CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

PENETRATION TESTING

Pakete für klein- und mittelständische Unternehmen

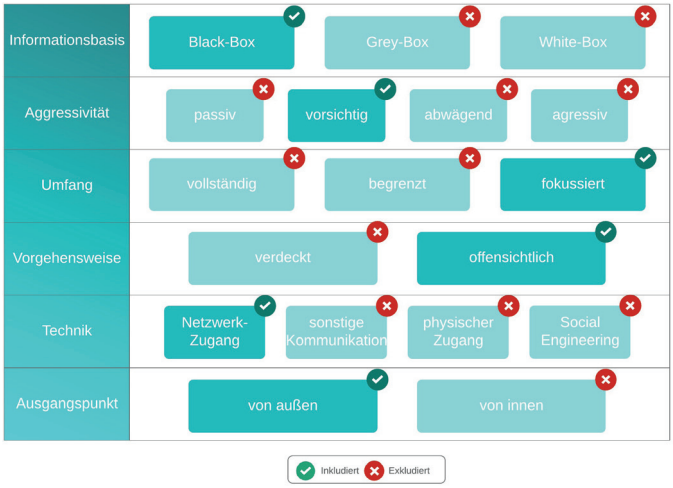
IHR NUTZEN

- **Nachweis der Erfüllung der Sorgfaltspflichten** des IT-Infrastruktur-Managements im Kontext von geschäftskritischen, sensiblen und personenbezogenen Daten
- **Lagebild zur IT-Sicherheit durch unabhängiges externes Audit**
- **Empfehlungen** für notwendige bzw. sinnvolle Sicherheitsmaßnahmen **zur langfristigen Erhöhung des Sicherheitslevels Ihrer Organisation**

ZIELSETZUNG

Das AIT bietet, neben individualisierten Pentests, drei für klein- und mittelständische Unternehmen optimierte Einstiegspakete für Penetrationstests an, um die Exponierung gegenüber Cyber-Angreifern aus dem Internet zu evaluieren. Dabei wird nach folgendem Schema vorgegangen:

- **Black Box:** Ohne Detailkenntnisse (z.B. Zugänge, Sourcecode, Dokumentation, etc) über das zu untersuchende System
- **Vorsichtig:** Schwachstellen werden nur dann ausgenutzt, wenn diese Ausnutzung zu keiner Beeinträchtigung des untersuchten Systems führen
- **Fokussiert:** Ausschließlich auf IT-Systeme der vom Auftraggeber zur Verfügung gestellten IP-Adressen
- **Offensichtlich:** Umfangreiche, auffällige Scans
- **Netzwerkzugang:** Der Zugang erfolgt ausschließlich über das Netzwerk
- **Von außen:** Der Test wird über das Internet durchgeführt



ANGEBOTSINHALTE

Es stehen folgende Leistungspakete zur Auswahl:

Basis Paket	Standard Paket	Premium Paket
Durchführung toolgestützter, automatisierter Tests sowie vereinzelt manueller Tests. Verifikation und Interpretation der Ergebnisse. Erhöhung der Basissicherheit mit Schutz vor allem gegen „Script-Kiddies" und „Hobby-Hacker".	Durchführung toolgestützter, automatisierter Tests sowie manuelle Tests durch unsere Experten. Verifikation und Interpretation der Ergebnisse.	Durchführung toolgestützter, automatisierter Tests sowie ausführliches Testing durch unsere Experten. Verifikation und Interpretation der Ergebnisse. Imitiert am ehesten das Verhalten professioneller Angreifer.

Im Rahmen der zuvor genannten Pakete werden IT-Systeme hauptsächlich im Hinblick auf direkte Angriffe über das Internet untersucht. Viele weitere mögliche Schwachstellen (Social-Engineering als besonders relevante Gefahrenquelle, direkter physischer Zugriff, Penetration des Wi-Fi-Netzwerks etc.) können in individuell vereinbarten Folgeprojekten überprüft werden.

Die Ergebnisse des Penetrationstests werden in einem Bericht festgehalten, der die zum Zeitpunkt der Durchführung der Tests identifizierten Schwachstellen, Fehlkonfigurationen und Abweichungen von „Best Practices" auflistet. Die Erkenntnisse und die daraus abgeleitenden Maßnahmen werden während der Bericht-Abschlussbesprechung erläutert.

VORAUSSETZUNGEN

Der Auftraggeber übermittelt zur Durchführung des Penetrationstests notwendige Informationen (IP-/DNS-Adressen, Systembeschreibungen) und verpflichtet sich zur Unterzeichnung des zur Verfügung gestellten „Permission to Attack"-Dokuments vor Durchführung der Sicherheitsüberprüfung.

Es gilt im Allgemeinen, dass die Anzahl der gefunden Schwachstellen mit dem investierten Aufwand und dem vorhandenen Informationsstand über die zu testenden Systeme steigt. Sollte der angebotene Testaufwand in Bezug auf den Umfang und der Komplexität der zu testenden Systeme kein sinnvolles Mindestmaß aufweisen, behält sich der Auftragnehmer das Recht vor, vom Angebot zurückzutreten bzw. einen sinnvollen Mindestaufwand aufzuzeigen.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Manuel Kern, MSc
Tel +43 50550-4170
Giefinggasse 4, 1210 Wien
manuel.kern@ait.ac.at
www.ait.ac.at/cyber-security