SOCIAL ENGINEERING

COMMON TYPES OF ATTACKS

There are various techniques that a criminal may use to infiltrate your business.

Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Pretexting

Pretexting is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.

Tailgating

An attacker, seeking entry to a restricted area secured by unattended, electronic access control, simply walks in behind a person who has legitimate access. Following common courtesy, most people will hold the door open for them.

Quid Pro Quo

Quid Pro Quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service such as technical support.

Dumpster Diving

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network.

Baiting

Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that hackers use to entice.

EUROPA IT

Network, Telecom & PC Support

SOME EXAMPLES:

Attacker calls random numbers at a company, claiming to be from technical support. Eventually, they reach someone with a legitimate problem. Grateful tech support called them back, they will follow the attackers instructions. The attacker will "help" the user, but will really have the victim type commands that will allow the attacker to install malware.

Attacker creates USB Flash drive with malware on it and puts a label on it that sparks curiosity. Label might say something like: 2016 Financial Data or Employee Performance Reviews. Attacker then leaves the flash drives in places they can be found by a target company employee. A curious employee finds the flash drive and plugs it into their computer to see what is on it and unknowingly installs malware so the attacker has access.

COUNTERMEASURES

- Standard Framework: Establishing frameworks of trust on an employee/personnel level (i.e., specify and train personnel when/where/why/how sensitive information should be handled)
- Scrutinizing Information: Identifying which information is sensitive and evaluating its exposure to social engineering and breakdowns in security systems (building, computer system, etc.)
- Security Protocols: Establishing security protocols, policies, and procedures for handling sensitive information.
- Training to Employees: Training employees in security protocols relevant to their position. (e.g., in situations such as tailgating, if a person's identity cannot be verified, then employees must be trained to politely refuse.)
- Event Test: Performing unannounced, periodic tests of the security framework.
- Review: Reviewing the above steps regularly: no solutions to information integrity are perfect.
- Waste Management: Using a waste management service that has dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff.

EUROPA IT

Network, Telecom & PC Support

Visit us: www.europait.net

Call us: (802)275-4848