Kaspersky for Business

Kaspersky Security Assessment

www.kaspersky.com
#truecybersecurity
Kaspersky Security Assessment

Security Assessment Services from Kaspersky Lab are the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

Because no two IT infrastructures are exactly the same, and because the most powerful cyberthreats are tailor-made to exploit the specific vulnerabilities of the individual organization, our expert services are also tailor-made. The services described on the following pages form a part of our professional toolkit – some or all of these services, in part or in full, may be applied as we work with you.

Our objective, above all, is to work with you, one on one, as your expert advisors, helping to evaluate your risk, harden your security and mitigate against future threats.

Security Assessment Services include:

- Penetration testing
- Application security Assessment
- ATM/POS Security Assessment

Penetration Testing

Ensuring that your IT infrastructure is fully secured against potential cyberattack is an ongoing challenge for any organization, but even more so for large enterprises with perhaps thousands of employees, hundreds of information systems, and multiple locations worldwide.

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls in your corporate network to obtain high privileges in important systems.

Kaspersky Lab’s Penetration Testing gives you a greater understanding of security flaws in your infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of your current security measures and suggesting remedial actions and improvements.

Penetration Testing from Kaspersky Lab helps you and your organization to:

- **Identify the weakest points in your network**, so you can make fully informed decisions about where best to focus your attention and budget in order to mitigate future risk.

- **Avoid financial, operational and reputational losses caused by cyber-attacks** by preventing these attacks from ever happening through proactively detecting and fixing vulnerabilities.

- **Comply with government, industry or internal corporate standards** that require this form of security assessment (for example Payment Card Industry Data Security Standard (PCI DSS)).
Service scope and options

Depending on your needs and your IT infrastructure, you may choose to employ any or all of these Services:

- **External penetration testing**: Security assessment conducted through the Internet by an ‘attacker’ with no preliminary knowledge of your system.
- **Internal penetration testing**: Scenarios based on an internal attacker, such as a visitor with only physical access to your offices or a contractor with limited systems access.
- **Social engineering testing**: An assessment of security awareness among your personnel by emulating social engineering attacks, such as phishing, pseudo-malicious links in emails, suspicious attachments, etc.
- **Wireless networks security assessment**: Our experts will visit your site and analyze WiFi security controls.

You can include any part of your IT infrastructure into the scope of penetration testing, but we strongly recommend you consider the whole network or its largest segments, as test results are always more worthwhile when our experts are working under the same conditions as a potential intruder.

About Kaspersky Lab’s approach to penetration testing

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky Lab security experts with full regard to your systems’ confidentiality, integrity and availability, and in strict adherence to international standards and best practices including:

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Project team members are experienced professionals with a deep, current practical knowledge of this field, acknowledged as security advisors by industry leaders including Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens and SAP.

Application Security Assessment

Whether you develop corporate applications internally, or purchase them from third parties, you’ll know that a single coding error can create a vulnerability exposing you to attacks resulting in considerable financial or reputational damage. New vulnerabilities can also be generated during an application’s lifecycle, through software updates or insecure component configuration, or can arise through new attack methods.

Kaspersky Lab’s Application Security Assessment uncover vulnerabilities in applications of any kind, from large cloud-based solutions, ERP systems, online banking and other specific business applications, to embedded and mobile applications on different platforms (iOS, Android and others).

Combining practical knowledge and experience with international best practices, our experts detect security flaws which could expose your organization to threats including:

- Syphoning off confidential data
- Infiltrating and modifying data and systems
- Initiating denial of service attacks
- Undertaking fraudulent activities

Following our recommendations, vulnerabilities revealed in applications can be fixed, and such attacks prevented.
Service benefits

Kaspersky Lab Application Security Assessment Services help application owners and developers to:

• **Avoid financial, operational and reputational loss**, by proactively detecting and fixing the vulnerabilities used in attacks against applications

• **Save remediation costs** by tracking down vulnerabilities in applications still in development and test, before they reach the user environment where fixing them may involve considerable disruption and expense.

• **Support a secure software development lifecycle** (S-SDLC) committed to creating and maintaining secure applications.

• **Comply with government, industry or internal corporate standards** covering application security, such as PCI DSS or HIPAA

Results

Vulnerabilities which may be identified by Kaspersky Lab Application Security Assessment services include:

- Flaws in authentication and authorization, including multi-factor authentication
- Code injection (SQL Injection, OS Commanding, etc.)
- Logical vulnerabilities leading to fraud
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Use of weak cryptography
- Vulnerabilities in client-server communications
- Insecure data storage or transferring, for instance lack of PAN masking in payment systems
- Configuration flaws, including ones leading to session attacks
- Sensitive information disclosure
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

The services are tailored to your needs and application specifics, and may involve:

• **Black-box testing** – emulating an external attacker

• **Grey-box testing** – emulating legitimate users with a range of profiles

• **White-box testing** – analysis with full access to the application, including source codes; this approach is the most effective in terms of revealing numbers of vulnerabilities

• **Application firewall effectiveness assessment** – applications are tested with and without firewall protection enabled, to find vulnerabilities and verify whether potential exploits are blocked

About Kaspersky Lab’s Approach To Application Security Assessment

Security assessments of applications are performed by Kaspersky Lab security experts both manually and through applying automated tools, with full regard to your systems’ confidentiality, integrity and availability and in strict adherence to international standards and best practices, such as:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Other standards, depending on your organization’s business and location

Project team members are experienced professionals with a deep, current practical knowledge of the field, including different platforms, programming languages, frameworks, vulnerabilities and attack methods. They speak at leading international conferences, and provide security advisory services to major vendors of applications and cloud services, including Oracle, Google, Apple, Facebook and PayPal.

ATM/POS Security Assessment

ATMs and POS devices are no longer vulnerable only to physical attacks like ATM burglary or card skimming. As protection measures applied by banks and ATM/POS vendors evolve, so attacks against these devices also shift up a gear, becoming ever more sophisticated. Hackers are exploiting vulnerabilities in ATM/POS infrastructure architecture and applications, and are creating malware specifically tailored to ATM/POS. ATM/POS Security Assessment services from Kaspersky Lab help you to recognize the security flaws in your ATM/POS devices, and to mitigate the risk of being compromised.
There is no single solution that offers comprehensive protection. As a business manager, it's your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

Security Assessment Services from Kaspersky Lab – the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

Why you should do this

ATM/POS Security Assessment by Kaspersky Lab helps vendors and financial organizations to:

• Understand the vulnerabilities in their ATM/POS devices and improve your corresponding security processes
• Avoid the financial, operational and reputational losses that can result from an attack, through proactively detecting and fixing the vulnerabilities which attackers could exploit.
• Comply with government, industry or internal corporate standards, which include the carrying out of security assessments, e.g. PCI DSS (Payment Card Industry Data Security Standard).

What we are testing

The service includes comprehensive ATM/POS analysis including assessment of software components, hardware devices and network communications. Service can be conducted on a single ATM/POS device or on a network of devices. We recommend you to choose for assessment the type of ATMs/POS device in most common use within your organization, or those that are most critical (which have, for instance, already suffered from incidents) in their typical configurations.

How we do this

During analysis, our experts will not just seek out and identify configuration flaws and vulnerabilities in obsolete software versions, but will deeply analyze the logic behind the processes performed by your ATMs/POS devices, undertaking security research aimed at identifying any new (0-day) vulnerabilities at component level. If we uncover vulnerabilities which could profit an attacker (resulting, for example, in unauthorized cash withdrawal), our experts can provide demonstrations of possible attack scenarios using specially crafted automation tools or devices.

Though an ATM/POS Security Assessment involves emulating the attack behavior of a genuine hacker in order to practically assess the effectiveness of your defenses, it is entirely safe and non-invasive.

Threats for Financial Industry

As banks, stock markets, and other financial institutions are under persistent interest of cybercriminals due to the very nature of the financial business, to avoid financial and reputational losses they have to stay ahead of the curve in the field of cybersecurity. Kaspersky Lab offers a set of proactive threat intelligence services for financial institutions that are looking to enhance their security operations and take a proactive approach against advanced threats:

• Security Assessment Services (Penetration Testing, Application Security Assessment, ATM and POS Security Assessment)
• Threat Intelligence Reports (APT Intelligence Reports, Customer-Specific Threat Intelligence Reports)
• Cyber-Attack Readiness Testing
• Botnet Threat Tracking
• Threat Data Feeds
• Malware Analysis and Digital Forensic
• Training: Threat Analysis, Forensic and Investigation

See more at www.kaspersky.com/enterprise