Week 1 cyb

Technology, Information Technology

Week CYB Week CYB Tiger Team As an independent group whose objective was to challenge and eventually improve the effectiveness of the security system of Symbolic Motors, the Tiger Team applied the penetration testing aspect of red teaming. This was achieved by viewing the security problems from the point of view of an adversary.

The actions of the team are mainly based on wireless and wired hacking, social engineering and entering buildings without being granted legal access by breaking into them. It is through such means that the Tiger Team is able to establish that a skylight on the roof is one of the organisation’s security weaknesses as it will provide them with discrete access into the car dealer’s premises.

They challenged the assumption that every potential buyer who walks in the showroom is genuinely interested in buying a car and photographed motion sensors and cameras in the building. They then used a rogue wireless access point and carried out social engineering to gain access to sensitive information on customers.

This means that security at the organisation was highly compromised because, apart from the customer information, the collection of the expensive, luxury vehicles was also easily accessible to potential thieves, and the Tiger Team actually made away with one.

The security at the organisation is not yet perfect, and ways in which it could be defeated include the ability of intruders to gain physical access into the premises unless the building’s design is improved. Then, since the Tiger Team was able to install a rogue camera that filmed the alarm keypad without being noticed, it means the organisation does not carry out regular

inspections of its installed devices.

Challenging Assumptions

It is often assumed that computer systems can best be protected by practicing cyber hygiene. However, this assumption can be challenged because most devices' default settings are configured by the manufacturers to facilitate their ease of use at the expense of security. The result is usually vulnerabilities that do not require experienced hackers to exploit. Essentially, this means that any user of a system, and not necessarily a hacker, is a potential threat to its security. The Internet has grown into a concept that relies on an interwoven system of trust for its security. However, guest users of a system may stumble upon administrator accounts which grant them higher degrees of control of other computers' settings and programs (Pelgrin, 2013).

Approaching such a situation from a red teamer's perspective, it is easy to see that a user can breach the assumed trust and develop malicious intentions the moment he discovers he has stumbled upon such administrator rights.

Therefore, the ease-of-use standards to which computers are set are not only convenient for genuine users but also compromise the purpose of cyber hygiene and make systems vulnerable to cyber crimes.

While cyber attackers will routinely search for and exploit possible flaws and programming errors, cyber hygiene often tends to be structured and the attackers will easily know how to circumvent most of the security measures put in place (Pelgrin, 2013). Further, the technical team that installs and implements the cyber hygiene protocols can give away the information to an

adversary at a price.

References

Pelgrin, W. (2013). Cyber hygiene with the top 20 critical security controls. Cyber Security Newsletter, 8(12), 1.