C&W Social Engineering

Identify vulnerabilities in your processes which may be exploited by tricking your employees and work on improving internal policies to prevent information leakage.

The most valuable asset of any company is information. This is why it is so important to take care of it, not only at a technology infrastructure level, but also in terms of the information management performed by the company's employees to prevent said information from being stolen.

C&W Social Engineering is a service that seeks to detect the non-technical shortcomings of existing security through multiple social engineering techniques and human interaction.

C&W Social Engineering aims to produce an extensive report in order to close any gaps found in the processes policies, and users' training before a malicious attacker detects them.

Services

Passive Internet Recognition

Using public access sources such as websites, search engines, and DNS records, all relevant information will be gathered, such as names, positions, phone numbers, and email addresses available online of the company and its employees.

External social engineering

Social engineering will be performed by making phone calls to people within the company. The purpose of these calls will be to induce users to disclose sensitive information over the phone, thus violating the company's information security policies.

Attacks through email, "phishing"

Emails will be sent to individuals and groups within the company to entice users to click on an external link that will either try to get sensitive information or deliver a malicious download to their desktop, that may include buffer overflows to the browser and/or operating system, trojans, and keystroke loggers.

Questions we have to answer

How can I know whether employees are aware of common threats to information security?

How can I know if my employees write passwords somewhere visible or share them with others?

How can I know if my employees apply the company's security policies?

How can I know if there are physical security vulnerabilities that the competition may take advantage of?

How can I reduce the risk of data loss because of a social engineering attack?

How can I prove if the company's confidential information is vulnerable to theft?

Benefits

- Identification of weaknesses in the human factor of security.
- Identification of the most vulnerable areas within a company.
- Reduce the risk of information leakage by employees by their lack of preparedness when faced with a social engineering attack.
- Validation of the operation of the company's processes to prevent a social engineering attack.
- Information to improve the company's training procedures and security policies.

C&W Social Engineering helps to prevent attacks like:

Shoulder surfing

Checking the rubbish
(commonly referred to as 'Dumpster Diving')

Phishing

Forensic analysis

Telephonic cheats

Spam

POP-Up Window Attack

Identity theft