KPMG

Technical security reviews

IT Risk Advisory Services

Did you know that information security solutions relying on a traditional, compliance-based approach by themselves do not provide sufficient security against well-organised attackers with strong financial backing, nor against certain internal risks? Is your enterprise ready to build up an effective defence for the sake of cyber security?

Globally, an increasing number of security incidents resulting in significant financial losses indicates that periodically reviewed compliance with international information security standards and legal regulations alone does not provide full-scale protection against well-prepared attackers who use targeted tools.

When implementing a risk management system that is capable of responding to this challenge, one needs a good foundation for deciding where to apply financial resources– besides on compliance-based solutions – in order to increase the efficiency of data protection.

Such a well-founded decision is not possible without thorough knowledge of high level threats which affect the given business environment and infrastructure nor without comprehensive information on the vulnerabilities of the systems in question.

Do the following issues sound familiar to you?

- You receive numerous reports on new information security risks, but you cannot get up-to-date information regarding what business-specific threats you should keep in mind in your own economic environment. Your company has no solution for systematising and analysing data on security events which occur in your IT systems, thus you cannot focus your IT security-related efforts on actual threats.
- You have doubts as to whether your IT security solutions can in practice handle the challenges of constant changes in the firm's infrastructure.
- Although the company's internal network is effectively protected against external intrusion, your colleagues do not provide you with objective information on the effectiveness of measures which handle internal risk factors (e.g. abuse of system administration rights).
- Past penetration tests on your network were performed via automated methods and covered the entire infrastructure. However, you are lacking targeted, manual penetration test results for the most critical elements of the infrastructure (e.g. servers for financial processes), thus you lack sufficient practical information on their protection.
- Your enterprise uses more and more business applications for mobile devices (e.g. smart phones, tablets), but you do not have mobile platform-specific solutions for client side security.

KPMG

How can we help you?

Meeting today's challenges requires a complex cyber security strategy. Our services help you build-up a cost-efficient defence.

Review of the risk environment: In co-operation with your enterprise's employees we assess sector-specific technical, business and regulation-related risks which arise in the field of information security. We also review the documents created in connection with general risk analysis and earlier security events. Relying on the results of our review, our analysis supports the improvement of your IT security solutions, with focus laid on high-level risks.

Vulnerability assessment: Using active and passive information gathering methods in cooperation with your enterprise's employees we explore the company's network, identify perimeter systems and vulnerable services running on them. Depending on your needs, our review can be extended to the testing of client–server applications, web applications (e.g. session management, encryption methods), workstations and servers (e.g. system configuration, virus protection), as well as of network security (e.g. controls of remote access, firewalls).

Penetration tests: Our penetration tests rely on KPMG's "PTM" methodology and are carried out according to a plan which covers the scope (system elements) and goals of the penetration tests, all defined in agreement with your company and based on a review of the physical environment and on the results of a vulnerability assessment.

There are four scenarios we can carry out, tailored to your needs, in accordance with the identified risks:

- external penetration testing without authentication (from the perspective of a "naive" hacker)
- external penetration testing with authentication (from the perspective of an adversarial client or contractor)
- internal penetration testing without authentication (e.g. from the perspective of a visitor at the company)
- internal penetration testing with authentication (from the perspective of an adversarial employee).

Partial reviews and supplementary services
In addition to the aforementioned services, we can undertake a technical review of single elements of your system infrastructure (e.g. wireless network, mobile platforms, source code of crucial applications).

- social engineering audit, which is an assessment of the security awareness level of your enterprise's employees
- security awareness training, based on KPMG's "3C" methodology
- compliance review of the physical security of the system infrastructure.

What advantages do we bring?

KPMG's Security Lab team has broad experience in the technical review of IT systems, in both the business and the public sectors.

Our methodology-based services, the transparent structure of our reviews and KPMG's global quality assurance system help to ensure, that our reports and the real-time remediation of vulnerabilities requiring immediate action, contribute to the cost-effective improvement of your firm's cyber security, in line with today's IT security challenges.

If our service offering has aroused your interest, please contact us for further details via the following contact information.

Contact:

György Sallai
Director
T.: +(36) 1 887 6620
E.: gyorgy.sallai@kpmg.hu

KPMG.hu