TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Social Engineering Campaigns

So as to be able to sufficiently protect information values of a company, the persons responsible should be informed about all existing methods to obtain or manipulate intragroup-data. Taking into consideration a broad variety of factors, it quickly becomes evident that often times the causes for security breaches are not to be found in technical vulnerabilities. By manipulating employees, adversaries attempt to enter company premises, gain access to IT-infrastructures and steal or tamper with business-critical or customer-sensitive data.

(Social-) Hackers make use of multifarious instruments: They take advantage of the employees' benevolence, unawareness, comfort and trust, thus making them unknowing accomplices. This does not have to be the case! Apart from implementing appropriate technical security measures and contingency plans, an efficient IT security concept requires all staff members to be sensitised with regard to information security.

With the help of social engineering campaigns tailored to your individual needs we will support you in gaining insight into the current security level of your company. The results can serve as a basis for adequate measures to sustainably strengthen the security awareness of your employees.

Approach

Upon consultation with you, our experts will act like "real" adversaries and try to obtain information without being given login credentials or inside knowledge. For planning and conducting social engineering campaigns we apply a methodology called "social engineering attack cycle":

I. Research and Preparation

Initially, it will be attempted to gather as much information about your company as possible. The greater the amount of information available, the easier will it be to build a relationship of trust.

II. Pretexting

For every attack scenario simulated a pretext-story will be invented to camouflage the attack as a regular procedure or to distract from the actual attack. The primary objective here is to establish a relationship of trust with one or several employees.

III. Exploiting

This position of trust will now be used to perform the attack. During this phase our experts will try to gain the desired entry, admission or access to your IT-infrastructure.

IV. Collecting, Analysing and Evaluating

Provided access has been gained successfully, it will then be tried to collect as much inside information as possible. The data thus obtained can either be analysed while the attack is still in progress to deduce opportunities for further-going attacks or it can be examined and evaluated a posteriori.

This basic methodology allows for various types of attack

TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

scenarios - customised according to your individual needs - to be performed (excerpt):

- Phishing: Attempt to gain sensitive information that can be used for an attack, mostly by means of forged e-mails.
- Vishing: Attempt to entice users to disclose sensitive information via phone calls (voice phishing).
- Entrance by Persuasion: Attempt to gain physical access to company premises in order to access internal IT-systems and networks.
- Tailgating/Piggybacking: Attempt to enter secured areas by inconspicuously following employees, e.g. by holding the door open.
- Alternative Access Paths: Examination of the site in search of possible alternative way to access internal networks, e.g. wireless networks, mobile devices etc.
- Baiting: Distribution of bait locally or via postal services, functioning as a Trojan horse. Usually this refers to prepared USB-sticks.

All of the above mentioned methods as well as all actually conducted attacks are performed carefully so that no actual harm will arise.

Your Benefits

- Insight into the current protection level of your company and the degree of your employees' security awareness
- A management report listing the performed attacks, the state of affairs concerning the security level as well as a catalogue of measures with recommendations on fixing identified vulnerabilities
- Laying the groundwork for security awareness measures to enhance and evaluate the overall awareness regarding the handling of sensitive company information
- The actual occurrence of threat scenarios that were beforehand only theoretically outlined will ensure the emotional consolidation of the learning experience
- A periodic combination of social engineering and security awareness campaigns will enable you to protect your company in a sustainable manner

TÜV TRUST IT GmbH
TÜV AUSTRIA Group

Waltherstraße 49–51
D-51069 Köln
Phone: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Phone: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com