Tailored IT Security Audits

Effective security and vulnerability analyses based on penetration tests and IT security audits
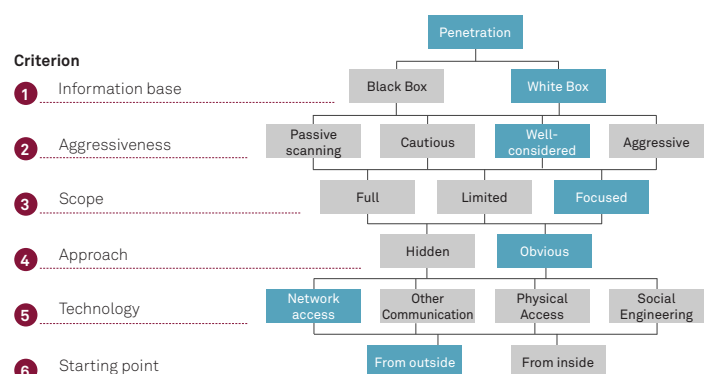
IT attacks can be expensive for your company: production or service downtime, loss of customer data and industrial espionage do not just mean monetary burdens, but the loss of your good reputation as well. Thus, there is no way around effective security measures. Our experts examine whether your current measures are sufficient. We use penetration tests or security audits and give you concrete recommendations on how to optimize your information security.

Tailored Penetration Tests

Individual penetration tests have proven to be an effective tool in the targeted analysis of vulnerabilities, whether for security evaluations or for preventative measures to protect Web applications, software and IT infrastructures. Your individual requirements serve as the benchmark for our tests. Even during the early quotation phase, we are working with you to define criteria such as scope, aggressiveness, technology, type of tests (black or white box test), and many other general parameters.

Do you know how well your company is protected against viruses, malware or espionage programs and whether your applications, systems and infrastructures are safe from attacks? The experts in msg's Information Security division have extensive experience with security audits, penetration tests and security source code reviews. They provide a clear and detailed presentation of the actual state of your company's IT security. With holistic consulting and concrete measures, we help you identify threats early on and sustainably optimize your company's IT security.

Criterion				
		Penetration		
1 Information base		Black Box	White Box	
2 Aggressiveness	Passive scanning	Cautious	Well-considered	Aggressive
3 Scope		Full	Limited	Focused
4 Approach		Hidden	Obvious	
5 Technology	Network access	Other Communication	Physical Access	Social Engineering
6 Starting point		From outside	From inside	

Evaluation of the general parameters pursuant to Germany's Federal Office for Information Security's (BSI) guidelines.

.msg

Our five-phased approach to penetration tests offers the excellent balance between effectiveness and efficiency and enables flexible use of the standards most suitable to your situation.

1. **Preparation:** We work with you to determine goals, timelines and the type of testing, as well as your best corresponding internal counterpart. During a white box test, we review existing documents and question the product owners when necessary.

2. **Information Procurement and Analysis:** To this end, we conduct a scan and collect information from public sources.

3. **Evaluation:** We analyze the collected data and use it as the basis for planning the next steps.

4. **Qualified Attacks:** Simulated penetration tests allow us to test suspected vulnerabilities. We have even developed our own tools to support this step.

5. **Final Analysis:** We evaluate and document the results of the controlled attack. Based on those results, we create a prioritized catalog of measures and render potential threats and risks transparent in a report that includes a management summary.

Tailored Security Audits

Penetration tests are not usually performed as singular measures; instead, they are part of more extensive IT security audits.

During **risk-based audits**, we focus on concrete threat scenarios that your company might face, such as industrial espionage, loss or manipulation of customer data, and help you eliminate or at least minimize vulnerabilities and risks.

Our **compliance audits** examine how well standards and laws are being complied with throughout your entire organization; for example, ISO/IEC 27001, IDW PS 330, OWASP Best Practices, the Payment Card Industry Data Security Standard (PCI-DSS), MaRisk or the Federal Data Protection Act. In doing so, we also take individual requirements into consideration, such as those set forth in contracts.

Our Approach to Security Audits

1. We begin by **analyzing your documentation** on IT security strategy, IT security guidelines and policies, procedures, system documentation and security-related contracts.

2. Based on those results, we work with your security officers and select employees to perform targeted **interviews on security-related questions** throughout your company.

3. We **conduct an on-site assessment of your systems**, which includes random sample inspections, such as how information security guidelines and specifications are being put into practice. At your request, we can also analyze physical security and your data centers or even perform social engineering. Finally, we create a management-compliant report, which we would be glad to present to you.

Our independent, competent experts guarantee efficient, tailored penetration tests and IT security audits. We deliver objective results including meaningful suggestions for improvement that are in line with your business goals and your security strategy.