Was ist ein Penetrationstest?

Ein Penetrationstest ist ein kontrollierter realitätsnaher Angriff auf Netzwerke, Systeme oder Applikationen, um Schwachstellen zu identifizieren, die durch potenzielle Angreifer genutzt werden können.

Abgrenzung zu Schwachstellenanalysen / Vulnerability Assessments

Vulnerability Assessments durchsuchen die Zielsysteme automatisiert nach bekannten Schwachstellen ab und listen diese auf. Es findet also kein Versuch der Verifizierung direkt am System statt, ob die Fehlerquellen ausgenutzt werden könnten. Beim Penetrationstest dagegen erfolgt mithilfe von Experten eine manuelle Überprüfung auf bekannte und unbekannte Schwachstellen, diese werden anschließend verifiziert und kategorisiert.

Mit der Durchführung eines Penetrationstests decken unsere Pentester die IT-Lücken Ihres Unternehmens auf und geben Ihnen konkrete Maßnahmen zur Eliminierung bzw. Risikoreduzierung aller Schwachstellen an die Hand.

Warum sollte man einen Penetrationstest durchführen?

Kaum ein Tag vergeht, an dem nicht versucht wird, in Anwendungen, Systeme und Netzwerke einzubrechen. Selbst große Konzerne wie Facebook, Twitter und Instagram sind nicht davor sicher - wie jüngste Vorfälle belegen.
Cyber-Attacken werden auch in Zukunft bei einer Vielzahl deutscher Unternehmen zu einem großen Schaden führen und deren Existenz bedrohen.
Eine Firewall und ein Antivirentool sind daher längst nicht mehr ausreichend, um ein Unternehmen vor diesen Gefahren zu schützen.

Kontrollierter und gezielter Einbruch als Prävention

Die Robustheit Ihrer IT sollte daher „auf Herz und Nieren" geprüft werden, um für künftige digitale Bedrohungen gewappnet zu sein. Ein Penetrationstest deckt genau diese Szenarien ab und zeigt Ihnen den realen Sicherheitszustand ihrer IT-Umgebung auf. Er gibt Auskunft darüber, wie anfällig Ihre Systeme sind, wie wahrscheinlich ein Angriff auf Ihre IT-Infrastruktur ist und gibt Handlungsempfehlungen, wie Sie sich in Zukunft besser vor potentiellen Angriffen schützen können.

Einfach ausgedrückt, Penetrationstests werden zu EINEM Zweck durchgeführt, nämlich zum Schutz Ihrer Organisation.

Wir haben es uns zum Ziel gesetzt, diese Schwachstellen für Sie zu identifizieren, bevor diese zu realen Bedrohungen für Ihre IT-Umgebung werden.

BKA warnt: Gefahr durch Cyberkriminalität während Corona stark gestiegen!

Vorteile eines Penetrationstests

- Aufdeckung von unbekannten Sicherheitsrisiken
- Gewährleistung von Compliance Richtlinien
- Vorteile bei der Cyber-Risk-Versicherung
- Vermeidung von Bußgeldern bei Datenpannen nach DSGVO
- Schutz von Firmengeheimnissen
- Schutz vor Image-Schäden
- Reduzierung von Ausfallzeiten und Folgekosten
- Stärkung des Kunden- und Partnervertrauens

Welche Schäden können Hacker verursachen?

102 Milliarden Euro betrug der geschätzte Gesamtschaden im Jahr 2019 durch digitale Angriffe in Deutschland. Der Schaden ist damit fast doppelt so hoch wie noch vor zwei Jahren.

75% aller deutschen Unternehmen waren Ziel von digitalen Angriffen im Jahr 2019 und 70% der Unternehmen sind durch digitale Angriffe zu Schaden gekommen.

67% aller kleinen und mittleren Unternehmen (KMU) in Deutschland gaben an, ohne eine funktionierende IT nicht operative arbeiten zu können.

67% aller kleinen und mittleren Unternehmen (KMU) in Deutschland brauchen 3 oder mehr Tage um ihre Systeme wieder zum Laufen zu bringen.

Nur **20%** aller kleinen und mittleren Unternehmen (KMU) sehen bei sich selbst Handlungsbedarf. Das Cyberrisiko und ihre Folgen werden bei der Mehrheit der Unternehmen grundlegend unterschätzt.

©Quellen:
GDV - Cyberrisken im Mittelstand (2019)
Bitkom - Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt (2020)

Ablauf des Penetrationstests

1 Vorbereitung & KickOff

- Aufbereitung vertraglicher und rechtlicher Aspekte
- Abstimmung in Bezug auf Umfang und Vorgehensweise
- Definition von Notfallmaßnahmen und Eskalationsstufen
- Informationssammlung über das Zielsystem

2 Testdurchführung & Analyse

- Automatisierter Schwachstellenscan mit Hilfe von Enterprise Anwendungen und eigenen Lösungen
- Tiefgreifender manueller Penetrationstest durch unsere Experten
- Beweissicherung und Revalidierung der gefundenen Schwachstellen

3 Ergebnisbericht & Präsentation

- Detaillierter Abschlussbericht mit konkreten Handlungsempfehlungen
- Darstellung der Risiken und Maßnahmen per Videokonferenz als Präsentation

4 Nachtest & Retrospektive

- Nachtest der Handlungsempfehlungen nach Behebung der Schwachstellen
- Retrospektive und Lessons Learned der Zusammenarbeit

Normen und Standards im Einsatz

Bei der Durchführung der Penetrationstests setzen wir auf bewährte, anerkannte, deutsche sowie globale Standards, um höchste Testqualität zu gewährleisten:

BSI - Bundesamt für Sicherheit in der Informationstechnik
DSGVO - Datenschutz-Grundverordnung
OWASP - The Open Web Application Security Project
OSSTM - Open Source Security Testing Methodology Manual
NIST – U.S. National Institute of Standards and Technology
CIS - Center for Internet Security

360° Schutz in einem Paket

Wir verbinden das beste aus beiden Welten. Spezialisierte juristische Expertise für eine maximale rechtliche Sicherheit bei der compliancegerechten Durchführung und Nachbetreuung (insbesondere gemäß DSGVO, BDSG und GeschGehG) durch die AGOR AG und mehr als 5 Jahre Erfahrung im Bereich Penetrationstests bei unserem IT-Partner IT2Pi.

AGOR STRATEGY | PRIVACY | ACADEMY
info@agor-ag.com
+49 (0) 69 - 9494 32 410
www.agor-ag.com

IT2Pi A NEXT GENERATION COMPANY
info@it2pi.com
+49 (0) 89-21529188
www.it2pi.com