arco
IT SECURITY SERVICES

Penetration Testing

Jeden Tag decken Hacker potenzielle Schwachstellen in IT-Systemen auf. Im Jahr 2022 wurden über 22.500 Sicherheitslücken veröffentlicht. Viele davon werden von Angreifern ausgenutzt, bevor IT Abteilungen die Lücken bemerkt oder geschlossen haben.

Mit einem Penetrationstest werden Sie sich der Sicherheitslücken bewusst, die Ihr Unternehmen verletzbar und offen für Cyberangriffe machen könnten. Um sicherzustellen, dass Ihre IT sicher ist, führt unser engagiertes Team von PenTest-Experten erstklassige White-, Black- oder Grey-Box-Penetrationstests mit einer Kombination aus automatischen, halbautomatischen und manuellen Tools durch.

Während bei einem automatisierten Penetrationstest spezialisierte Software-Tools oder Skripte verwendet werden, um ein System automatisch auf potenzielle Schwachstellen zu prüfen, erfolgt bei einem halbautomatischen Test eine manuelle Überprüfung. Die Ergebnisse werden von einem Sicherheitsanalysten überprüft und validiert. Dieser multidisziplinäre Ansatz für Pentesting erstellt in regelmässigen Abständen eine umfassende Momentaufnahme der Gefährdung Ihres Unternehmens, die potenzielle Sicherheitsschwachstellen aufzeigt und verwertbare Erkenntnisse zur Risikominderung liefert.

WIE ES FUNKTIONIERT

Mit Hilfe unseres PenTest-Teams werden Ihre Systeme von aussen getestet, um eine klassische Überprüfung Ihrer Perimetersicherheit durchzuführen. Wir können auch innerhalb Ihrer IT-Umgebung testen, um Ihre "Defense-in-Depth"-Sicherheit zu validieren.

1. ENTDECKEN

Unser Penetrationstest-Team nutzt Erkennungstools und Sonden innerhalb Ihres Netzwerks (insbesondere bei "Defense-in-Depth" -Tests), um den Umfang der Systeme zu ermitteln und erste Daten zu sammeln, z. B. erreichbare Hosts, offene Ports, Fingerabdrücke aktiver Dienste, Versionen von Webservern usw.

Zusätzlich zu den klassischen IT-Geräten, die von den meisten Infrastrukturgruppen gut verwaltet werden, entdecken wir auch Netzwerkgeräte, IoT-Geräte, IT-Systeme und andere Hardware, die möglicherweise nicht in Ihren internen Verwaltungsprozessen berücksichtigt wurden. Das Ergebnis ist eine umfassende Bestandsaufnahme der vernetzten Geräte.

2. SCAN

Die Daten werden anschliessend sorgfältig analysiert, um mögliche Angriffswege zu ermitteln. Dieser Prozess ist wichtig, um die Schwachstellen des Zielsystems zu verstehen und den besten Ansatz zur Durchführung eines gründlichen und effektiven Penetrationstests zu bestimmen. In diesem Schritt sucht unser PenTest-Team mit automatisierten Tools nach Schwachstellen. Wir verwenden umfassende Datenbanken mit bekannten Schwachstellen, um die Systeme unserer Scan-Tools zu füttern. So erhalten wir eine Liste von Schwachstellen, die wir vorrangig ausnutzen wollen.

3. EINDRINGEN

Sobald das PenTest-Team ein klares Bild der Umgebung hat, kann es sich darauf konzentrieren, die Sicherheitsgrenze zu durchbrechen oder ein Zielgerät auszunutzen. Wir setzen fortschrittliche Techniken ein, um uns kontinuierlich Zugang zu verschaffen oder uns seitlich in Ihrem Netzwerk zu bewegen, ähnlich wie es ein echter Angreifer tun würde. Für jedes System, in das wir eindringen konnten, sammeln wir Beweise und eine Beschreibung, wie der Einbruch möglich war.

Um das Schwachstellen- und Patch-Management zu unterstützen, können wir nach erfolgten Wartungsarbeiten durch einen erneuten Test sicherstellen, dass Ihre Systeme auf einem sicheren Stand sind. Unser Team kann auch regelmässige Scans einrichten, um zu prüfen und Sie zu alarmieren, wenn neue Schwachstellen gefunden werden.

WAS SIE ERWARTEN KÖNNEN

Ihr Unternehmen ist auf ein solides Fundament angewiesen, das keine Risse oder Schwachstellen aufweist. Wir helfen Ihnen dabei, dieses Fundament zu legen und es regelmässig zu verstärken, um sicherzustellen, dass Ihre IT-Infrastruktur stabil ist. Mit unseren kontinuierlichen Schwachstellen-Scans können Sie ausserdem sicher sein, dass Ihre Sicherheitsstandards und Patch-Management-Prozesse Angreifern die Tür vor der Nase zuschlagen.

IHRE VORTEILE

- Eine Bestandsaufnahme der vorhandenen Dienste und Infrastruktur: Dies hilft Ihnen, einen klaren Überblick über Ihre Infrastruktur und Dienste zu gewinnen, und ermöglicht es Ihnen, proaktiv auf Systeme einzuwirken, die Sie vielleicht noch nicht kannten.
- Eine Liste der Sicherheitsschwachstellen mit einer Risikobewertung für Ihre extern exponierten oder internen Systeme, damit Sie Ihre Sicherheitsanstrengungen nach Prioritäten ordnen und die wichtigsten Schwachstellen zuerst angehen können, um Ihr Risiko eines erfolgreichen Cyberangriffs schnell zu verringern.
- Ratschläge von Experten zur Behebung der festgestellten Probleme, damit Sie Ihre Abwehrkräfte stärken und Ihre Systeme vor Cyber-Bedrohungen schützen können.

arco Albulastrasse 34, 8048 Zürich 044 244 02 20 info@arco-it.ch www.arco-it.ch