KRYPTON SECURITY
IT SECURITY & CONSULTING SERVICES

EMAIL : INFO@KRYPTONSECURITY.COM
WEBSITE : WWW.KRYPTONSECURITY.COM

Social Engineering Assessment Services (SEAS)

Introduction

Cybercrimes & frauds are increasing at a high rate, Information is invaluable, and the need to secure data and records has become a major concern to all.

IT Security companies such as KRYPTON are engaged by clients every day to help detect weaknesses and increase protection. While there is no doubt that the technical aspect of a penetration testing helps to decrease the threat, this alone is not sufficient; ***the technical effort must also be accompanied with some form of intervention on the human aspects.***

Social Engineering (SE) is a concept and a name given to the matters that deal with the human side of what essentially amounts to breaking into entities where sensitive data can be obtained. Companies, financial institutions and government installations, with all the means for protection and tools such as monitoring software and firewalls, still remain vulnerable to attacks, if an employee willingly or unwittingly gives away some key information.

SE also counts on people's inability to keep up with a culture that relies heavily on information technology. Social Engineers rely on the fact that people are not aware of the value of the information they possess and are therefore somewhat careless about protecting it.

57% of workers surveyed were willing to share their company passwords with their friends.
Source: Infosecurity Europe 2003 Information Security Survey, April 2003

More and more, "hackers" are utilizing SE due to the fact that often the human weakness factor is substantially easier to penetrate than the network vulnerabilities. Again, it appears to be much simpler to "trick a person" into revealing information (e.g. a password from one colleague to another) than to carry out an elaborate "hack" for the same purpose.

Physical security, while frequently forgotten, is no less critical than timely update of critical software, putting in place appropriate password policies, and proper user permissions. One could have the most hardened servers and networks, but that would not make the slightest difference if someone can gain direct access to a keyboard, or worse yet, walk right out of the door with one of your hard drives.

An organization's IT security is only as strong as its weakest link (i.e. the human element!)

By 2017, 40% of enterprise contact information will have leaked into Facebook as a result of employees' increased use of mobile device collaboration applications.
Source: Gartner Symposium/ITxpo 2012

Clients engage KRYPTON to perform Social Engineering Assessments in order to not only establish the level of such strengths [or weaknesses], but also in order to allow the client's management team to gauge the organization's exposure to potential real-world attack scenarios.

Finally, every bit of the implemented network security may be negated by a single unlocked door. Of course, most physical security risks are not as simple to identify or correct as an unsecured entryway.

The average total cost per company that reported a breach in 2011 was $5.5 million.
Source: 2011 Cost of a Data Breach: United States, Ponemon Institute and Symantec, March 2012

KRYPTON's Approach

At KRYPTON we do not just test the technical defenses, but given that we are quite conscious of the human factor, we also focus on this key element within the security and protection equation.

We conduct different types of SE engagements, which range from performing phishing(1) exercises to social media attacks as well as attempts to compromise individuals via phone contact. The engagement can include physical and in-person compromise, where a highly trained KRYTPON expert would attempt to bypass your defense perimeter and gain access to potentially sensitive zones within your offices with the objective of accessing critical data.

KRYPTON will work diligently within a predetermined time frame on breaching the client's organization using the same technical tools and methodologies that are available and in use by malicious actors on the global stage.

Information gathering

KRYPTON will do manual as well as automated research of publicly accessible information sources. This includes, but is not limited to:

i) Internet websites,
ii) presence on social networks or even
iii) direct contact with the target organization in order to attempt to gather any form of intelligence. The results of the above would provide an organization with a much better understanding of its public Internet-based persona.

Planning

During an engagement, KYRPTON consultants identify and construct scenarios that could be used to gain access to restricted areas of buildings or sites belonging to the target organization. The objective of the test would be to evaluate the organization's reactions and to try and gain access to information that is considered sensitive. These scenarios would be discussed with the client, selecting elements that would maximize the effectiveness of test.

Onsite Testing Activities

KRYPTON consultants will make contact with a target organization via the agreed scenarios, either by phone, email or in person and onsite. During this activity, the KRYPTON expert would impersonate a trusted internal staff, an external contractor or even other 3rd parties. The target of these activities could range from obtaining user names and passwords, access to sever rooms or simulation of placing malicious software or devices on the target network.

Remote Testing Activities

KRYPTON consultants will call the target organization or send emails attempting to illicit information from individuals. Remote Social Engineering also includes the testing of an organization through the use of phishing attacks or use of "malware" (e.g. Trojans) sent to infect the target company's systems.

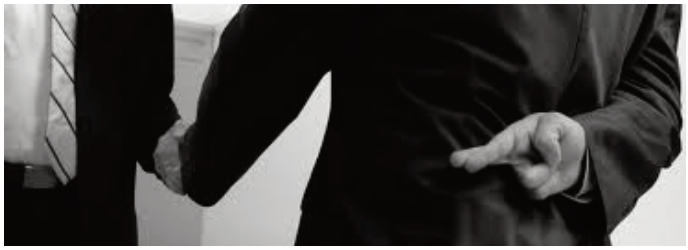
KRYPTON services do not stop there, in that we will also make sure that ***every SE engagement is a learning experience for your staff***, so they would be more aware and better prepared for when the real attack occurs. Of course, KRYPTON is always prepared to conduct additional training or T3 sessions to increase the level of awareness and preparedness even further.

Deliverables

KRYPTON delivers a detailed and comprehensive report at the conclusion of each Social Engineering assignment that includes an executive summary, details of scenarios used that could be the source of attack on the organization, including illustrative walkthroughs supported by videos and photographs. The report will also contain recommendations for the client's management team on how to improve their protection when it comes to potential dangers of Social Engineering attacks.

"All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."

Sun-Tzu: The Art Of War



(1) Phishing is the act of attempting to acquire information such as usernames, passwords or credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity.