Master Thesis
Computer Science
Thesis no: MCS-2008:13
March 2008

Social Engineering and Internal Threats in Organizations

Miguel Tames Arenas

Department of
Computer Science
School of Engineering
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

This thesis is submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Supported by the Programme Alβan, the European Union Programme of High Level Scholarships for Latin America, scholarship No E06M101896MX and by the Mexican scholarship programme CONACTY, scholarship No 206379.

Contact Information:

Author(s):
Miguel Tames Arenas
E-mail: migueltames@yahoo.com

University advisor(s):
Dr. Guohua Bai
E-mail: gba@bth.se

Department of
Computer Science
Box 520
SE – 372 25 Ronneby
Sweden

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : +46 457 102 45

Abstract

Organizations are taking computer security more seriously every day, investing huge amounts of money in creating stronger defenses including firewalls, anti-virus software, biometrics and identity access badges. These measures have made the business world more effective at blocking threats from the outside, and made it increasingly difficult for hackers or viruses to penetrate systems. But there are still threats that put organizations at risk , this threats are not necessary from external attackers, in this paper we will analyze what are the internal threats in organizations, why are we vulnerable and the best methods to protect our organizations from inside threats.

Keywords: social engineering, computer security, risks, threats.

CONTENTS

INTRODUCTION

Today, more than never before, security threats are an important issue for every organization, no matter what they do or where they are. Most of these security threats are well identified and there is a wide range of techniques to protect systems from those threats, security audits are also an important tool in detecting this type of threats but there is still an increasing need for protecting systems from inside the organizations itself.

According to [15] during 2006 there was an incredible increase in security attacks, but most of these security attacks are related to vulnerabilities within Internet Browsers that allow attackers to download malicious code in background or luring users to malicious websites via SPAM or Phishing, this type of attacks are specifically directed to users, whether at home or inside organizations.

Inside attacks are most of the time given less priority than external attacks nevertheless inside threats is becoming an increasing concern in most organizations. In the 2005 global business security index report, IBM identifies an increasing trend towards small, specific attacks rather than mass attacks like virus or SPAM.[17] and in his 2006 report "Stopping insider attacks" [14] IBM suggests that the prioritization of external threats over internal dangers is misguide and this allows attackers to exploit security risks in the organization's security strategy.

When talking about security threats, there is a wide range of tools available in the market which work extremely well against attacks (when properly installed, monitored and updated), but still, there are security problems in organizations involving data security in most cases the worst security issues always involve the human factor inside of the security perimeter.

Currently most research papers are done within the "technical" areas of Computer Security, either in the Network Security area (Firewalls, IDS, Wireless Encryption Methods) or in the Software Security (Buffer Overflows, Virus, Malware) But the "Social" part of the Computer Security has been left behind as if it was not crucial in the process of protecting information systems and still when taking a look at recent security attacks in organizations, inside employees are always the target in this attacks , making humans the weakest link in the corporate security policies.

On the following chapters we will discuss what are the techniques used in Social Engineering attacks and other internal threats like Phishing and Spyware and what are the differences between a group of users with formal training in security policies and a group of users without training, this way we would be able to identify whether or not security policies play an important role in protecting organizations against external attacks.

CHAPTER 1

BACKGROUND

1.1 Background and Related Work

In previous years, computer attacks were single mass-broad attacks directed to penetrate as many systems as possible and to cause as much damage as possible without specific goals, but in recent years attacks have became complex and user specific attacks, this multi-threat attacks use several different attack techniques to avoid being detected by current protection systems. Organizations using traditional protections systems are at risks from being attacked by modern malware methods or techniques.

The malicious code used in modern attacks has more devastating consequences than worms and viruses of the previous era. Many existing protection systems are inadequately prepared to stop new forms of malicious code. Largely signature-based, these legacy security products rely on known attack signatures. When one of these attack signatures is recognized the older security systems sound an alarm and may attempt to block the attack. Signature-based protection can only prevent known attacks however. Hackers recognized the weakness of a signature-based defense and began to develop new zero-day attack.

One important characteristic on modern attacks is that they focus on the weakest link in the security chain, this is, humans. As suggested in [1] “Social Engineers attacks can succeed when people are stupid or, more commonly, simply ignorant about security practices”.

Social Engineers attacks are mainly directed to users and thus during this research we will focus on these types of threats or what we call “Internal Threats”.

1.2 Traditional Threats vs. Internal Threats

Traditional security threats are those aimed to affect security vulnerabilities in network devices in organizations, devices with access to the external world, devices that, if properly configured and regularly updated, are safe. Examples of these traditional security threats are shown in Figure 1.1 and they include Denial of Service or unauthorized network access, Denial of Service is aimed to overload network devices or servers by flooding with requests of service and unauthorized network access attack is directed to trespass external protection to illegally access internal networks. All these types of attacks have something in common; internal users in the organization are not directly targeted in the attack.

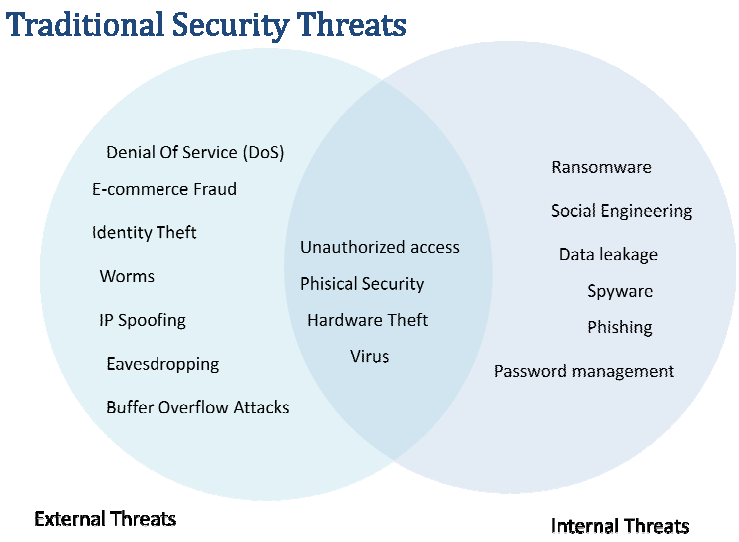

Figure 1-1

In this research we will make a difference between Traditional Threats and what we call “Internal Threats”, We will refer to Internal Threats as threats in which internal users or employees play a important part in the attack by being the first target of the attackers, this type of threat can not succeed without the user’s participation. Internal Security Threats will be the main topic in this research. Examples of these types of attacks are shown in figure 1.2 and will be explained in detail in chapter 3.

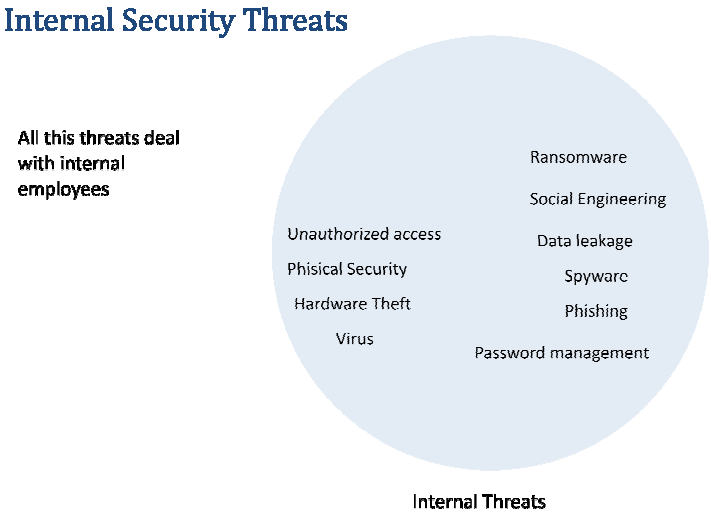

Figure 1-2

1.3 Statistics

In the 2007 Internet Security Threat Report from Symantec [8] we find interesting statistics numbers about the new trends in attacks, this shows that the new generation of attacks are increasing, particularly targeting the financial sector, making this type of attacks a high priority risks in banks.

Another interesting data is that Web-vulnerabilities and Trojans are particularly high in recent years, this is relevant in this paper because web-vulnerabilities and Trojans are directly related with users therefore the chances of a successful attacks will be affected by the level of user competence or knowledge in the information security area.

Finally another relevant data in these statistics is that insecure policies and the theft or loss of computer or another data-storage medium were also an important percentage in the total incidents in 2007. These type of vulnerabilities can be easily reduced by giving users a proper training in handling corporate information and by having specific security policies for corporate assets management.

Following is the list with relevant statistic information from the 2007 Internet Security Symantec Report.

- The Symantec network detected a total of 196,860 unique phishing messages, an 18 percent increase over the last six months of 2006.

- Financial services sector accounted for 79 percent of the unique brands that were used in phishing attacks.

- The second most common cause of data breaches that could lead to identity theft during the first quarter of 2007 was insecure policy, which made up 34 percent of all incidents.

- Sixty-one percent of vulnerabilities disclosed during the first half of 2007 affected Web applications.

- During the first half of 2007, Trojans made up 54 percent of the volume of the top 50 malicious code reports.

- Of the top ten new malicious code families detected in the first six months of 2007, four were Trojans, three were viruses, one was a worm, and two were worms with a virus component.

- Spam made up 61 percent of all monitored email traffic.

- In the first half of 2007, the primary cause of data breaches that could facilitate identity theft was the theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a back-up medium.

CHAPTER 2

PROBLEM DEFINITION

People are always the biggest problem regarding security issues, this is mainly because they are the only element within the secured environment that has the ability to choose to violate the rules. People can be coerced, tricked, or forced into violating some aspect of the security policies in order to grant access to someone.

Protection against social engineering is primarily education[9]. Training personnel about what to look for and to report all abnormal or strange interactions can be effective countermeasures. But this is only true if everyone in the organization realizes that they are a social engineering target. In fact, the more a person believes that their position in the company is so minor that they would not be a worthwhile target, the more they are actually the preferred targets of the hacker.

2.1 Research Motivation

Social risks or risks caused by human behavior has been underestimated in recent years, unlike the traditional risks that we discussed in chapter one (virus, buffer overflow attacks and unauthorized access attacks), Social risks require a different approach when implementing security defenses in organizations. Currently most of the security solutions in the market include only "technology" mechanisms to countermeasure security attacks from traditional threats therefore we identify a gap in this area, we believe that a different approach should be used when working against internal threats, an approach where user training and security policies are the main tool to fight against these type of threats.

2.2 Research Questions:

- How important is user training in preventing security violations?
- How can we avoid Social Engineering attacks and internal threats?
- How different organization environments affect the way users react to this threats?

Q1 – How important is user training in preventing security violations?
By analyzing the responder's answers from a carefully formulated questionnaire we can confirm whether security policies or user training makes a difference in the users behavior when dealing with specific information security risks.

Q2 –How can we avoid these threats?
By doing a systematic literature review, we can find out what methods are proven to reduce the efficacy of the selected attacks.

Q3 -How different organization environments affect the way users react to this threats?
Through the analysis of the environments where the questionnaire was applied and the answers from the different groups we can identify certain tendencies from the responders.

2.3 Research Methodology

The intention of this research is to effectively identify the role of user training and security awareness in the complex environment of computer security and how important it is for reducing the effectiveness of Social Engineering attacks and in general security attacks directed to users. This will be done by using a mixed method conducting a sequential procedure, trying to derive knowledge based on systematic review of current research on social engineering and computer threats and through observation of human behaviour by formulating a questionnaire where specific questions would be used to identify weakness in the user's behavior when dealing with computer decisions, the questions are mixed in a way that the user do not notice our main purpose and the data from the collection processes from questionnaires will be used in a qualitative way rather than quantitative.

We choose a mixed method because we need to obtain information from human observation and also from external experience on the IT Security topic this could be done by reading prominent literature related to our study. If we use only a questionnaire, we would only obtain knowledge about human behavior and their risks but we will not obtain knowledge about up-to-date information on current threats and best methods to reduce this risks , only by using this mixed method we can identify potential dangerous behavior in users from the user observation process and identify this behavior in recommendations from other authors in prominent literature.

2.4 Delimitation

Despite that there are many type of computer threats, In this paper we will only cover the so called "internal threats" or threats where internal employees are directly involved or directly targeted in the attacks as explained in chapter 1, we will not cover threats or risks that are originated outside the company's perimeter and which doesn't have the employees as main target.

CHAPTER 3

THEORETICAL WORK

3.1 Spyware

Spy programs, or also called "Spyware", are computer applications that gather user's information by monitoring behavior and preferences while surfing on the internet. This data is later sent to third-party software developers for different purposes, could be legitimate or illegitimate purposes.

Spyware can be installed in a computer in different ways: Trojans, which are installed without users consent, visiting websites that contains certain ActiveX controls or malicious code that exploits vulnerabilities in the web-browser, Shareware or Freeware applications that includes Spyware in the installation package. In general, spyware can be installed with or without requesting user's approval and it may not inform about the type of information gathered by the software and how it will be used.

The most common type of information monitored by the Spyware software on average users is (but not restricted to) the address of most visited websites, the search engines websites used by the user, operating system version, software being used in infected computers and user's e-mail addresses.

After the information is processed is then sold to third-party companies that use user's email and behavior patterns to advertised similar products or to send malicious e-mails trying to direct users to fake websites and request sensitive bank information using phishing techniques .

3.2 Phishing

Phishing can be described as an attempt to fraudulently acquire sensitive financial or personal information, such as credit card information or Social Security number by pretending to be a legitimate employee or authority person. Phishing attempt are usually initiated through e-mail, phone calls or Instant Messaging.

Before explaining Phishing further, it is probably important to explain the difference between Phishing and social engineering. In my opinion, the difference lies within the scope of the attacks, and the delivery method. A social engineering attack is targeted towards a single, often specifically selected person (or organization), where a Phishing attack uses techniques used by spam in order to target thousands, or even millions, of users. The difference is, however, not always clear. In fact, one can argue that social engineering is an important part of most Phishing attacks, as they often, to some extent, focus on deceiving humans , others view Phishing as simply social engineering using technical means [1].

3.2.1 Spear Phishing

Spear Phishing is a relatively new technique that does not use the wide attack patterns of Phishing, but instead send highly targeted e-mails. The main idea is to make the receiver believe that the source of the e-mail is someone within the same organization and with some type of authority. While the goal of Phishing is to steal information from an individual, the goal with Spear Phishing is to gain access to an organizations computer system .

This specific targeting makes Spear Phishing much more dangerous than ordinary Phishing, and probably more prone to be used by professional attackers in order to get financial gains, trade secrets or even military information .

Spear Phishing could be seen as the "perfect" mix of social engineering and Phishing, and it seems that it is also a lot more efficient, and dangerous, than ordinary Phishing. It uses a higher degree of authority and the fact that the attackers pretend to be someone that the mark has a relation with.

3.2.2 Spy-Phishing

A "Spy-Phishing" attack consists of the attacker sending an e-mail, or a link, where the mark can download or execute a piece of software, which then installs itself on the selected computers then it monitors traffic until the infected computers visits a specific web site. When the infected computer visits this site the software becomes active, and sends the login info and other sensitive information to the attacker.

3.3 Social Engineering

Social engineering is the method used by an external person to obtain sensitive information from a regular private person or from an employee, usually the attacker pretends to be a legitimate person with some type of authority to request the information. The social engineering attacker usually uses this privilege information to access a system or database by braking passwords or by directly asking for the confidential information.

"Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a Web site, which exploits a technical flaw and allows the hacker to take over the computer."[1]

A social engineer would basically use the phone or internet to fool people and make them reveal sensitive information or to brake typical security policies. By using this method, social engineers take advantage the human tendency of trust people instead of using security breaches on computer systems. The main principle used in Social Engineering is that humans are the weakest link in the security mechanisms.

An example of a Social Engineering attack is the use of malicious attachment in e-mails, these files could be used to launch massive spam e-mails, after this problem, the software developers disabled the automatic-launching feature when opening e-mail so the users have to explicitly open the attachments to execute the code, but still many users open the attachments without even thinking on the risks and thus executing the malicious code.

Maybe the simplest attack that is still useful is to fool a user by making the user believe that we are a System Administrator and requesting a password for different purposes. Internet users usually receive e-mails requesting passwords or sensitive credit card information to create and account or to re-activate and existing account. This type of users should be regularly reminded to not release passwords and sensitive information to persons identifying themselves as administrators. Real systems administrators rarely or never need to know a user's password to perform specific tasks.

One of the best options for organizations to protect their privacy against Social Engineer attacks is to train employees on how to properly use Security Policies.
One of the most famous social engineer is Kevin Mitnick, according to him, Social Engineering is based on 6 basic human tendencies.[1]

- Authority
- Natural Tendency to be Helpful
- Liking and Similarity
- Reciprocation
- Commitment and Consistency
- Low Involment

"Social engineering relies on falsehood and ingenuity from common users".[4] Lies, bribes and seduction can trick honest or almost-honest employees into facilitating private data or even physical access to a site. One of the cheapest and most effective attacks are often non-technical attacks just by exploiting humans instead of technology weakness.

3.4 Why does Social Engineering work?

The problem when trying to use Social Engineering techniques is that there are no exact rules on how to fool someone, there is no method that works with everybody, there are many techniques that can be used when trying to convince someone about your identity but in general when talking about Social Engineering there are more psychological issues rather than technological that can help to succeed in the attack. According to [5] the most common technique is to be kind and to present some type of authority.

There is quite a selection of materials on influence, that to some extend explains why and how humans react to certain techniques of influence.

The six techniques for influence listed before are highly likely to affect decisions, and therefore can be used to influence others. One of the fundamental issues with influencing humans is the fact that a good motivation is seldom crucial when asking people to do something, it was found that simply using "because" is as effective as using it in together with an actual motivation[4]. Another fundamental principle is to use the contrast principle, where e.g. something expensive is contrasted against something inexpensive, or in a security setting, something extremely insecure is contrasted against something clearly less extreme. This is a simple technique, but it is often successful.

Apart from the psychological reasons, in [8] researchers conducted an experiment to find out why Phishing techniques work. They analyzed a large set of phishing attacks and developed a set of hypothesis with a usability study in which 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. Results show that users did not look at security indicators in the web explorers nor verify authentication information in the web sites security certificates, this shows that users either do not know how to interpret security information from web explorers or they are reluctant to verify detailed information.

These findings show that, as we expected, many security risks are caused by users, either by ignorance or by disregard to security policies. In chapter 4 we will try to confirm these findings by using a questionnaire in two different groups, one with no user training and not exposed to security policies process and another group with some user training in information security and exposed to security policies. The results will show if user training and awareness reduce the risk of Phishing techniques and Social Engineering attacks.

CHAPTER 4

EMPIRICAL STUDY

4.1 Questionnaire

We will use a closed-ended questionnaire to respect the confidentiality of the participants and also due to lack of time to do personal interviews, although we could get more valuable information using personal interviews. The questionnaires will be handled to responders without any possible way of identification and without sex or age distinction.

The target of our questionnaire will be two different organizations, one environment in where user training and security policies are implemented and another where users are not formally introduced to computer risks or security policies and do not receive any user training.

The environments selected to do this research are:

a) Universities where last-year students without proper training in enterprise policies can be easily reached.
b) A mid-size company where security policies are implemented.

We will refer to the university group as Group A and to the company group as Group B. For Group A we got 80 answers and for Group B we got 32 answers. The difference in the amount of responders is because in Group A there are more possible samples than in B, the mid-size company have around 50 administrative employees while in the university there are much more students. Despite the difference in the sample we believe the research is still valid because 32 is still a good sample quantity.

The questions are specifically designed to find out:

1. The level of knowledge about some of the internal risks that we talk in this paper, like Spyware and Phishing.
2. The password behavior for each responder and try to find a relation between weak password policies and some other answers.
3. The level of awareness about security policies and personal behavior towards procedures.
4. The level of importance that users give to Software License agreements during Software Installations
5. How users feels about being responsible for protecting corporate systems and information.

4.2 Results

Two of the most important questions in the questionnaire were related to the amount of information that the responders knew about Spyware and Phishing, these questions are of vital importance to find out what is the level of knowledge about current security tendencies or if they are unaware of new attack methods and thus vulnerable to these new type of attacks.

In one question, we give the definition of Spyware to the participants and ask if they were aware of this information, in Group A an surprising 94% answered "Yes", this high percentage is probably due to the Computer Science background of the responders, while in Group B 78% responded "Yes" this is also a high percentage, this extraordinary high percentage of knowledge about Spyware could be cause by an increasing advisement of Anti-Spyware software and also because the Spyware techniques are not as new as Phishing.

Participants were also asked if they were familiar with the term Phishing and if their definition of Phishing was correct. The results show that Phishing techniques are somehow well know among participants in Group A with a 54% of positive answers (Figure 4.1) partly, like in previous results, because of the Computer Science background but in group B is widely unknown with only 31% of the responders answering positive to this question, this means that users working in the private company are not regularly informed about new computer security threats, this is a clear indication that this is an issue that should be addressed during the user training program proposed in the last chapter.

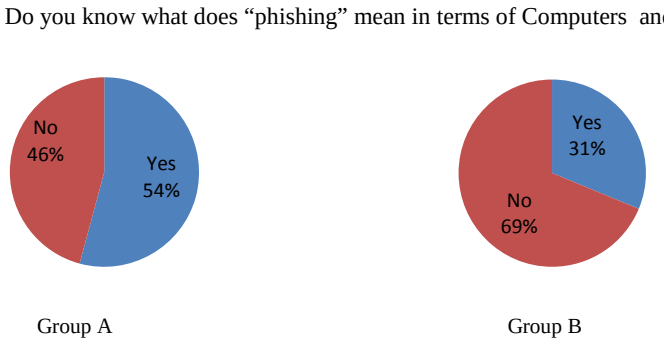

Figure 4.1

Participants from the private company are more willing to keep unchanged the automated generated passwords compared to users in Group A , this means that users are better trained in password management but still only 28% that group would keep their "difficult" password unchanged, the rest would prefer to change it for a password used in other accounts, this clearly means that system administrator should enforce password rules without option to change passwords otherwise security policies could be compromised.

When asking participants about Computer Use Agreements, generally speaking, neither users from Group A nor users from Group B have a good memory about the content of a Computer Use Agreement that they sign (Figure 4.2), this is also a weakness in the users behavior and therefore should be also included in our proposed

User Training program. From group A, although 48% have never signed an Computer/Internet Usage Agreement only 6% from the ones that have signed a Usage Agreement remember the content of the agreement. In Group B we find that 20% remembered the content of the agreement while 27% responded “remember most of it” and 30% “almost don’t remember”.

When asking about Software License Agreement, in group A, 57% never read the agreement when installing software, while in Group B 53% never read it this is a high percentage but at least in group B a 19% always read it when installing software, while in group A only 3% always read it. Users may think that EULA is not important or that it contains only legal terminology, but in reality EULAs should specify what type of software is being installed and whether or not contains Spyware.

If you have ever signed a Computer/Internet Usage Agreement, do you remember its content?

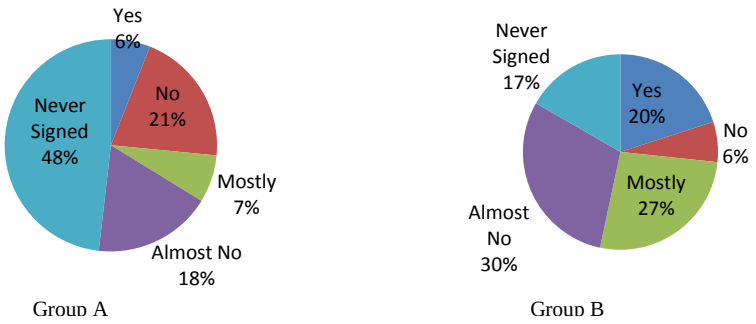

Figure 4.2

We used another set of questions to find out if participants were willing to reveal sensitive information about their passwords. In some way, users working in a corporate environment which have signed a Computer Usage Agreement are slightly more cautious about revealing this information but still 67% of the total participants in group B and 78% in Group A revealed something that could lead to discover a password by using Social Engineering techniques. We carefully selected questions like “Your password is made of numbers? , characters? or a mix between numbers and characters? or prefer not to answer?” and “Your password consist of a word?, a date ?, a mix? or prefer not to answer?” , the ideal answer or the expected answer for a well trained user would be “prefer not to answer” , only 22% in Group A and 33% in Group B responded “Prefer Not to Answer”.

Finally we wanted to know the users’ point of view about information security and how willing are they to cooperate with IT departments in the task of protecting corporate systems. In group A, 70% of participants stated that they think they also have responsibility in the role of protecting corporate systems , as we said before, group A is made of last year students in compute science , they are still not familiar with corporate terms or something similar but still a surprising 70% answered in a positive way. In group B, 81% think that somehow they are responsible for information security. This shows that users in general feel somehow concern about security information and they are willing to cooperate with IT departments to ensure information security, this is issue is very important for a successful user training and security awareness program.

From all this results, we can list all our findings and use them as a starting point to develop our user training and security awareness program and to make sure we cover these points in the Security Policy design.

- Spyware is well known among participant from both groups.
- Phishing is not well known particularly in group B.
- Users that are exposed to Security Policies have better password management
- Users usually do not remember the content of Computer Use Agreements
- General disregarding about Software License Agreements when installing software, whether at home or at the office.
- Most users are willing to give sensitive information about their passwords when asked in a proper way but group B has a slightly lower probability.
- General acceptance to cooperate with IT departments to protect corporate systems.

As we can see in the results, some issues like Spyware awareness, Computer Use Agreement content and Software License Agreements are common to both participant groups but critical issues like password management and level of knowledge about new security tendencies are different between groups, this shows that there is "something" that makes the results different from participants in group A and group B, we believe this "something" is the user training and the security policies implemented in group B.

4.3 Study Validity

During the design of the questionnaire there are some issues that could affect the validity of the results and which is interesting to mention in this chapter.

Group A is formed by Computer Science students; this means that they are more willing to answer in a positive way questions related to computer knowledge compared to participants not involved in Computer Science environment. When comparing results from questions related to terms like Spyware and Phishing, 54% of participants in Group A are familiar to the term Phishing, while only 31% from Group B are familiar with this term. In questions related to Spyware, 94% of participants from Group A and 81% from Group B are familiar with that term. As we can see, while the difference between results about Phishing is clearer, the difference in the results about Spyware is not so clear, this could be caused because Phishing is a relatively new term which participants from Group B are still not familiar with but university students in Computer Science are in constant contact with new technologies and tendencies.

Another relevant issue is that even though group A was made by university students, we carefully selected which students could participate in the survey, only students from last year courses were selected, this way the participants have the most similar knowledge to a graduated student or to a person working in a private company.

The number of participants in Group A and Group B is different. While in Group A there are 80 responders, in Group B there are only 32 responders. This small amount of participants in the private company survey can be explained because access to personal in private sectors is much more difficult than in universities where there are not information or privacy restrictions. Even with this difference in participants numbers we believe the results are still valid because since we are using the results as qualitative study 32 is still a big enough sample size for this type of survey.

We would also like to describe the environments in where the survey was performed so future readers in similar environments can take this study as a reference and to whom the results are the special interest.

Survey in group A was performed in 4 different universities, the universities do not implement any type of computer use training for students nor require students to sing a computer use policy before using the universities computers and networks, user's age is around 21 and 23 years old and all participants are enrolled in computer science careers, the survey was performed in groups at the end of a lecture session with the supervision of the professor.

Group B survey was performed in a mid-size company in the manufacturing sector with a total of 300 employees from which only 40 employees are in the staff or office areas having a personal computer assigned to them, the rest of the employees do not have access to a personal computer or data system. Users in the staff area are required to sing a Computer Use Agreement that explains what behavior is not allowed when using a computer or the enterprise network. The agreement is signed when the employee is hired and re-signed every year. The signed agreements are kept in the HR department so users do not have direct access to it. Users are not formally trained in security policies or any other techniques on how to use computer systems in a safe manner. Users are required to change their passwords every 3 months. Users work in an environment where several quality and finance audits (ISO and SOX) are performed every year so they are familiar with standard processes routines.

The questions selected for the survey were chosen according to the research questions, but without giving too much information to the responders so they do not identify the purpose of the survey, Social Engineering is not mention in the questionnaire neither any sentence mentioning security attacks. Some questions are not related to the research and they were used to distract the attention of the participant from the real topic.

CHAPTER 5

SOLUTION

In this research paper we propose a two-level method as a solution to countermeasure Social Engineering attacks and in general attacks where employees are the main target. The purpose of this method is to create a user training and security awareness program where users become aware about the important role they play on the information security strategy and the second step is based on designing a correct and complete security policy covering all aspects of information security.

- User Training and Security Awareness
- Design the right policy

5.1 User Training and Security Awareness

The idea of using User Training and Security Awareness as a tool against Social Engineering attacks and Phishing is that users should be aware of the techniques used by attackers and more important to convince people that information security is part of his/her role in the company, this is an interesting point because from our survey we identified that 70% of students from the selected universities believe information security is part of their responsibilities as students, while a surprising 81% of employees in the selected private company believe the same, this indicates that users are willing to cooperate during the user training program.

5.1.1 User training in Social Engineering techniques

One important thing in developing a user training program is to make everyone in the organization aware that malicious person exists and even if our company is not related to specific finance or vulnerable business our company could still be the target of attackers. Employees must be educated about what information needs to be protected, and how to protect it. Once people have a better understanding of how they can be manipulated, they are far in a better position to recognize an attack.

Security Awareness also means educating everyone in the enterprise on the company's security policies and procedures, policies are necessary rules to guide employee behavior to protect corporate information systems and sensitive information.

To develop a successful training program, you have to understand why people are vulnerable to attacks in the first place. By identifying these tendencies in your training you can help employees to understand why we can all be manipulated by social engineers.

According to [1] a great motivator in this instance is to explain how employees participation will benefit the company.

The basic guideline that should be kept in mind during development is that program needs to focus on creating in all employees an awareness that their company might be under attack at any time. It is too easy for employees to think that security problems are handled by security technology.

Mitnick quotes in his book [1] Albert Einstein "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former".. In the end, social engineering attacks can succeed when people are stupid or more commonly, simply ignorant about good security practices.

Security is not a product, it's a process. "Moreover, security is not a technology problem – it's a people and management problem" [1]

5.1.2 User training in Phishing attacks

In a study called "Why Phising Works"[8] the authors analyzed a set of phishing attacks and presented 20 websites to 22 participants, they asked them to identify which websites were fake. The data suggests that some phishing attacks have convinced up 5% of the participants to provide sensitive information to fake web sites.

The results of the study are:

- Good phishing websites fooled 90% of the participants.
- 23% of participants in the study did not look at the address bad, status bar or other security indicators to try to identify fake websites.
- 40% of the time users made mistakes.

The reason why these users did not detect the spoof websites is that users did not look at security indicators in the web-browsers, they only look at the website content to validate the website authenticity.

As we mentioned before, education is also the best tool to fight Phishing and any user training should focus on how to avoid getting tricked by phishing methods, in every educational program to fight phishing the following tips must be explained to participants.

• *Never reveal sensitive information in an e-mail or Instant Message.*
• *Be wary of clicking on links in messages.*
• *Check whether the webpage is genuine or not, and that the information you submit are protected.*
• *Keep your computer updated and use a firewall and anti-virus software.*

5.1.3 Different methods to implement user training

As we said before, a successful user training program should be permanent, and employees who have taken the training should be continuously remembered that they are still at risk, if users are not presented with updated information in a regular basis there are chances that they forget critical information, using as s reference [3] some options to use when implementing a permanent user training program are:

- Intranet/Internet
  Network administrators can use different resources inside the company to remind users that there is always a risk of being under attack, some internal resources are the intranet websites and corporate e-mail, these can be used to publish or send security notifications about new threats or just to remember users about current security policies.

- Online Curses
  Users can feel motivated if they are invited to take online courses as part of their regular training, online courses are usually offered to train users in their related competencies within the company, but it can also be used to train employees in general competencies. Online curses are particularly useful because then can be updated in a regular basis, they require less personal and they can be adapted to every employee schedule.

- Screen Savers
  Screen Savers can be used to show small advertisements in employees' computers, although the amount of information that can be presented to employees is limited, the amount of users with access to this advertisements is bigger than other methods.

- Posters
  Colorful posters or displays can be used to highlight important information to all employees, not only those with access to computers. They should clearly show one idea and not merely text that could be boring to read and as any other information should be regularly updated.

- Inspections and Audits
  Inspections and Audits are vital to raise awareness among employees being audited. A variant of this technique is that staff members lock around offices after work times and leave a congratulation message to employees that implement security tasks and correctly lock down information. Another possibility mentioned in [3] is that security personal periodically demonstrate social engineering by attempting to request passwords to selected users. Users who refuse to give information would be rewarded and users who fail would be instructed that they have failed a random test.

5.1.4 Minimum Content

It would be too difficult to explain in detail every specific paragraph that all security awareness program should include because every program changes according to the company where is implemented, but here we explain what are the minimum requirements.

- Risks:
  All organization employees should be informed about the risks in information security and how to recognize these risks. Examples of this could be how to recognize Spyware in an infected PC by showing a practical case, how to recognize a fake website used in a Phishing attack or to show a typical SPAM e-mail with malicious code as an attachment.

- Countermeasures:
  Once that the employees have been trained in recognizing information security risks they should be trained in how to react to these risks, this includes; procedures for using information in a secure way, training in security policies like password management or corporate information handling.

- Responsibilities:
  The training should also indicate what are the responsibilities of every employee in the task of protecting corporate information and assets. All employees should be informed that every person is responsible in one way or another in protecting the information.

- Contact Information
  Finally, the last minimum point to cover in every security awareness program is the contact information for reporting cases in the event of a security break. Users must be informed of the procedures for reporting security incidents, who and how should be informed and what to do when this type of events happens.

5.2 Design the right Security Policy

Today one of the biggest problems when trying to protect corporate information from external or internal threats is the lack of security policies in organizations. Security Policy is defined in [3] as "The rules and regulations set by the organization, in compliance with applicable law, industry regulations and decisions from the enterprise leaders", In most cases, Security Policies are mandatory and require compliance. Policies vary according to companies but in general they include guidelines for goals, objectives, behavior and responsibilities of the users and most of the time policies are followed by instructions and procedures.

One of the reasons why Security Policies are important is that most organizations try to secure their operations by installing as much security devices as possible (whether software or hardware) but they create a false illusion of being secure because of those products but in most cases the policies and procedures needed to implement those products are the ones that bring security to the company. For example, if a company implements a control-access system, they first need to define security roles and user functions, the adequate selection of these profiles is critical for the correct use of the system.

As Chad Perrin suggests in [10], we believe that one important step to make any Security Policy successful is to work together with the users and not against them. Most of the time, when users do not comply with policies is not because they do not want to follow the rules, it's just that users try to do their job as best as they can with the available tools that they have thus it's very common to find organizations where IT departments are seen as a bureaucracy bottle-necks rather than useful tools to help them accomplished their daily goals.

The solution to know how to work with users is basic, do not ignore the user's needs when designing and implementing a security policy. When IT departments refuse to give solutions to problems in modern workspaces users start looking for their own solutions and here is where users brake most of the security policies, that's why it's important to work together with end users to solve their problems and avoid users trying to find their own solutions.

According to [18] another important issue when implementing a security policy is the management participation, when management participates in the creation of the policies, it shows that the high level managers support the initiative and therefore gives more credibility to the project, this is vital if we want to have all levels of the company to actively work in the security policy implementation. Without leadership, employees will not take policies seriously and therefore the project will fail.

Ideally, before designing the right Security Policy a complete risk and vulnerability assessment should be done in order to identify all possible weakness and should include documentation from previous security attacks [18] this is to specifically address the vulnerability of each company where the Security Policy is implemented.

Although risk and vulnerabilities assessments can be done by staff employees or network administrators, some authors [18][3] emphasize that hiring an external

consulter is a better option, the main reason is that they do not know the system to be audited or any other information that could cause prejudice in the assessment. The outside auditor can assess the system with a hacker point of view, this is sometimes called Certified Ethic Hacking.

As a guideline to design security policies we can take the next example from the book "Computer Security Handbook" by S. Bosworth and M.E. Kabay [3], this guideline includes all possible points that should be cover in a Security Policy, but as we mention before, policies change from companies to companies. We could use the following list as a checklist for doing a risk assessment and also when designing our security policies documents.

- Physical Security
    - Servers
    - Workstations
    - Portable Computers
- Hiring, Management and Firing
- Data Protection
    - Classifying Information
    - Data access controls
    - Encryption
    - Countering Industrial Spionage
- Communications Security
    - Perimeter Controls
    - Web usage and content filtering
    - E-mail usage and privacy
    - Telephone and fax usage
- Software
    - Authorized products only
    - Proprietary software
    - Development Standards
    - Quality assurance and testing
- Operating Systems
    - Access Control
    - Logging
- Technical Support
    - Service-level agreements
    - Help Desk function

Since every Social Engineering attack is directed to a human, the attacker has to somehow get in contact with his target and for this reason he/she could use a wide variety of communication methods, when designing a Security Policy, we should not only focus on electronic communication systems like websites and e-mail but also in phone communication, voice mail systems and physical security should also be covered. The following is a list that covers some points that we should have in mind when trying to protect our organization from Social Engineer attacks.

- Security Policies related to computer and voice mail passwords
- Procedures for disclosing sensitive information

- Email usage policy
- Physical security measures
- Best security practices for voice mail usage
- How to determine the classification of information
- Proper disposal of sensitive documents.

Something common to find in all literature related to Security Policies [11] [3] is that Security Policies should be easy to read, easy to understand and easy to access, avoid vague vocabulary and complex terminology, this policy must be read by employees in all levels of the organization, not only by IT personal but still, all rules and process should be detailed to avoid different interpretations from different readers.

Another recommendation is to mention that security policies can be enforced by technology solutions like web-filters or password managers, and that violations to the rules will face disciplinary actions and could cause employee suspension or termination of contract.

CHAPTER 6

CONCLUSIONS

The only way to understand how to defend our organizations against social attacks is to know the methods that can be used against a person or an organization to break into a secure systems and get valuable information. Knowing the methods used by malicious persons can make employees adopt a more alert role on the security policy without overloading their responsibilities.

Social Engineering focuses on the weakest link in every security policy landscape and people can often hear the phrase “the only safe computer is the one that is always turned off”. The human factor is an essential part in every computer systems, there is no computer system that does not require some data or value entered manually by an operator, this means that this security weakness is universal, no matter what operating system, software or network we use.

Despite many people think, often is easier to use people to obtain confidential information than trying to exploit system vulnerabilities but it takes more time and resources to train users against social engineering techniques rather than convince a system administrator to reinforce his security mechanism.

By doing a questionnaire survey in two different groups we discover that users in an environment where security policies and user training is implemented have better password management behavior, better knowledge about malicious techniques and in overall they are better prepare to handle risky security situations than users without user training and users in environments where security policies are not in used, but still users were not aware of latest security vulnerabilities in part because the user training implemented in the selected company was not used in a regular basis.

An ongoing security awareness program should be always used with up-to-date content to update the users knowledge about new vulnerabilities. Security is not a static “field”, new technology in both sides of the fence makes attackers to develop new methods to bypass security solutions and as statistics show, attackers are targeting users more and more everyday therefore new protection methods should focus more in training users and not in using more and more network devices to protect the networks.

In this paper we propose a two step method to reduce the effectiveness of attacks directed to internal employees whether by using social engineering or other malicious techniques. This method is based on designing a correct and complete security policy covering all aspects of information security and the second step is to create a user training and security awareness program where users become aware about the important role they play on the information security program and by training users is a regular basis in security vulnerabilities.

As a future work, it would be interesting to do a case study in a company where employees do not have formal user training in security awareness and are not familiar with security policies agreements, then by taking this paper as a reference we can design a training program and a security policy for this company in particular and evaluate the users before and after the training program. The evaluation could be done by using questionnaires similar to the one used here, by doing security audits and performing penetration tests.

REFERENCES:

[1] K. Mitnick and W. Simon, The art of deception. Indianapolis: Wiley, 2002.

[2] B. Schneier, Secrets and Lies. Indianapolis: Wiley, 2000.

[3] S. Bosworth and M.E. Kabay, Computer Security Handbook, 4th ed. New york: John Wiley, 2002.

[4] M. Nohlberg, "Social engineering: understanding, measuring and protecting against attacks", ph.d. Licenciature, dept. Hum. And inf., univ. Of skövde, sweden, 2007.

[5] T. Qin and J. K. Burgoon. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering, Univ. Of Arizona, 2007.

[6] C. Onwubiko and A. P. Lenaghan, " Managing security threats and vulnerabilities for small to medium enterprises", fact. Comp. Info. Syst. Math., Kingston Univ. , London, Uk. IEEE 1-4244-1330-3/07, 2007.

[7] L. Laribee, D. Barnes, N. Rowe and C. Martell "Analysis and defensive tools for social-engineering attacks on computer systems", in 2006 workshop information assurance, US. Military Academy, West Point, NY, USA.

[8] R. Dhamija, J.D. Tygar and M. Hearst "Why Phishing Works", dept. Comp and Soc., Harvard Univ. 2006.

[9] C. Jones, "Social Engineering: Understanding and Auditing" ,GSEC, SANS Institute 2004.

[10]C. Perrin, "Work with End Users, not against them, to improve security", available online: http://blogs.techrepublic.com.com/security/wp-trackback.php?p=290 last visit: January 2008

[11]N Flynn, "e-Policy Best Practice", The e-Policy Institute, 2006 , available online http://www.epolicyinstitute.com last visit: February 2008

[12] H. l. Parness"Legal risks of uncontrolled e-mail and web content", Columbia Law School of Counsel , New York. Available online: http://www.pmi.it/file/whitepaper/000050.pdf last visited: febreary 2008.

[13] "Data Leakage: The stealth threat to business", ClearSwift, available online http://resources.clearswift.com/Main/Pages/Clearswift/RSRCCTR/default.aspx last visit: January 2008.

[14] IBM "Stopping insider attacks: how organizations can protect their sensitive information", IBM, 2006, available on http://www.ibm.com/services/us/imc/pdf/gsw00316-usen-00-insider-threats-wp.pdf, last visit Janary 2008.

[15] K. Prince. "Where Online Hackers Are Headed in 2007", Perimeter Software, 2007, available on http://www.zdnet.com.au/whitepaper/0,2000063328,22430133p-16001385q,00.htm, last visit: February 2008.

[16] Symantec Internet Security Threat 2007, Symantec, available online http://www.symantec.com/business/theme.jsp?themeid=threatreport, last visit: December 2007.

[17] 2005 Global Business Security Index Report , IBM , available online http://www-03.ibm.com/press/us/en/pressrelease/19141.wss, last visit: December 2007.

[18] S. Barman. "Writting Information Security Policies".1st Ed. Indianapolis, New Riders,2001.

[19] M.B. Desman. "Building Information Security Awareness Program", 1st Ed. Florida, Auerbach, 2001.