TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

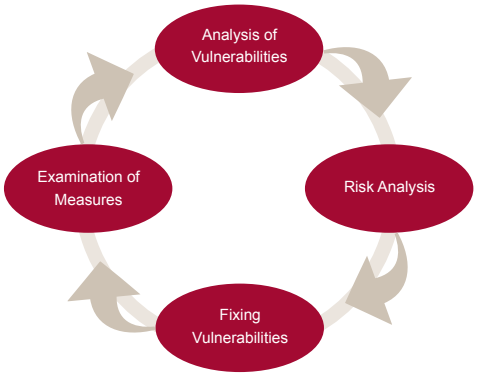
Cyber Watchdog: Establishing a Constantly Maintained Security Level

IT security is a rapidly changing and dynamic process that is increasingly subject to changes in IT security processes. If a system is considered to be “safe” today, it can already be classified as critical on the next day as a new vulnerability or misconfiguration becomes known. The consequence is a threat to the security goals of confidentiality, availability and integrity. For this reason punctual penetration tests are no longer sufficient today, a permanent review is required. Vital systems should hence be checked on a regular basis. The results of the monitoring should also speak the language of risk management so that manageable reports can be generated.

TÜV TRUST IT offers a permanent, risk-oriented and technical vulnerability management with the Cyber Watchdog. The use of vulnerability scanners and targeted penetration tests determine whether your IT systems are adequately protected. In addition, you will be optimally supported in keeping your systems permanently secure. Upon request, the experts from TÜV TRUST IT will prepare the findings on a management-individual basis according to your customised risk methodology.

Approach

The Cyber Watchdog offers the optimal combination of a tool-based security management and the advice of experienced security experts. For this purpose, we first determine with you in a timetable, which systems should be continuously monitored and how often the IT security level should be verified. Different schedules for different systems can be realised. Thus systems of higher criticality will be scanned more frequently than less critical ones.



Processes of the Cyber Watchdog

Individual Timetable

After creating your individual schedule, a regularly recurring process begins with the following steps:

To begin with, we identify vulnerabilities in your IT systems through a comprehensive analysis using a vulnerability scanner and performing point-of-penetration tests. After identifying the hazards, a detailed assessment is made with regard to the endangerment of the security objectives. The findings are assigned to one of the four risk classifications, critical, high, medium and low, or based on your own risk management methodology. In the next step, suitable measures for remedying the weak points are developed and described in detail for all vulnerabilities, and the implementation of the specified measures is verified.

TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Permanent Reporting

All activities and results from this process are summarised regularly in a management report. You will be immediately informed about vulnerabilities that are rated “critical”.

If your company does not have an appropriate tool for the relevant process steps, we usually use the Security Configuration Management System Chief Compliance and provide TÜV-certified compliance profiles for specific contexts. This solution identifies and analyses vulnerabilities. Our experts evaluate these weaknesses and illustrate possible corrective actions.

Your Benefits

- Optimal protection of your IT system landscape - and not just at a specific time, but permanently
- Permanent review of your IT systems to ensure a continuous level of security
- Objective assessment of IT risks by our seasoned experts
- Recommended measures so as to maintain and constantly improve your security level

TÜV TRUST IT GmbH
TÜV AUSTRIA Group

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