SQS SERVICES

sqs.com

Security Testing

Systematic identification of security gaps

Nothing is ever completely secure. But what is secure enough?

Software and IT systems can never be completely secure. The question is: How secure are your systems, and are they secure enough?

Various methods can be used to systematically test and improve the security of IT systems and organisations. The basis for the tests may vary and will depend on the needs of the company concerned.

Apart from testing individual software components for security-related (programming) errors, all components of the IT infrastructure can also be tested, and the associated processes can be systematically examined and improved.

Depending on the initial situation, technical security tests may start at various testing stages, from all phases of the software development cycle to integration testing and acceptance of the production infrastructure.

The benefits

With this holistic approach, any security gaps can be systematically detected in all areas. There is a particular focus on high-risk areas. Based on the results obtained, counter-measures can then be taken to address the existing risks.

You can identify and eliminate security faults and the resulting risks at an early stage for relatively little cost. This will enable you to save money, improve the accuracy of your planning and stay one step ahead of potential hackers.

With Security Testing, we can analyse and significantly improve the security of your systems and processes.

Holistic Quality & Risk Management (ISO 25010)

Software security

- 360° security throughout the software development process using a combination of proven methods
- Threat modelling and requirements review
- Secure design and coding guidelines
- Architecture and design review
- SAST and DAST

Infrastructure security

- Assessment of the security level and configuration of all types of infrastructure component (hardware and software, mobile devices etc.)
- Penetration testing to identify and monitor potential security gaps (internal and external)

Organisational security

- Review and implementation of regulatory and internal requirements
- Compliance
- Assessments and certifications (e.g. ISO 27001)
- Introduction and testing of Information Security Management systems and Business Continuity plans

Secure software development

You can never produce completely error-free software. But by systematically applying a combination of different methods, you can achieve the highest possible level of security. Tests can be run throughout the software development cycle, so that security-related errors can be prevented in a holistic way.

Even at the requirements and design phase security gaps can be systematically identified and closed by means of threat modelling. Static Application Security Testing (SAST) enables security-related errors in the code to be detected and then removed without running the program, while Dynamic Application Security Testing (DAST) can be used to identify security-related programming errors in software at run-time. By monitoring the target application, we can draw conclusions as to the causes. This results in almost error-free and therefore secure software. Our extensive expertise enables us to support your entire software development process and eliminate security-related errors at an early stage.

Infrastructure security

Individual testing of infrastructure components to identify potential and existing security gaps.

Penetration testing scrutinises your software environment to identify security gaps by means of realistic attacks. The client decides how much information to give our consultants when testing begins – so hacker attacks can be simulated as realistically as you like. The test can be run from outside (e.g. over the Internet) or from your own network. It is also possible to test the configuration of individual systems separately. Any weaknesses found will be set out in a comprehensive report, together with suggested improvements. This will enable you to target and eliminate these weak points.

Organisational security

Review, evaluation and introduction of processes and measures to guarantee information security.

An audit is carried out to review and evaluate internal processes and measures in terms of IT security. Based on the findings, conclusions can be drawn concerning the fulfilment of norms and standards (e.g. ISO 27001 or ‘Basic IT Security’ from the Federal Office for Information Security - BSI) and other regulatory requirements, so steps can be taken to ensure compliance.

If you wish, our consultants can also help you to deploy and establish appropriate measures (such as Information Security Management systems) and assist with the relevant certifications.

Contact

For further information, or if you have any other questions, please do not hesitate to send us an e-mail: info@sqs.com