KERKAPORTA
</ IT SECURITY GMBH>

Portfolio

Kerkaporta offers a customised security package that comprehensively covers your IT security requirements.

</ Web Application Audit >

Potential attackers use security flaws to gain access to confidential data in your company, such as user names, passwords, e-mail contents, or various documents. Additionally, access to servers or connected systems by third parties can lead to financial as well as image damage for operators and customers.

Recent studies show that at least 70% of the worldwide accessible websites have security gaps.

To protect your online presence comprehensively, Kerkaporta offers Web Application Security Audits for your web applications:

- Content Management Systems
- Intranet pages
- Webshops
- Online editorial systems
- Weblogs
- In-house developments

Security relevant mistakes in the design, implementation or operation are easily made, particularly concerning in-house developments. Since web applications are not always subjected to special security tests before the initial operation, many contain weaknesses such as cross-site scripting (XSS), SQL injection, or cross-site request forgery. Logical errors, which, for example, make contents accessible to unauthorized users, are also often part of such software.

We test your web applications with numerous years of experience, know-how, and in compliance with high-quality standards. The audits are carried out according to OWASP guidelines and thus meet the current standards as well as the highest quality requirements.

</ Client Audit >

The Client Audit focuses primarily on tools worked with daily: workstation, notebook, and smartphone. Find out in detail which authorisations your employees have and to which degree they are able to gain access to the company's systems.
The security settings, the encryption of hard disks, and the actuality of your systems are also subjected to a comprehensive analysis.

After a Client Audit, you will have certainty as to who and to what extent your systems can be accessed. If necessary, security measures can then be taken and permissions changed.

</ Server Audit >

Besides Client Audits, also servers can be audited. These audits provide you with information on the server configuration, its settings in the Active Directory, and whether all security patches have been installed.

</ Network Security >

How well do you know your network?

Network security goes beyond secure networking within the company: protecting network access and connections to external and mobile devices, cloud services, and other Internet services has also become a high priority. Networking brings many advantages, but the risks, such as electronic eavesdropping operations or manipulation of transmitted data, are also increasing. Therefore, monitoring of network infrastructures and protection against unauthorized access are essential to maintain the highest level of security.

Learn more about your network and its composition. Kerkaporta will give you an understanding of hacker attacks on your network and what damage an unknown device in your network can cause. With our professional expertise, you will get comprehensive protection for your network.

</ Training >

To ensure security in your company, not only a well-protected IT infrastructure is required, but also a basic understanding of IT security among your employees is crucial. Especially in the daily routine of handling IT systems, cybercriminals see a potential point of attack. The "human factor", therefore, becomes the focus of criminal attacks. Through awareness training, your employees, one the one hand, learn to recognise potential dangers and, on the other hand, to avoid risky or incorrect behaviour in their daily routines. Strengthen your employees' awareness of IT security and give them the necessary know-how to be able to recognise attacks in time and to react appropriately.

Contents of our Awareness Training:

- Put yourself in the perspective of a hacker: What damage can hackers do and how do they proceed?
- Handling e-mails: Detecting phishing e-mails
- Password security
- Detection of forged links in e-mails or documents
- Computer viruses: How do you react in case of a virus attack and what possibilities do you have in this situation?

</ Secure Coding >

Errors, bugs, or logic errors are common causes of software weaknesses that create potential threats for cyber attacks. Security-critical errors are frequently detected only in the course of penetration tests or successful hacking attacks. The removal of these errors can be associated with high costs. To develop secure software, secure coding is a necessary prerequisite to prevent security weaknesses from arising in the first place.

For Kerkaporta IT Security GmbH, security is the focus when programming web applications. The security aspect is already included in the planning of the programming. Benefit from customised, security-oriented applications that offer user-friendliness and easy handling.