Social Engineering – A Life Cycle View

ABSTRACT
Cyber security is an increasingly serious issue for the whole world with intruders into large company organizations with the motive of getting access to restricted content. CSI Cyber Crime and Security Survey report for the year 2010-2011 stated that nearly half of the respondents had tough a security incident, with 45.6% of them reporting that they had been subject of a minimum of one targeted attack.

KeyWords
Cyber crime, intrusions, cyber security, Social Engineering
INTRODUCTION
Merely trying to stop infiltration on a technical level and ignoring the physical-social level, cent p.c security will ne'er be achieved. number of examples can be the scenes from Hackers that shows dumpster diving in the target company's trash in order to obtain money information from printouts and also the scene from War Games wherever Matthew Broderick's character studied his target before attempting to crack the password of the military computing system. 'Social Engineering' may be a threat that is unnoticed in most of the organizations but will easily be exploited because it takes advantage of human science instead of the technical barricades that surrounds the entire system. Below may be a classic example of this:
A person receives an e-mail on his official mailbox oral communication that his laptop has been infected with a deadly disease. The message provides a link and suggests that he downloads and installs the tool from the link to eliminate the virus from his laptop. The person in a state of confusion clicks on the link to get rid of the virus from his laptop however unwittingly giving a hacker a straightforward entrance into his company network.
To ensure complete security of a corporation from all types of internal and external factors, the protection adviser should have complete data of the Social Engineering cycle, the techniques that may be employed by company and also the counter-measures to cut back the probability of success of the attack.
In this paper we are getting to take you thru the varied phases therefore on perceive what's Social Engineering, Social Engineering Lifecycle, the varied Techniques employed in Social Engineering attack with careful examples so finally conclude with the counter-measures to guard against each of the Social Engineering attack techniques.

DEFINITION(S) OF SOCIAL ENGINEERING
The term "Social Engineering" will be outlined in varied ways that, with reference to both physical and cyber aspects of that activity. Wiki defines social engineering as:
"...the art of manipulating folks into playing actions or divulging confidential information".
Many authors have provided the following definitions:
“An outside hacker’s use of psychological tricks on legitimate users of a computing system, so as to obtain data he has to gain access to the system”.
“The observe of deceiving somebody, either in person, over the phone, or using a laptop, with the express intent of breaching some level of security either personal or professional”.
“Social Engineering could be a non-technical kind of intrusion relying heavily on human interaction which often involves tricking other people into breaking traditional security procedures” the assaulter uses social skills and human interaction to obtain data regarding a corporation or their computer systems.
In reality Social Engineering can be any of these definitions looking on the circumstances that surround the attack. Social Engineering is really a hacker’s manipulation of the natural human tendency to trust so as to get sensitive data required to gain access to a system. Social Engineering does not need any high level of technical experience however requires the individual to own tight social skills.
Many folks, for several decades have used social engineering as a method to analysis and collect data. The early social engineers would use the gathered data as a style of blackmail against the other organizations. Social engineering has been accustomed gain unauthorized access into several large organizations. A hacker United Nations agency spends several hours to interrupt passwords might save a good deal of your time by line up an employee of the organization, motility as a helpdesk or IT employee, and may simply inquiring for it.
THE SOCIAL ENGINEERING LIFE CYCLE
Social Engineering attacks are unique, but with a small degree understanding of the situations encountered, we will draft a rough cycle of all
the activities that a Social Engineering project goes through resulting in a in outcome.
The figure shows a general representation of the Social Engineering Life Cycle in four main stages:

---

**Footprinting**

It is the technique of accumulating info regarding the target(s) and therefore the close setting. Footprinting can reveal the people associated with the target with whom the wrongdoer has got to establish a relationship, thus on improve the probabilities of a productive attack.

The information gathering throughout the Footprinting phase includes but is not limited to:

- Information of employee names and phone numbers
- Organization Chart
- Department info
- Location info

Footprinting typically refers to 1 of the pre-attack phases; tasks performed prior to doing the particular Social Engineering attack.
Establishing Trust:
Once the doable targets have been listed out, the wrongdoer then moves on to develop a relationship with the target might be an associate employee or somebody working within the business so on develop a decent rapport with them.

The trust that the social engineer is gaining can later be used to unveil confidential items of data that could cause severe damage to the business.

Psychological Manipulation:
In this step, the thereforecial engineer manipulates the trust that he has gained in the previous section therefore as to extract as lead or get sensitive operations associated with the target system performed by the employee himself so as to penetrate into the system with much ease.

Once all the required sensitive info has been collected, the social engineer might locomote to consecutive target or move towards exploiting the particular system into consideration.

The Exit
Now, on balance the particular data has been extracted, the Social Engineer has got to build a transparent exit in such the simplest way therefore as to not divert any kind of unnecessary suspicion to himself.

He makes absolute to not leave any kind of proof of his visit that could lead a trace-back to his real identity nor link him to the unauthorized entry into the target system in the future.

THE HUMAN BEHAVIOR
Every Social Engineer targets specific behavioral traits in the victim so on extract most information out of him. These behavioral traits embrace but don't seem to be restricted to:

Excitement of triumph
Mr. X gets e-mail stating, “You have won one Million bucks and to say the winning quantity, fill in the attached document and forward it to the email id: XXXX@XXXX.com. switch your antivirus as it might block the transfer as a result of extremely encrypted Digital Signature of the documents”. Out of ease he switches off his Antivirus and proceeds as ordered and downloads the document and opens it but finds it corrupted. Little will he understand that he has simply downloaded a malware on his machine that allows the email sender to realize remote access to his machine?

Fear of Authority
Many people are apprehensive within the presence of someone they understand as associate authority, it is not that person they’re apprehensive concerning however possibly the position and power of the person who intimidates them and makes them.

The attackers war roles of authority figures such as law enforcement officers or high-ranking company officers to extract sensitive organizational info from the victims.

Desire to be helpful
Keith A. Rhodes, chief applied scientist at the U.S. General Accounting office, which features a congressional mandate to check the network security at 24 totally different government agencies and departments same in one in every of his interviews that, "Companies train their folks to be helpful, but they seldom train them to be a part of the protection method. we tend to use the social connection between folks, their need to be helpful.”

People in their want to be helpful and to solve different people’s queries, provide out a lot of data that otherwise should not be disclosed to outsider as it might provide offenders an opportunity to urge unauthorized access to the target system causing a potential loss.

Fear of Loss
Mr. X gets e-mail stating, “You have won one Million greenbacks and to claim the winning amount, deposit $75,000 in Account number: XXXXXXXX in 10 days from receiving this e-mail, failing to that the winning amount would be declared unclaimed and there would be a heritable lucky-draw to come to a decision the next winner”. Out of fear that he may lose such a good chance, to the account number provided.

when the future replies to the e-mail address goes nonreciprocal for the next 2 months nor will the one Million dollar gets deposited to the
account, it is understandable that he has been scammed.

Laziness
All the people have come to some or the opposite job that requires us to do solely a fixed set of activities and not linger around probing for higher ways in which of doing that activity. This causes dissatisfaction to the one that performs constant task repeatedly on daily and over the time learns “shortcuts” to do the tasks are lowest efforts and still meeting the targets. Such people over a amount of time become lazy and area unit susceptible to attackers the agency targets such people as they know that they would get the specified information with abundant ease attributable to the set back attitude of those people towards their work.

Ego
Most of the times, the attacker makes the person more showing emotion positive of himself/herself and therefore removing the logical awareness of the protection breach that's occurring.

The result is that, the person being hacked senses no damage in providing no matter it is that the attacker is requesting, the rationale that such attack succeeds is that the attacker could be a receptive audience for victims to display how much knowledge they have.

Insufficient data
Knowledge regarding the target system is one amongst the key factors that differentiate the assaulter from different employees of the organization. many an times, due to lack of correct coaching, the workers ar themselves not sure if they have complete data regarding the merchandise and Social Engineers make the most of such situations by creating a sense of urgency and not permitting the worker abundant time to assume and understanding the very fact that they are under fire.

THE WEAPONS OF A SOCIAL ENGINEER
The old-fashioned technical manner of breaking into the computer systems by brute-forcing the user logins or ports have currently been replaced by sophisticated strategies that not only area unit easier, but yield better and quicker results based on human psychological science. These attacks can help the assaulter get access to any system irrespective of the platform, software package or hardware concerned.

How specifically goes someone to carry out Social Engineering attack? The figure below shows some of the most standard techniques used to perform a Social Engineering attack:
Shoulder surfriding
Shoulder surfriding is a security attack where-in, the assaulter uses empirical techniques, like trying over someone's shoulder, to urge data whereas they are playacting some action that involves express usage of sensitive, visible data. this will be performed at a detailed range likewise as at a long range mistreatment binoculars or alternative vision-enhancing devices.

Dumpster Diving
Many a times, Brobdingnagian organizations dump things like company phone books, system manuals, structure charts, company policy manuals, calendars of meetings, vacations, events, printouts of sensitive information or login names and printouts of source code, passwords, disks and tapes, company letter paper and memorandum forms, and noncurrent hardware carelessly into the company dumpsters. The assaulter will use this stuff to get a huge quantity of information about the company organization and network structure. This technique of searching through the container, longing for doubtless useful data discarded by a company’s staff is thought as container Diving.

Role enjoying
It is one amongst the key weapons for a Social Engineer. This involves persuading or gathering information through the utilization of an internet chat session, emails, phone or any other technique that your company uses to move on-line with the public, deception to be a service, employee, technician, helpless or a crucial user to break in steer.

Trojan horses
It is one among the foremost predominant strategies currently employed by hackers that involve tricking the victims to download a malicious file to the system, which on execution creates a backdoor within the machine that may be employed by the wrongdoer any time within the future and so having complete access of the victim’s machine.

Phishing
It is the act of making and exploitation Websites and e-mails designed to look like those of well-known legitimate businesses, financial institutions and government agencies to deceive web users into revealing their personal data and incorrectly claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering non-public data that will be used for identity theft.

Surfing Organization Websites & on-line forums

Huge amount of the data concerning the organization structure, email ids, phone numbers area unit out there overtly on the company website and different forums. This information can be used by the aggressor to refine his approach and make a concept on whom to target and the methodology to be used.

Reverse Social Engineering

A reverse social engineering attack is attack during which attacker convinces the target that he encompasses a problem or may need a certain problem in the future which the attacker, is prepared to help solve the matter. Reverse social engineering involves three parts:

Sabotage: once the attacker gains a simple access to the system, he corrupts the system or offers it appearance of being corrupted. once the user sees the system in the corrupted state, it starts looking for help so as to solve the matter

Marketing: in order to create sure that the user approaches the assailant with the problem, the assailant advertises himself because the solely one who can solve the problem.

Support: during this step, he gains the trust of the target and obtains access to sensitive data.

DEFENSE AGAINST SOCIAL ENGINEERING

There is no effective thanks to defend against a Social Engineering attack because regardless of what controls enforced, there's forever that „human factor” that influences the behavior of a private.

But, there is certain ways to cut back the probability of success of the attack. it's additionally vital for organizations to determine a transparent and strong security policy and processes to cut back the threat of social engineering.

The following is a number of the steps to make sure protection against Social Engineering attack:

Security Awareness Trainings

Security Awareness is the simplest resolution to stop Social Engineering attacks. all and sundry in the organization must provide the basic security awareness training on timely basis that he/she ought to ne'er give out any data without the acceptable authorization which he/she ought to report any suspicious behavior.

Background Verification

There is many other probabilities that offender may join the company as an employee therefore as to gather info about the company . This makes background screening a very necessary a part of company policies to counter Social Engineering attack. It should not only be restricted to internal employees but should also be extended to vendors and different written agreement employees too before they become the part of the organization or is given access to the organization network.

Physical security

There should be correct access control mechanism in place to make certain that solely authorized people are allowed access to restricted sections of the organization. There is supposed to be no tail-tagging.

Limited data outflow

There ought to be constant observance on what all information concerning the organization is floating on the globe Wide web. Any kind of irregularity ought to be at once taken care of. this can make passive operation troublesome for the aggressor.

Mock Social Engineering drills

Special Social Engineering activities should perform on the inner employees of the organization by either the protection team or by the ven-
Data Classification policy

There should be proper classification of knowledge on the premise of their criticality levels and therefore the access personnel. Knowledge classification assigns grade of sensitivity to company info. Each level of knowledge classification includes totally different rules for viewing, piece of writing and sharing of the data. It helps to discourage social engineering by providing staff a mechanism for understanding what info will be disclosed and what cannot be shared while not proper authorization.

Some of the other controls that should be taken care of, to scale back the success of a Social Engineering attack are listed below:

- Maintain and install firewalls, anti-virus, anti-spyware software’s, and email filters.
- Never enable people to tailgate with you.
- There is supposed be a proper Incident response strategy set for the organization.
- Usage of company ID’s on public domain, blogs, discussion forums etc should be restricted.
- Pay attention to the URL of an internet site. tho' malicious websites generally look a twin of a legitimate site, however the URL might use a variation in spelling or a different domain.
- Confidential and significant online details like company mail box should not be accessed publicly places, cafes, and hotels etc. wherever internet security cannot be trusted.
- Don't send sensitive data over the internet before checking an internet sites security.
- Don't reveal personal or money data in email, and do not respond to email solicitations requesting this data.
- Ensure all physical entry and exit points area unit secured the least bit times.
- Do not offer personal data or data about your organization to anyone unless you are bound of the person’s authority to have that data.
- Use virtual keyboard wherever applicable.
- Be terribly careful what is provided on your company web site. Avoid posting structure charts or lists of key people wherever possible.
- Make sure to shred any document that's discarded which will contain sensitive information.

CONCLUSIONS

Through this text we can perceive that, but secure your application is, it's continually prone to one thing “The Human Factor”. This human issue is the weakest link in security which might be patched not by just the once training however solely by ongoing process of improvement.

Many times it's rather the interaction between the information and also the person needs to be secured rather than the interaction between data and server.

REFERENCES