Penetration Testing

Wissenschaftlich fundierte Cybersicherheitsprüfungen für höchste Ansprüche

In einer digital vernetzten Welt sind IT-Infrastrukturen das Rückgrat moderner Organisationen. Gleichzeitig steigt die Komplexität der Systeme – und mit ihr das Risiko von Sicherheitslücken, Cyberangriffen und regulatorischen Verstößen. Penetration Testing des AIT Austrian Institute of Technology bietet eine evidenzbasierte, technisch hochentwickelte Methode, um reale Angriffsszenarien zu simulieren, Schwachstellen aufzudecken und Organisationen im öffentlichen wie privaten Sektor resilienter zu machen. Dieser Ansatz verbindet wissenschaftliche Exzellenz, langjährige Forschungserfahrung und modernste Technologien – und schafft damit einen verlässlichen Sicherheitsstandard, der weit über herkömmliche IT-Audits hinausgeht.

So funktioniert es

Penetration Testing ist ein empirischer Sicherheitscheck, der die Werkzeuge und Methoden realer Angreifer nutzt, um Schwachstellen, Fehlkonfigurationen und Abweichungen von Best Practices zu identifizieren. AIT führt diese Prüfungen ausschließlich durch zertifizierte Sicherheitsexperten durch – ausgestattet mit tiefem wissenschaftlichem Know-how und umfangreicher Projekterfahrung aus nationalen und internationalen Sicherheitsforschungsprogrammen.

Der Prozess folgt einem klar strukturierten Vier-Phasen-Modell:

Planung – Definition des Prüfungsumfangs, Auswahl der Testmethoden, Festlegung branchenspezifischer Bedrohungsszenarien.

Vorbereitung – Informationsgewinnung, Analyse potenzieller Angriffspunkte, Bewertung möglicher Vektoren.

Durchführung – kontrollierte Ausnutzung identifizierter Schwachstellen, Simulation echter Angriffe (einschließlich Black-Box-, White-Box- oder Hybridmethoden).

Präsentation – Abschlussbericht mit allen Befunden, Risikobewertungen und klar priorisierten Handlungsempfehlungen.

Neben klassischen IT-Infrastrukturen können Anwendungen (Web, Mobile, Desktop), Netzwerke (LAN, WLAN), Cloud-Dienste, IoT-Umgebungen sowie physische Sicherheitsaspekte getestet werden. Für KMU bietet das AIT drei abgestufte Servicepakete (Basic, Standard, Premium), die sowohl automatisierte als auch manuelle Prüfverfahren kombinieren. AIT verfolgt zudem einen erweiterten Forschungsansatz: Neben der Prüfung bekannter Schwachstellen werden im Rahmen von Red Teaming und Reverse Engineering auch bislang unbekannte Zero-Day-Schwachstellen identifiziert. Damit bietet das Institut ein Sicherheitsniveau, das deutlich über den Marktstandard hinausgeht.

Fakten

- Lösungsbereich: **Prozesse, Regulierungen und Konformität, Soziale Teilhabe und Engagement, Technologische Innovation**
- Verwaltungsebene: **Bundesland, Bund**
- Lösungsprozess: **Digitalisierung und Technologie, Justiz, Öffentlicher Dienst, Sicherheit und Verteidigung, Wissenschaft und Forschung**
- Technologie: **Informationstechnologie, Internet of Things, Netzwerke**

Penetration Testing

Wissenschaftlich fundierte Cybersicherheitsprüfungen für höchste Ansprüche

Das große Ganze

Penetration Testing des AIT ermöglicht es Organisationen, Compliance- und Sorgfaltspflichten nachweisbar zu erfüllen, Risiken proaktiv zu minimieren und Sicherheitsstrategien langfristig zu optimieren. Behörden, kritische Infrastrukturen und große Unternehmen profitieren von einer unabhängigen, fundierten Sicherheitsbewertung, die reale Angriffsrisiken quantifiziert und strategisch adressiert. Durch den klar strukturierten Prüfprozess erhalten Organisationen eine valide Momentaufnahme ihrer Cybersicherheit – ergänzt durch konkrete Empfehlungen, die technische, organisatorische und prozessuale Verbesserungen ermöglichen. Dies reduziert nicht nur das Risiko finanzieller Schäden, Datenverluste oder Reputationsschäden, sondern unterstützt auch die betriebliche Resilienz und die Einhaltung europäischer Vorgaben wie NIS2, GDPR oder Cyber Resilience Act. In einer Umgebung, in der Bedrohungslagen und Angriffstechniken sich ständig weiterentwickeln, schaffen regelmäßige Penetration Tests eine belastbare Entscheidungsgrundlage für Investitionen in Sicherheitsmaßnahmen.

AIT empfiehlt jährliche Tests oder kürzere Intervalle bei veränderten Rahmenbedingungen. Dadurch wird gewährleistet, dass Unternehmen und öffentliche Stellen auf aktuelle und zukünftige Cyberbedrohungen vorbereitet sind – wissenschaftlich fundiert, technologisch präzise und praxisorientiert.

aed – Agency for Economic Cooperation and Development
Ferdinandstraße 4,
1020 Wien, Österreich

+43 (1) 448 00 55 10
platform@bestpracticeaustria.at