von Maßnahmen zur effektiven Behebung von Schwachstellen.

Profitieren Sie vom Automated Penetration Testing von T-Systems

- **Vermeiden Sie massive Cyberangriffe:** Durch die Identifizierung von Schwachstellen stärkt Ihr Unternehmen die Cyber Security, reduziert die Cyberrisiken und schützt sensible Daten.
- **Kosten sparen:** Die Optimierung des Testprozesses reduziert den Bedarf an Arbeitskräften und spart dadurch Zeit und Ressourcen für kontinuierliches Monitoring
- **Einhaltung gesetzlicher Vorgaben:** Durch die Einhaltung von Richtlinien wie der DSGVO und NIS 2 vermeiden Sie Strafen und stärken das Vertrauen Ihrer Stakeholder.
- **Verbesserte Reaktion auf Sicherheitsvorfälle:** Mit dem Wissen um mögliche Sicherheitslücken können Sie prompt reagieren und Sicherheitsrisiken minimieren.
- **Schutz Ihrer Reputation:** Wenn Sie Cyber Security zu einer Priorität Ihres Unternehmens erklären, stärken Sie Vertrauen und Glaubwürdigkeit und schützen die Markenintegrität.

Warum T-Systems?

- Wir verfügen über ein Team von Cyber Security Expert:innen mit Erfahrung und Zertifizierung von Offensive Security Certified Professionals (OSCP), Global Information Assurance Certification (GIAC) und weiteren Organisationen.
- Wir liefern Ihnen detaillierte Berichte mit Ergebnissen und Handlungsempfehlungen, sowie einen Executive Report als Zusammenfassung für das Topmanagement.
- Wir nutzen Best Practices und Rahmenwerke wie MITRE und ATTT&CK um bei Cyberbedrohungen und Sicherheitstechnologien immer auf dem neuesten Stand zu sein.
- Sie können aus mehreren Arten von Testprozessen wählen: Black Box, Grey Box oder White Box.
- Unsere Teams nutzen modernste Tools, abgestimmt auf Ihre IT-Landschaft und die unterschiedlichen Testszenarien.
- Wir verfügen über Tools zur Simulation unterschiedlicher, böswilliger Cyberattacken, zum Beispiel Weak Credential Exploit, Endpoint Security Tests, Active Directory Tests, Datenlecks, Simulation von Ransomware und vieles weitere.
- Ihr Tagesgeschäft bleibt von den Penetrationstests unberührt.
- Zusätzlich bieten wir Ihnen umfassenden Beratung zum Thema Cyber Security, sodass wir Ihr Unternehmen langfristig begleiten können.

Entdecken Sie Sicherheitslücken in Ihrer Infrastruktur. Wählen Sie aus unseren Paketen, um Ihren individuellen Geschäftsanforderungen gerecht zu werden.

Kontaktieren Sie uns gleich

Expert Kontakt
Andreas Pecka
Head of International Expert Sales & Pre-Sales
Cyber Security
a.pecka@t-systems.com

Kontakt us
www.t-systems.com/contact
cyber.security@t-systems.com

Herausgeber
T-Systems International GmbH
Hahnstrasse 43d
60528 Frankfurt am Main
Deutschland

T Systems