TÜV
TRUST IT
TÜV AUSTRIA Group

AGILE CYBER SECURITY QUICK TEST

Do you also have an uneasy feeling about the status quo of your IT security? Are you perhaps already under attack and you don‘t even know it yet because the attackers are proceeding very carefully to avoid attracting attention? And do you know all the possible vulnerabilities and gateways for attackers in your IT environment?

The aim of our agile cyber security quick test is to provide you with an initial overview of the cyber security of your infrastructure quickly and affordably. It includes action plans and recommendations for improving your IT security.

This quick test consists of three steps and can be carried out for externally accessible systems as well as for internal systems and networks.

PROCEDURE

Step 1 „Screening“: Gaining an overview and verifying weak points

- Initial review of existing network plans and IT documents
- Definition of the systems to be tested
- Identification of initial attack points based on the reviewed documents

Step 2 „Vulnerability analysis“: Analysis and verification

- Checking the selected systems for open ports and services (port scan)
- Use of an automatic vulnerability scanner that analyses the systems for known vulnerabilities, misconfigurations and security problems
- Verification of the identified vulnerabilities

Step 3 „Evaluation and report“: Summary with initial tips for improvement

- Short summery of steps 1 and 2
- Our IT security experts explain the quick test results and discuss possible further action if required
- Provision of a quick test evaluation as a summary of the test results

ASSESSMENT BASIS AND RISK CLASSIFICATION

The identified risks are assigned to four categories (high risk, medium risk, low risk, recommendation). The identified risks are categorised from the perspective of IT security in relation to the infrastructure, systems, services and processes in the scope of the analysis. Recommendations are made for the identified risks to sustainably improve or optimise the IT security of the infrastructure, systems, services and processes in the scope.

CLOSING REPORT

The closing report is based on the respective audit principles when assessing the identified weaknesses and contains information such as audit basis, management summary (max. 1 DIN A4 page), list of risks (grouped by systems, technologies, departments, etc., if applicable), description of the performed activities, the identified risks and the appropriate measures for these risks.

COST POINT

Implementation of an agile cybersecurity quick test with a focus on the core systems of the internal IT infrastructure (limited to 25 systems, incl. quick test results report)

flat-rate package price **€ 4.900,- plus VAT** (service is performed remotely, optionally on site)

We look forward to your enquiry:
vertrieb@tuv-austria.com

For questions or further information:

TÜV TRUST IT
TÜV AUSTRIA Group

TÜV TRUST IT GmbH
TÜV AUSTRIA Group

Waltherstraße 49–51
51069 Cologne/Germany
Phone: +49 (0)221 969789 - 0

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