Physical Penetrations; The Art Of Advanced Social Engineering
Scott Higgins
22 February 2001

Introduction

If you ask an Information Security professional to tell you about their security architecture they will probably rattle on about Intrusion Detection Systems (IDS), Firewalls (FW), and AntiVirus (AV). The subject of physical security may come up after all the current day buzzwords for security have been thrown out. In actuality, physical security may not come up at all. When we think of physical security we visualize cipher locks, electric fences, huge vault doors, guards, and the like. These devices are intended to keep the unauthorized individuals out and keep the honest people honest, as the saying goes.

ABSTRACT

What this paper intends to address is the specific situation of someone gaining access to your facility by defeating your physical security utilizing social engineering techniques. Realizing that this type of attack would hopefully only be able to succeed in a large business with at least 100 employees. However, much depends on the security atmosphere in the organization. If users are not aware of their environment and the people they work with then this attack has a high probability of success in smaller companies.

MAIN

In industry this type of activity is commonly referred to advanced social engineering. Why is it called advanced social engineering you ask? Typically social engineering is conducted in a non-face to face interaction. A person calls up and claims to be so and so from the Information Technology division and is installing some new type of software on your machine and needs your password to complete the process, or some similar scenario. The user may or may not give it to them. The user does not see the individual at any time during the conversation.

How does an individual gain access to an establishment that has guards checking for the proper identification? Have you ever experienced the lunch rush at a large corporation or the 0900 get to work on time rush? Most security guards randomly check badges and ID in order to facilitate the egress or ingress of the entire building. No one wants to impede the flow of traffic and be subject to everyone’s directed anger. An individual can easily gain access during this period of high activity. In addition, usually wearing something that resembles a building badge will be enough to get by security. They usually key on 1) Is the person wearing a badge and 2) Is the color of the badge the correct one for this building, if different colors are used. The human factor here is the capability of the guards. How well can they pick someone out of the crowd that does not belong. This is usually the easiest barrier to defeat. A solution would be to place a scanning mechanism in addition to the guard to assist in verifying authorized workers. This way you would have in essence two layers of security. The scanner would authorize entrances and exits in addition to the guards. After gaining access the only security mechanism left is to rely on your employees to question unknown individuals as to their business. Unknown in this sense implies individuals who a person does not know or has any legitimate reason to be where they are.

The next question is where does a non-employee usually find valuable information in an office full of legitimate employees? One place is right on top of their desks, to include the Vice-President’s and President’s offices. Are file cabinets locked? How difficult is it to get into the communications closet where all the telephone and network communication links terminate? Casually strolling around the office while other employees are busy doing everyday work an individual can easily browse through desks and empty offices. Usually no one will question them unless it is their desk or office. Copying faxes, and printouts is another way of gathering data. Another way is by interacting with the company’s legitimate employees during lunch or on breaks. By either listening to or interacting with employees, valuable information can be extracted. The company employee thinks nothing of some one asking questions that would otherwise raise their suspicion if they were not “inside the company.” In addition, a person could attach a lap top computer to any of your Intranet drops and run a sniffer to collect sensitive or proprietary data.

How do penetrations succeed? A large number of security problems arise due to a lack of awareness on the part of a company’s employees of the company’s policies and procedures regarding information security and protection. If employees and contractors of a company do not know the proper procedures for handling proprietary or sensitive information, they are much more likely to allow that information to be left unprotected. If employees are unaware of the company policies on discussing sensitive company information, they will often volunteer (sometimes unknowingly) information about their company’s future sales, marketing, or research plans simply by being asked the right set of questions. Many penetrations succeed because people often do not pay adequate attention to the situations and circumstances in which they find themselves. The art of social engineering relies heavily on this fact. Social engineering is a con game used by intruders to trick people who know secrets into revealing them.

Another often-overlooked situation is the cleaning team. The nightly cleaning team usually has unrestricted and unescorted access to all of a company’s office area and information. It would be extremely easy to temporarily get hired onto a contracted cleaning team for several days in order to browse a company’s files, desks, trash, and even implant devices for gathering information. A New Zealand firm makes a device called KeyGhost that installs in line with the keyboard connector that captures everything that is typed on the keyboard. It comes in several different configurations and supports encryption of the stored data. The most basic one, which stores data unencrypted, can hold 10 days worth, approximately 97,000 keystrokes, of data before if fill s its capacity. How many of us actually look at the back of our computer to examine the connections? An individual could install it one night and retrieve it several nights later with all the keyboard strokes captured. This also applies to some one posing as an employee for a single day and retrieving it at the end of a day.

In addition, there are numerous other facets of social engineering that could be exploited. If your Internet services are contracted out to a third party they usually incur all the maintenance requirements. Do you know who works for them? Do you know if they are trust worthy? Are they running a sniffer on your network or planting a KeyGhost device. A security professional needs to be ever vigilant to office sign in/out procedures. Are escorts required or verification of services needed before they can gain access to your network? A commonly used practice is to impersonate a telephone repairman. Does any phone actually work correctly? The odds are that a person in the office will be experiencing phone problems and want them fixed.

How does a Chief Information Security Officer combat these types of attacks? A company can employ the same techniques that a potential hacker or attacker would use to evaluate their social engineering vulnerabilities. This type of penetration testing is a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system's or organization's resentence to such an attack. A penetration test can sometimes be used to bolster a company's position in the market place. A test, executed by a reputable company and indicating that the subject's environment withstood the tester's best efforts, can be used to give prospective customers the appearance that the subject's environment is secure. A penetration test can be used to alert the corporation's supper management to the security threat that may exist in I ts systems or operations. A well-executed penetration test can systematically uncover vulnerabilities that management was unaware existed.

Training your employees is another way to combat social engineering. Training takes on a similar essence of how to detect spies and the like. Security education and awareness programs rarely, if ever, address this type of attack to watch for. How could they if a company has 1000s employees? Security education supported by situational awareness training would provide a large extent of the training required to combat this attack. Training must include any guards that are employed also. Before any attempt is made at entry, an individual will usually perform some type of surveillance of the security features. For example, what is the traffic flow during peak hours, do the guards scrutinize everyone entering and exiting the building or do they casually glance at some one every so often. Inform the guards to be aware of individuals hanging around close to the building maybe taking notes or drawing diagrams. Employees should be reminded to stay alert for individuals they do not recognize. Employees should also be encouraged to challenge individuals when they feel the need. Any person that is wondering around will stand out and should be challenged. It will be the individual employees that stop the advanced social engineers. They are on the front lines of this battle. They need to be trained and equipped with the proper tools in order to be successful.

CONCLUSION

Social engineering is an art used by hackers and the like to capitalize on the weakness of the human element of information security. Employees are going to socialize with each other weather they actually know each other or not. A Chief Information Security Officer needs to realize this and turn it into a tool for use in information security. By having employees educated in information security, they can realize when something is amiss and needs to be investigated further. Face to face interaction allows people to read body language and determine other actions that do not fit with the situation. Security and situational awareness training will allow a security professional to add all the company's employees in his fight against advanced social engineering. Penetration testing can be a valuable tool for understanding and improving the security of a computer or computer network. However, it can also be used to exploit system weaknesses and attack systems and steal valuable information. By better understanding social engineering and the tactics employed by its practitioners, a well defined defense and training program can be devised to deter it.

All the issues brought to light in this short paper can all be mitigated to a certain extent. What is absolutely necessary is a strong Information Security policy addressing these issues. A strong policy serves as a good foundation for a start and we must start somewhere.

SIMILAR TOPICS

Competitive Intelligence

Open Source Intelligence Gathering

Counterintelligence in Information Security

REFERENCES

www.totse.com/en/politics/political_spew/milimpst.html

http://www.infosyssec.com/infosyssec/physfac1.htm

http://cseng.awl.com/book/toc/0,3830,0201433036,00.html

http://www.keyghost.com

http://www.combsinc.com/handbook.htm

http://www.cio.com/CIO/arch_0695_cicolumn.html

http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html

My eleven years of intelligence & counterintelligence activities in information security operations and investigations working with the DOD, CIA, FBI, and NSA