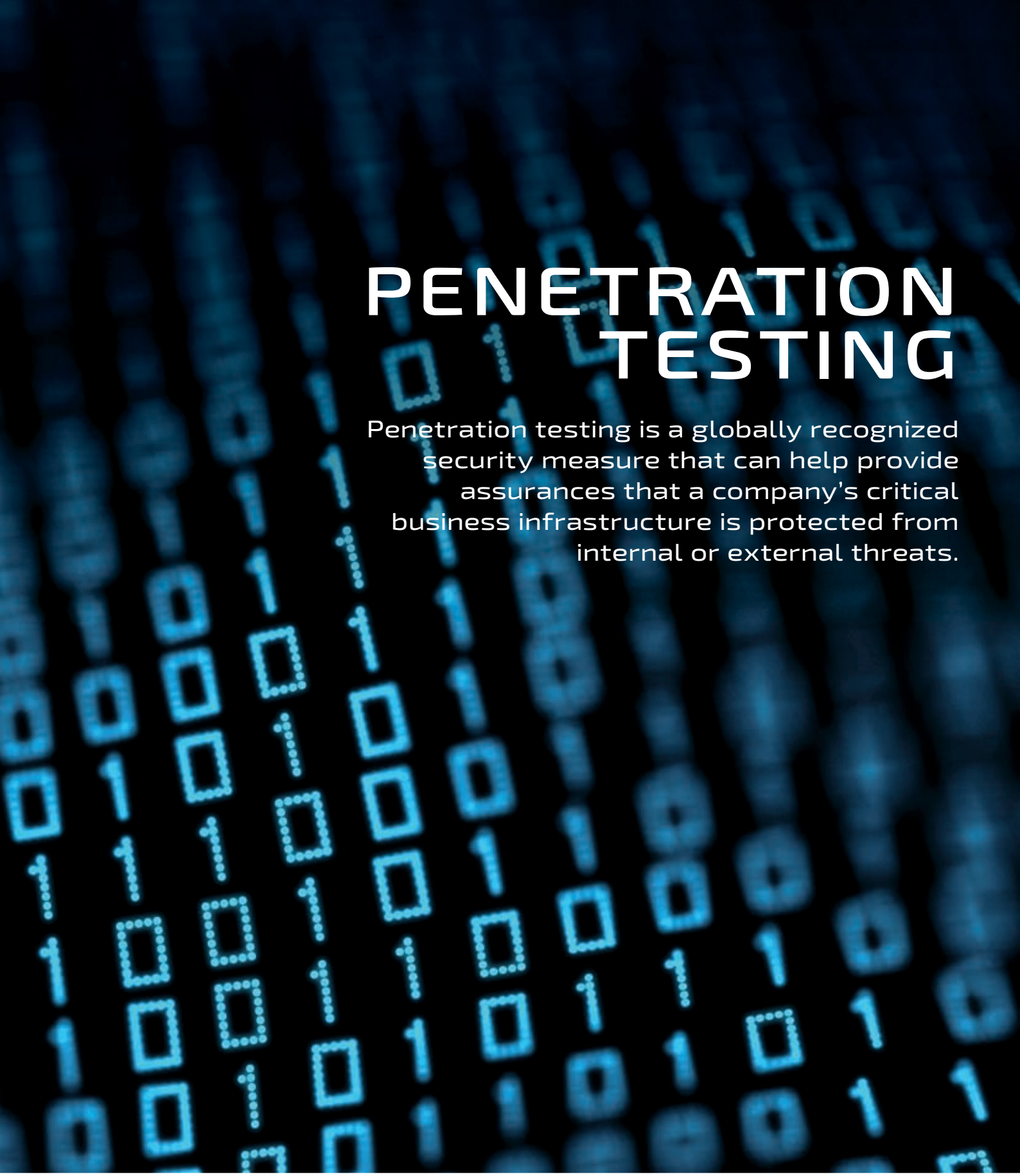

PENETRATION TESTING

Penetration testing is a globally recognized security measure that can help provide assurances that a company's critical business infrastructure is protected from internal or external threats.

www.infigo.hr

INFIGO Information security

INFIGO IS PENETRATION TESTING TEAM

Penetration testing is one of the core competencies of INFIGO IS. Our services are recognized and recommended by our range of customers, small and large, in Croatia, Europe, and beyond.
Our experience, expertise and professionalism make us a leader in IT security testing and ensure our service delivers the maximum value to your business. Our penetration testers have numerous industry standard certifications from leading certification bodies including SANS (GCIH, GPEN, GWAPT, GMOB).

We are experienced, passionate and motivated security professionals with more than 15 years of experience in penetration testing.

Our customers

Our customers cover a range of industries including:

- Finance/banking
- Energy and utility
- Government
- Telecommunications
- Retail
- Media and entertainment

References can be provided upon request.

PENETRATION TESTING

Performing a penetration test is a small cost compared to the loss that may result from a successful security breach of a business' critical systems.

Business critical systems, the information they store and process are one of the most valuable company assets. A security breach of these systems can result in significant financial, legal and reputational loss - it is critical they are protected.

Penetration testing is a globally recognized security measure that can help provide assurances that a company's critical business infrastructure is protected from internal or external threats.

During a penetration test, the target information system or application is tested for security vulnerabilities using the same approach that cyber criminals would use to penetrate the systems and gain unauthorized access to a business' information.

Unlike a real attack, a penetration test is a controlled, organized and legitimate process performed by security professionals. All activities are carefully planned and monitored in a controlled environment, to minimize the risk and mitigate the impact on the target information system or application, whilst simulating real attack approaches as close as possible.

In addition to revealing critical vulnerabilities, a penetration test can also identify lower-risk security gaps and weaknesses, such as configuration issues. These lower-risk issues may increase a system's risk to a cyber-attack or reveal useful information about infrastructure to attackers.

Regular penetration testing is considered a key part of best practices in information security management and a requirement of various standards, laws and regulations (e.g. PCI DSS).

Penetration testing vs. vulnerability scanning

Penetration testing and vulnerability scanning are differing services based on the nature of their complexity, testing methodology and final results. It is not uncommon for companies to offer automated vulnerability scanning services as penetration testing services. However, an important difference between a vulnerability scan and a penetration test is the former is a fully automated procedure, while the latter assumes active and often manual practice carried out by a security professional who is experienced in ethical hacking.

Although vulnerability scanning tools are useful for detecting so-called "low hanging fruit" vulnerabilities, their ability to detect flaws in complex applications or business logic is very limited or nonexistent.

INFIGO IS provides both vulnerability scanning and penetration testing services, with a clear distinction on the final deliverables and business value to the customer. In order to provide added value to our vulnerability scanning services, INFIGO IS experts will perform additional, manual verification of results in order to remove the most obvious false-positives, which are very common with automated scanning tools. If you are not sure on which service would be most appropriate and beneficial to you – contact us and we would be happy to discuss benefits and drawbacks of either service.

OUR SERVICES

We offer the following penetration testing services:

NETWORK PENETRATION TESTS

- **External penetration test** – simulates an external attacker trying to penetrate your network from the Internet. Depending on the approach, the test can be performed from the perspective of an anonymous Internet user (black box), however can be modified to also include a privileged/authenticated attack to certain system components or applications exposed on the Internet.

- **Internal penetration test** – performed from the internal network in order to identify how vulnerable your systems are to internal users (staff, contractors, third-party suppliers, vendors, etc.). The test can be performed from the perspective of an anonymous or authenticated internal user (typically the credentials of a standard domain user are used).

We pride ourselves as being on the cutting edge of security research and publish regularly in this area.

APPLICATION PENETRATION TESTS

- **Web application penetration test** – assesses how vulnerable your internal or external public web applications are. This is one of the most common penetration tests, as web applications are generally among the most exposed and vulnerable components of any information system. The test will identify the most common web application vulnerabilities according to the OWASP methodology including but not limited to:
  - Injection vulnerabilities (SQL, LDAP, command, Xpath etc.)
  - Cross Site Scripting,
  - XML vulnerabilities,
  - Cross Site Request Forgery,
  - Authentication and authorization weaknesses,
  - Encryption vulnerabilities,
  - Business logic vulnerabilities,
  - Directory traversal and much more...

Special attention is focused on the business logic vulnerabilities. Such vulnerabilities generally cannot be identified with automated vulnerability scanning tools, as they are largely agnostic of the application or workflow. However these are often the most critical, since they impact upon the business directly. Our experts ensure all potential business vulnerabilities are thoroughly examined and tested.

- **Mobile application penetration test** – with the massive growth and usage of mobile technologies, mobile application penetration testing is increasingly more important for companies, especially in the banking/financial sector. This penetration test covers different attack scenarios against the most popular mobile platforms including Apple's iOS, Google's Android, Windows and Blackberry. In addition to targeted attacks on the mobile application/device, the test also covers the server side of the application responsible for handling user requests. The test includes the following:
  - Application reverse engineering,
  - Analysis of crypto operations,
  - Security of sensitive data at rest and in transit,
  - Authentication and authorization weaknesses, etc.

Similarly as with web applications, special consideration is given to identify potential logic or business vulnerabilities.

- **Thick client penetration test** – a penetration test similar to the mobile application test, but the target is a thick/fat client running on the user's computer (i.e. a Windows application). The test covers client and server side vulnerabilities.

WIRELESS TESTING

- **Wireless penetration test** – testing to assess the possibilities of breaking into a corporate network via the wireless network. The test is carried out with specialized equipment and tools in order to ensure complete and accurate results.
- **Identification of wireless access points** – an assessment of a wireless network to identify unauthorized access points, which might be exploited by an attacker. The test can also identify and map areas of wireless accessibility. This type of test is specifically required by the PCI DSS standard.

SOURCE CODE REVIEW

Security test that identifies vulnerabilities through a review of source code instead of performing the test against the live production system. The test is carried out as a combination of manual review procedures and automated testing with specialized source code review tools.

INFIGO Information security

www.infigo.hr

PCI DSS

PCI DSS requires that internal and external penetration tests are performed annually in order to ensure that cardholder data is protected from unauthorized access; both network and application tests are required.

INFIGO IS can help define an appropriate penetration testing methodology and perform penetration tests that are fully aligned with PCI DSS requirements.

In addition to our dedication and passion for vulnerability identification and exploitation, we respect the sensitivity of our mission, and carry this work out with diligence to ensure all activities are performed with due care, consideration and caution.

DELIVERABLES

Our penetration test reports are written with care in order to ensure that all findings identified during the test are clearly communicated to the target audience. Our reports are aimed at both technical professionals and management; two key stakeholders for IS security.

Technical reports include detailed vulnerability descriptions (with examples of exploitation), recommendations for mitigation with detailed references, and CVSS scores. Technical personnel are provided with precise information on vulnerability removal and security improvements.

Management is provided with a short summary of the test including graphical visualisation and video demonstrations of critical vulnerability exploitations (where applicable). The management report provides insight into the overall security position of the organization and adherence to regulatory/compliance requirements.

INFIGO Information security

INFIGO IS d.o.o., Karlovačka 24a, 10020 Zagreb, Croatia
phone:+385 1 4662 700 / fax:+385 1 4662 701 / info@infigo.hr / www.infigo.hr