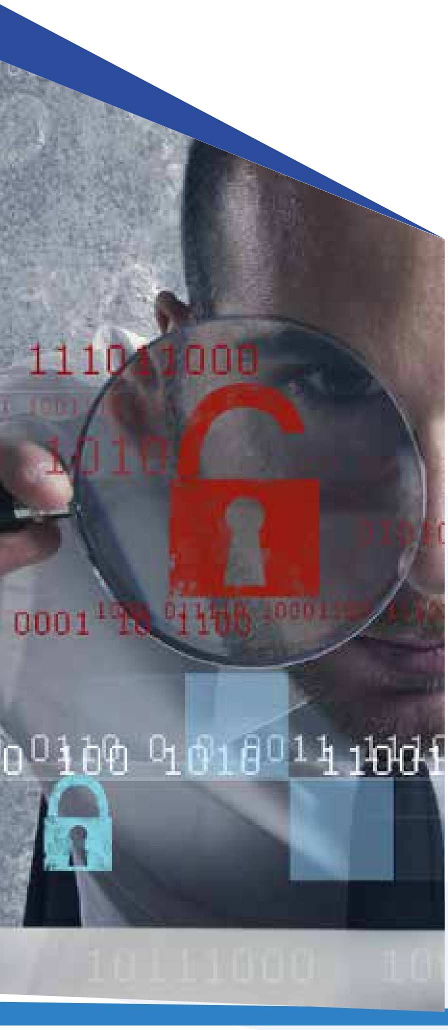
Digital Security

Cyber Security

The degree to which your computer system is vulnerable

The operations suitable for IT property security, thanks to our Cyber Security services, with solutions for every need.

Vulnerability Assessment and Mitigation



The Vulnerability Assessment and Mitigation (VAM) method adopted by the INSIDE Cyber Security Division consists of a series of non-invasive activities aimed at **evaluating the effectiveness and strength of the security systems** used by your company, and identifying known vulnerabilities in case of a cyber attack. These initial intervention phases are followed by the adoption of countermeasures aimed at improving the security of your systems.

VAM should be implemented in various stages throughout the year, since the technology is constantly developing, as are the tools used to attack systems.

The INSIDE Cyber Security Division develops the following levels of VAM:

- **Data Base**: our analysis focuses in particular on the DBs mostly commonly used by companies (Microsoft SQL Server, Oracle, SYBASE Server, etc.). The assessment is done using highly sophisticated tools and software, and includes an automatic scan of these databases to identify and analyse weak points that are prone to attack. All companies "store" their business information in these types of databases, which, being constantly reorganised for better use, are exposed to attacks by parties with malicious intent, such as competitors.
- **Telephone Network:** an attack on a telephone network is commonly known as 'war dialling'. It is a frequently used form of computer attack, as the telephone network is more vulnerable due to the presence of bugs. The attack involves automatic scanning of an entire telephone network, including switchboards, modems and telephone equipment.

Penetration Test

An evaluation of the security of a system or network

The Penetration Test is a service for assessing the security of a system or network through the simulation of an external or internal attack by a threat agent. The aim is to highlight the weaknesses of the platform, providing the greatest amount of information on the technological vulnerabilities that have enabled unauthorised access: it essentially involves putting ourselves in the shoes of the hacker, who exploits detected vulnerabilities to obtain information required for access to the computer infrastructure.

Web Application Penetration Testing

Computer security tests on web applications

With the advent of e-commerce, companies are increasingly using the web to promote and sell their products and/or services. The INSIDE Cyber Security Division conducts prevention and safety activities on all the web applications used by companies.

The process involves scanning and monitoring all the sections of the web application, with particular attention to areas protected by usernames and passwords, which, when entered, allow access to the services offered through HTTP or HTTPS protocols.

The work involves the following security fields:

- Scanning of sensitive data sent via the application and exposed to risk of interception by malicious parties, through an examination of the HTML code, scripts or other information that can be obtained through debugging mechanisms;
- Thorough analysis of interactive fields between the application and the user to identify any gaps created by (in)voluntarily input;
- Authentication procedures;
- Resolution of issues related to a specific session, such as timeouts, logouts, hijacking, logins using unverified addresses, etc.
- Validation and alterability of data;
- Execution of commands in unexpected areas of the application, for example, through specific SQL strings, which can lead to the direct manipulation of the database, with the possibility of acquiring, modifying and deleting stored data;
- Incorrect or inappropriate interactions with the operating system (shell escape).

Threat Detection & Analysis

Via our testing and verification process, protect your business from any hostile hardware or software (such as viruses) that may damage or forward sensitive data. Contact us now for a free consultation.

Computer Hacking Forensics

The digital generation is changing the workplace. Companies are increasingly using new technologies such as cloud computing, mobile technology, big data or IoT, rendering them increasingly vulnerable to cyber-attacks. It is therefore essential to know if your information has been manipulated, or if it is being monitored in any way. The activities of Computer Hacking Forensics conducted by Inside Agency identify any traces of a possible intrusion by correctly gathering the sources of evidence necessary to document the occurrence of such.

Computer Counterintelligence

Inside Agency detects the degree of **vulnerability of its clients' IT systems** and, following a careful diagnostic analysis, identifies the **appropriate interventions for the security of IT property**.

To provide the best possible support, Inside Agency has united the best expertise in the field of security, offering specific consultancy services for the execution of each analysis activity, with the aim of protecting the most important assets or **company know-how**.

Nowadays, the ways to find illicit information are constantly expanding. The digital revolution has favoured the birth of the so-called computer espionage, which affects individuals, but even more frequently, companies. How can you protect yourself? **Prevention** is the key!

Thanks to scrupulous counterespionage investigations, Inside Agency identifies and eliminates the danger, revealing any acts of espionage.