Penetration Testing

Scientifically grounded cybersecurity assessments for the highest standards

In an increasingly digital and interconnected world, IT infrastructures form the backbone of modern organizations. At the same time, system complexity is rising – and with it the risks of security vulnerabilities, cyberattacks, and regulatory non-compliance. Penetration Testing by the AIT Austrian Institute of Technology provides an evidence-based, technologically advanced method to simulate real attack scenarios, uncover vulnerabilities, and strengthen the resilience of public and private sector organizations. This approach combines scientific excellence, extensive research experience, and state-of-the-art technologies, resulting in a security standard that far exceeds conventional IT audits.

Quick Facts

- Solution area: **Processes, Regulations and compliance, Social participation and engagement, Technological innovation**
- Administrative level: **State, Federation**
- Solution process: **Digitization and technology, Judiciary, Public service, Science and research, Security and defense**
- Technology: **Information technology, Internet of Things, Networks**

How it works

Penetration Testing is an empirical security assessment that uses the tools and methods of real attackers to identify vulnerabilities, misconfigurations, and deviations from best practices. AIT conducts these assessments exclusively through certified cybersecurity experts with deep scientific expertise and extensive project experience gained from national and international security research programs.

The process follows a clearly structured four-phase model:

Planning – Defining the testing scope, selecting appropriate methods, and determining sector-specific threat scenarios.

Preparation – Gathering information, analyzing potential attack surfaces, and assessing possible vectors.

Execution – Controlled exploitation of identified vulnerabilities and simulation of real attacks (including black-box, white-box, or hybrid approaches).

Presentation – Delivery of a comprehensive report detailing all findings, risk assessments, and clear, prioritized recommendations.

In addition to traditional IT infrastructures, AIT tests applications (web, mobile, desktop), networks (LAN, WLAN), cloud services, IoT environments, and physical security components. For SMEs, AIT offers three tiered service packages (Basic, Standard, Premium) that combine automated and manual testing procedures. AIT also pursues an extended research-driven approach. Beyond testing for known vulnerabilities, experts identify previously undiscovered zero-day vulnerabilities through red teaming, reverse engineering, and advanced analysis. This delivers a security level significantly above market standard.

The Big Picture

Penetration Testing by AIT enables organizations to demonstrate compliance and due diligence, proactively mitigate risks, and strategically enhance their long-term security posture. Public authorities, critical

aed – Agency for Economic Cooperation and Development
Ferdinandstraße 4,
1020 Vienna, Austria

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

Penetration Testing

Scientifically grounded cybersecurity assessments for the highest standards

infrastructure operators, and large enterprises benefit from an independent, scientifically based security assessment that quantifies real attack risks and provides actionable guidance. The structured testing process delivers a validated snapshot of an organization's cybersecurity status, complemented by concrete, prioritized recommendations that strengthen technical, organizational, and procedural safeguards. This not only reduces the risk of financial loss, data breaches, and reputational damage, but also supports organizational resilience and adherence to European regulations such as NIS2, GDPR, and the Cyber Resilience Act. In a landscape where threat scenarios and attack techniques evolve continuously, regular penetration tests provide a robust foundation for informed security investment decisions.

AIT recommends annual penetration tests or shorter intervals when external or internal conditions change. This ensures that organizations remain prepared for current and emerging cyber threats – grounded in scientific rigor, technological precision, and practical applicability.

aed – Agency for Economic Cooperation and Development
Ferdinandstraße 4,
1020 Vienna, Austria

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