TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Technical Security Analysis / Penetration Test

Many companies are concerned about the security of their IT, and rightly so. The fear of falling victim to cyber-attacks is well-grounded. TÜV TRUST IT's security analysts will help you identify vulnerabilities, evaluate risks objectively and subsequently find measures to increase your protection level.

Approach

Performing penetration tests on a regular basis is one of the most suitable ways to protect your IT from unauthorised access. The penetration tests of TÜV TRUST IT are carried out by our experts with longstanding practical experience. In addition, TÜV TRUST IT is certified by the Federal Office for Information Security as an IT security service provider for the areas of penetration tests, IS audit and IS consulting.

Acting like a "Normal" Hacker

Our testers design their security analyses in accordance with the procedures of actual adversaries, thereby establishing a high degree of authenticity. Naturally, no actual harm will be done. From their insights gained, our experts will produce an easily intelligible report, recommending useful measures to be taken.
The security analysis consists of five phases: Preparation, information gathering, evaluation, penetration attempts and a final report. In the first phase, it is checked which attack vectors exist in the infrastructure or application to be examined. By means of a threat model it is determined, among other things, which security vulnerabilities arise through the interaction of different work areas, which in themselves may be relatively safe.
Our security analysts are following the same path as hackers, using the "low-hanging fruits". They check the infrastructure and try to attack the weakest points in order to penetrate the network. Once they are on the network, they check for more extensive threats. They collect information about the network components, about systems, services and applications within the investigation area. Then they try to find and exploit vulnerabilities, checking whether they can pretend to be other users (identity spoofing) or modify data (tampering). Important is the question of whether tracks can be blurred, for example by bypassing logging. In this case, accesses or changes cannot be assigned to a user (repudiation).

Error messages are actually intended to give the experienced programmer an assistance. But they can also contain valuable clues about the system that can be misused by adversaries. This unwanted leakage of information is called Information Disclosure. Relatively well-known are disturbances of services, which can result from massive simultaneous accesses. This can lead to a denial of service that, for example, makes your website unreachable. Such attacks can also completely block other services or block user accounts.

So that no productive systems are endangered, such attacks will be carried out only after separate agreement. The final test involves attempting to gain unauthorised permissions (elevation of privileges). Should this be successful, the risk of sensitive data getting into the wrong hands is particularly

Phases of the Security Analysis

TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

high. This analysis is structured in according to recognised standards and the best practice approaches of TÜV TRUST IT. One of the ways to ensure that tests stay comparable is to repeat them after one year.

Federal Office for Information Security
Certified IT-Security Service Provider
BSI Certificate No: BSI-APS-9041 valid 28.02.2025

Detailed Report with Recommended Measures

All results of the investigation, including our recommended measures, will be summarised in a comprehensible final report. Our security analysts evaluate and classify the individual risks during the analysis. The importance of early implementation depends on the respective risk-class. If an immediate threat to IT security is identified, the customer will be informed at once in order to initiate concrete countermeasures as soon as possible. In a final workshop, the report, including a Management Summary, will be presented. Meaningful and appropriate measures to remedy the weak points can then be discussed here.

Your Benefits

- Identification of vulnerabilities in your IT and objective risk analysis
- Final report with assessed and classified risks, including recommendations for appropriate improvement measures
- Providing the extensive know-how of the neutral and objective auditors of TÜV TRUST IT
- The proficiency of TÜV TRUST IT for conducting penetration tests has been confirmed by the Federal Office for Information Security (BSI) with the certification as a certified IT security service provider.
- Fulfilment of conformity to standards, among others:
  - DORA (Digital Operational Resilience Act)
  - TR-03109-6 Smart Meter Gateway Administration
  - ISO27001
  - IEC62443
  - Common Criteria

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Phone: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Phone: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com