Penetration test and IT security analysis: Detect vulnerabilities - prevent damage.

How secure is your IT environment?

Internal and external penetration tests and IT security analyses provide answers.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

FORESTALL HACKERS - WITH A SIMULATED CYBER ATTACK

Criminal hackers can exploit vulnerabilities in your network, your IT systems, applications or mobile devices to penetrate your organization and manipulate or steal sensitive business information and customer data. No organization is „too small" or „too insignificant" for an attack and many organizations are already compromised without even knowing it. Do you know what vulnerabilities the hackers can exploit in your systems and applications?

MORE INFORMATION ON IT INFORMATION SECURITY IN JUST A FEW STEPS

During our tests, we analyze your IT infrastructure and/or applications from the viewpoint of a hacker. In doing so, we simulate a realistic cyber attack and detect vulnerabilities in your IT before hackers can exploit them. Our experts will inform you if and how your IT is vulnerable and what consequences this may have for your organization. We also recommend countermeasures to eliminate the detected vulnerabilities so that you can better protect your organization, your data and your know-how in future.

YOUR ADVANTAGES

- A qualified overview of specific vulnerabilities in your network, your IT systems, applications or mobile devices.
- A reliable and objective assessment of the effectiveness of your IT security measures.
- Recommendations for efficient and economical countermeasures in order to eliminate vulnerabilities effectively and permanently.
- On request, we will help you to implement efficient protective measures.

OUR COMPETENCE

Every year, the Security Engineering Team at TÜV Rheinland performs more than 250 penetration tests and security analyses – a fast growing trend. We are proficient in the development and implementation of current attack scenarios against IT systems, networks and web applications through to mobile applications and WLANs. In addition to technical security analyses and penetration tests, we also carry out a detailed analyses (security assessments and source code analyses for applications). Certification is possible as proof of the attained high security standards. Simply ask us!

Procedure in penetration tests and IT security analyses

GATHERING OF INFORMATION

All the information relevant to an attack is collected. How does the organization appear from the viewpoint of an external hacker (via the Internet) or an internal hacker (via the Intranet)?

IDENTIFICATION OF VULNERABILITIES

We identify possible vulnerabilities in your networks, infrastructure components, mobile devices and applications.

EXPLOITATION OF VULNERABILITIES

Working closely with you, we try and access your networks, infrastructure components, mobile devices and applications.

REPORTING

We document and classify the detected vulnerabilities in a TÜV Rheinland test report. We show what damage a hacker can cause in your organization. The high-quality report and the clarity of the findings are ensured by means of a review based on the „four eyes" principle.

COUNTERMEASURES

We recommend suitable countermeasures to enable you to permanently eliminate the detected vulnerabilities. If required, we will help your experts to improve IT security in your organization by implementing specific countermeasures.

TÜV Rheinland
Digital Transformation & Cybersecurity
Am Grauen Stein
51105 Cologne, Germany
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/en/pentest

TÜVRheinland®
Precisely Right.