LUNDS UNIVERSITET
Ekonomihögskolan
Institutionen för informatik

Social Engineering

A study in awareness and measures

Kandidatuppsats 15 högskolepoäng, SYSK15 i informatik
2 juni 2015

Författare: Björn Kronberg
Joakim Svanlund
Hampus Jeppsson

Handledare: Umberto Fiaccadori

Examinatorer: Björn Johansson
Anders Svensson

Abstract

In our technology-based society, there has been a clear focus on technical weaknesses to information security. This study will present another danger that is just as important to be aware of and is just as lethal, Social Engineering. This is an attack against the human element of security. This study covers a basic description of social engineering as well as a more thorough description of how the specific attacks are being performed. It also gives a short description on the factors that can make humans susceptible to manipulation and the possible impact that social engineering might have on an organisation. A research model is created using previous research. The study aims to determine Swedish production companies' perception of social engineering and investigate what measures are being taken to prevent it. This is done through three qualitative interviews with IT professionals from Swedish production companies. Through our research, we have established that Swedish production companies have a good perception of social engineering and that the measures they take to protect themselves are in accordance with best practices. However, the companies put different emphasis on different measures and their view on social engineering's potential impact differed.

Table of Contents

1 Introduction

Today, it is not uncommon to read about malicious attacks on companies. We hear about industrial espionage accusations and compromised data servers more or less on a daily basis. It is not only limited to big companies either. The small store on your street or the average private person is just as susceptible to attacks. These kind of attacks, an attempt to access information meant to be hidden, is not a new phenomenon. Even during our ancient history, man tried to device ways to breach the vaults holding valuable information. Sun Tzu, famed author of the book "The Art of War", explains in depth how to fool your enemy into giving up sensitive information, which shows that even the ancient Chinese had realized the value of Social Engineering. However, one can argue that with the increased reliance on information technology, our society is becoming ever more vulnerable to attacks on our information. Imagine with the spread of the Internet of Things, which is a broad term associated with things like cars, watches and even toasters being connected to the Internet, a hacker might gain access to more and more of the technology people use every day and take for granted.

The cyber-attacks are increasing as well. According to FBI Director James Comey, "*There are two kinds of big companies in the United States. There are those who've been hacked…and those who do not know they've been hacked.*" (Cook, 2014).

Not only are these attacks happening more often but the economic impact is becoming more severe. A recent survey done by the Ponemon Institute showed that the annual average cost for U.S. retailers inflicted by cyber-crime doubled between 2013 and 2014 to a staggering $8.6 million per company. The survey also claimed that the annual cost for a company who suffered a successful attack increased to $20.8 million in the financial services, $14.5 million in the technology sector and $12.7 million in communications industries. (Walters, 2014).

While there seems to be a distinct focus on the technical threats to our information, we tend to forget about the human factor. When you are trying to protect your keep, it is not simply sufficient to have walls erected around it. An attacker would simply climb over the walls. You need guards that keep watch, that patrol and are able to respond to possible attacks to the integrity of the defence. But what if these guards could be fooled into thinking that the attacker is really a friend? What if the attackers are disguised as guards themselves? There would be a need for policies, protocols, education and systems that prevents these kinds of malicious attacks. Is this really something companies' take into serious consideration?

OWASP or Open Web Applications Security Project is a non-profit organization/community which strives to help making applications more secure. They have a list of what the community has determined is the greatest threats to companies IT security. (OWASP, 2013). The top 10 threats are (2013):

1. *Injection*
2. *Broken Authentication and Session Management*
3. *Cross-Site Scripting*
4. *Insecure Direct Object References*
5. *Security Misconfiguration*
6. *Sensitive Data Exposure*
7. *Missing Function Level Access Control*
8. *Cross-Site Request Forgery*
9. *Using Components with Known Vulnerabilities*
10. *Unvalidated Redirects and Forwards*

However, these 10 identified risks have failed to mention a single social aspect or a threat caused by the human factor. To focus simply on the technical aspects of IT-security is like leaving a window wide open while you have a securely locked door, kind of pointless.

1.1 Aim

The aim for this study is to explore Swedish production companies' knowledge and understanding of social engineering and to examine what kind of security measures are used. Our end goal is to establish Swedish production companies' perception of social engineering, investigate the measures taken to achieve a secure organization and finally, what possible impacts social engineering might have on a company.

1.2 Research Questions

1. How do Swedish production companies perceive social engineering and its potential impact and how are they protecting themselves from the threat?

1.3 Scope

We have limited our interviews to IT experts who are information security managers within their companies. The employees were excluded from the research since we wanted to investigate what kind of measures were used to protect against social engineering and only the information security managers would be able to provide that information.

We also limited the companies chosen to production companies based in Sweden. The reason only production companies were chosen is because they have valuable products and other information that is highly sought after, in other words a target for the social engineer. There are also other companies that could be targets for a social engineering attacks such as banks however these were excluded due to the short timeframe of the study there was not enough time to broaden the research field. The fact that they are all based in Sweden was a choice of convenience.

The human behaviours listed in the Research Framework was a section we felt was important in order to fully understand social engineering, as it explains why it works. However, we do not have a sufficient empirical base to highlight it further in the analysis or the discussion since the respondents we interviewed are IT security managers and not behavioural scientists.

1.4 Disposition

The study is divided into eight different chapters. The first chapter will present an introduction of the study as well as presenting the aim of the research and the research question. The second chapter, the Research Framework, will present a definition of social engineering to the reader, what kinds of attacks that could be expected by a social engineer, why these attacks works and what the potential impact of the attacks could be. Finally, we will present a number of security measures that previous studies have highlighted to prevent social engineering. In the third chapter, we will explain our Scientific Method. It includes a presentation of how and why the respondents were chosen, how the interviews were performed and some aspects that were taken into account in relation to the empirical material. In the fourth chapter, the Empirical Results are presented. This is done using tables with keywords summering the interviews, question by question. The fifth chapter, Analysis, is where we analyse the empirical material. This is presented by four themes, Awareness, Measures, Acceptance and Accessing the threat. In the sixth and following chapter, we will present the Discussion where we put the empirical results in comparison to the information presented in the Research Framework section. The seventh chapter is dedicated to the conclusion of the study. The eight and last chapter we briefly discuss the potential for future research.

2 Research Framework

In this section, we will present previous studies in the field of social engineering. We will start with an introduction on what social engineering is. As social engineering has many different aspects, we have chosen to highlight some common attacks that are separated into different headings. After this, we will present human behaviours that explain why social engineering works. We will also show the potential impact social engineering could have on a company. Lastly, we will present theories that previous studies have emphasized, i.e. theories of how to defend against these attacks.

2.1 Definition

"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 Website, which exploits a technical flaw and allows the hacker to take over the computer." (CNN, 2005).

The quote from Kevin Mitnick, a man many would call the father of social engineering, is his definition of social engineering, given during an interview with CNN. This is the definition we have chosen to use in order to describe what social engineering is. The reason we feel that it is appropriate is because it illustrates the great diversity of social engineering, a security threat that can take the form of both social and technical aspects.

In order to better understand what social engineering is and how previous studies perceive social engineering threats, we will now present six ways to use social engineering to attack employees in companies.

Tailgating

This kind of attack is used to target a specific defence mechanism, not entirely surprisingly, the gate. The gate is used to separate the outside world and the vulnerable inside, which can be done using keys, key cards or even biometric security measures. Tailgating is when the social engineer follows an employee inside and past the security measures in place at the gate, even though the social engineer does not possess the necessary identification to normally pass the security. This is done by waiting for an employee to attempt to pass the security measures. At this point, the social engineer simply follows the employee inside. (Long, 2008, p.14).

Pretexting

In this scenario, the social engineer fools the victim into divulging information by claiming to be someone they are not. Human emotions like fear, guilt and/or friendship make this kind of attack very effective. The social engineer will often have invested time and effort into gaining information on the victim beforehand, as well as building a believable profile. The social engineer can then call the victim and convince him or her of a scenario where the victim will provide the attacker with valuable information. (Rouse, 2011).

Phishing

This is a term used for attacks where the social engineer uses emails or banners in an attempt to lure the victim into providing information. These emails would look like they were coming from a legitimate source asking for some kind of information. This information can then be used by the social engineer to gain access to accounts or servers. The social engineer can also use these emails or banners to trick the victim into downloading a Trojan which then can be used for various crimes. (McDowell, 2013).

A study by Jagatic et al. (2007) called "Social phishing" was done to examine how effective phishing attacks were. The study was conducted at Indiana University and the test subjects were students aged 18-24 of both sexes. The students were selected based on how much information that was readily available about them on social networks. The study consisted of 1731 where 921 students received phishing attacks and 810 students had their email addresses spoofed. The attack was in the form of a message sent from one person to the other, having a link to a website that would harvest information.
The sender, who was a real person at the University, was unaware of the experiment and of the email. There was also a control group that received a different email that was sent from a fictitious person but with the same purpose. The results showed that the attack was successful against 72% of the subjects who belonged to the social network group and 16% of the subjects who belonged to the control group. (Jagatic et al., 2007, p.94-100).

Dumpster Diving

Like the name suggests dumpster diving means that the social engineer looks for documents that has been discarded, often in dumpsters or trashcans. These documents could hold a lot of valuable information to a social engineer, trained in knowing what to look for. It could be a letter of resignation from a disgruntled employee, insurance information or health care information. Such information could possibly be used to gain leverage over a person which can then in turn be used to penetrate defence mechanisms or to gain raw information. (Long, 2008, s.2-7).

Baiting

This kind of attack plays on the victim's curiosity. The social engineer might leave a USB drive or CD somewhere where an intended target works or lives. On the USB drive or the CD the engineer has installed a Trojan. When the victim then plugs in the USB or plays the CD the Trojan will infect the computer allowing the social engineer to harvest information from the victim's computer or even get access to a company's internal network and servers. (Stasiukonis, 2006).

Shoulder Surfing

The principal of this attack is quite simple. The social engineer attempts to harvest information by looking over the shoulders of legitimate employees. There is all kinds of information that can be collected by this quite simple manoeuvre, like passwords or documents if the victim is careless or simply not aware that the social engineer is watching. (Long, 2008, p.28).

Summary

The attacks that were listed are not all the attacks available to the social engineer but rather those we selected from the studies we read, which are the ones which were most commonly mentioned. It is important to remember that there are as many attacks and varieties as there are people and minds able to think of them. However it might not be important be aware of all the kinds of attacks but rather the nature of them. This understanding is further described in this section of the study.

2.2 Human Behaviours

In this section we will present a number of normal human behaviours that enables the social engineer to achieve his goals. They are all programmed into our backbones since birth and are hard to resist which is one reason why it's hard to defend against social engineering.

Social Rule System Theory

In order to define the underlying human behaviours that allows social engineering to be executed, we need to establish why people do things to begin with. Most human social activity – in all of its extraordinary variety – is organized and regulated by socially produced and reproduced rules and systems of rules. (Burns & Machado, 2014, p.2).
These unwritten rules decide how social interaction is performed. To be a successful social engineer, one needs to excel in the art of social interaction and without the social rule system, social engineering would be next to impossible.

Fear

Fear is an emotion which forces the subject to act, and act sooner rather than later, even in ways that the victim might not have expected. The social engineer might use this to his advantage when sending email in an attempt to perform phishing. The attacker could write something like “Urgent! Invalid information added to your PayPal account”. (Workman, 2007, p.321). The email would also conveniently have a link which the victim is encouraged to press to fix the problem. In order to make the email look legitimate the social engineer might add logos and other kind of information, simulating an authentic sender. An example from Sweden is the Trojan in the early half of 2012 that claimed to be from the Swedish police dealing with computer crime. When the Trojan activated, it accused the victim of committing some kind of computer crime and that the victim was to pay a fine of 100 euros. (Johansson, 2012). It was a convincing plot with police logos, meant to scare the victim into paying the social engineer in order to avoid further prosecution.

Authority

This is a strong behaviour that is best explained with the famous experiment of Stanley Milgram in 1963. The experiment was designed to investigate at what lengths a person would go as long as a person of authority was in charge, even though it resulted in real pain for someone else. The test had a teacher and a student, where the teacher would ask the student questions and then administer an electric shock if the student’s answers was incorrect. The voltage of the electric shock would increase with 15V for each incorrect reply. The test was then set up so that the student was an accomplice to Stanley and the subject would always become the teacher, the subject would however not be aware of this but rather thought it was randomly chosen. In the end the subject would administer high amounts of electric shock to the student even though it was clear that the student experienced enormous pain. The subject proceeded anyway because the authority in the white lab coat had explained that the pain would pass. (Stanley, 1963). In other words, a social engineer can force a victim into divulging information by convincing the victim that he or she is a person of authority.

Reciprocity

Reciprocity is a theory that states that in response to friendly actions, people are frequently much nicer and much more cooperative than predicted by the self-interest model; conversely, in response to hostile actions they are frequently much nasty and even brutal.
(Fehr & Gächter, 2000).
This is something that a skilled social engineer takes full advantage of, especially at the start of the scam. In the later parts, the social engineer already has some valuable information which the attacker uses to lure the target into thinking that the perpetrator actually is a part of the company. On the early stages, however, the social engineers rely solely on the victim's benevolence and attitude towards them.

2.3 Potential Impact of Social Engineering

There are various degrees of harm that a social engineer can cause companies, it all depends on what information the attacker has been able to collect. As with any IT attack there are several different direct consequences. A server or several servers might have been corrupted or destroyed. Hard drives and information might have been maliciously encrypted by the attacker in order to deny the victim access to it. Customer information might have been compromised. Sensitive and classified information on products, contracts and partners might have been leaked. These are all direct consequences but there are also several negative effects that might follow in its wake. This could be lost confidence in the company due customers no longer trusting the security of their sensitive information. It could be customers leaving the company due to its inability to supply products. It could be lost revenue due to websites and web stores not functioning properly. It could be lawsuits directed at the company due to failing to properly protect its information. In either case the company is likely to suffer severe damage to its reputation.

In 2003 the company Guess, Incorporated were forced to settle Federal Trade Commission charges that the company had failed to uphold appropriate security measures in protecting customer information. (Federal Trade Commission, 2003).

2.4 Social Engineering Defence Model

Our original approach included building a framework that would contain the most important factors when working with Social Engineering. However, we have decided to name this a research model instead. This is because we feel that, in order to build a complete protective framework, more extensive research must be conducted and a larger empirical study is required, something that we have not had the resources or the time to do.
We have selected four major themes that we believe has an impact on the success of a social engineering defence. We will use this model to design our interviews, analyse our empirical results and to guide us in our discussion.

2.4.1 Awareness

In 2011, Dimensional Research conducted a study with 853 participating IT-professionals from United States, United Kingdom, Canada, Australia, New Zealand and Germany. The study established that 97% of the security professionals and 86% of the IT professionals were aware or highly aware of the potential threat.

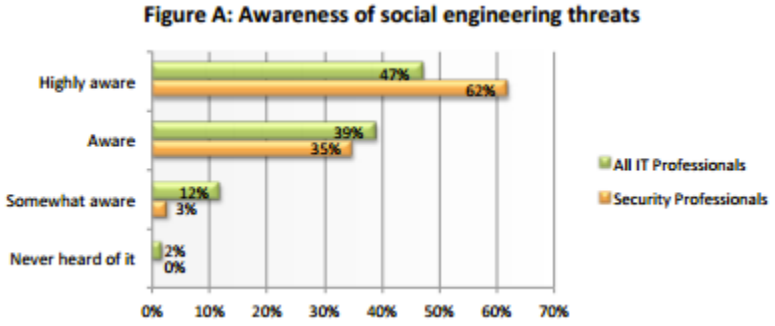

Figure 1: Awareness of Social Engineering (Dimensional Research, 2011)

A study performed by Bullée, et al. showed clear positive effects on prevention by spreading awareness of social engineering. The study targeted 118 employees of both sexes from the University of Twente. Awareness was spread using three methods, a leaflet explaining what social engineering is, a blue key chain with the text "Don't give me to a Stranger" and a poster containing a humorous quote and an explicit remark against password, key and PIN sharing. (Bullée et al., 2015, p.102-103). The awareness security measures were randomly administered to half of the subjects in an attempt to increase their resilience against social engineering. After this the subjects were exposed to social engineering by an attacker that used authority in an attempt to make the subject to surrender their key. Only 37% of those that had been exposed to an awareness intervention gave up their keys in contrast to 62.5% of those did not get extra awareness information. Those that did not get extra awareness had 2.84 times higher odds of being compliant to a social engineers attack. (Bullée et al., 2015, p.107). The study shows that awareness has a significant positive defensive effect.

Furthermore, a paper written by Mark Pielocik reviews several case studies regarding social engineering. In his conclusion, he states that "*it is my belief that the best way to combat "**social engineering**" is through continuous security awareness training…".*
(Pielocik, 2004, p.19).

In a book written by famed author Kevin Mitnick (2002) called Social Engineering: The art of human hacking, he claims that the only way to keep your product plans safe is by having a trained, aware and conscientious workforce. He feels that the most important factor in this is an ongoing awareness program. He even claims that some authorities recommend that a staggering 40% of a company's overall security budget should be targeted towards awareness training. (Mitnick, 2002, p.2232).

2.4.2 Measures

When discussing security measures against social engineering, we have chosen to consider technical measures a secondary rather than a primary factor. Not because they are not important but because we believe that they are a general IT security problem rather than a social engineering problem. It is as Kevin Mitnick (2002) said, "*Security is not a technology problem - it's a people and management problem.*

Education

In a study by Tim Thornburgh (2004) called Social Engineering: The "Dark Art", the author also stress the need for education about social engineering and to create awareness of the threat in order to defend against it. He also mentions seven things Kevin Mitnick claimed were good things to look out for when identifying a social engineer. (Thornburgh, 2004, p.135).

- Refusal to give call-back number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Show discomfort when questioned
- Name dropping

According to previously mentioned author Kevin Mitnick (2002), appropriate education and training for employees is part of the only true effective way to mitigate the threat of social engineering, combined with good security technologies and security policies. He claims that "*once people have a better understanding of how they can be manipulated, they are in a far better position to recognize that an attack is underway".* (Mitnick, 2002, p.233).
In an article written by Thor Olavsrud (2010) for eSecurity Planet, he conducts an interview with Chris Hadnagy, cofounder of Social-engineer.org and author of several Social Engineering books. In the interview, Hadnagy states that the first mitigation against hackers employing social engineering techniques was security through education. He believes that employees must be educated about the type of attacks that are being used in order to be able to defend against them. (Olavsrud, 2010).

Policies

According to Kevin Mitnick (2002), policies are clear instructions and guidelines for the employees of a company. They provide a guideline for their behaviour when safeguarding information and they are a vital building block in developing effective controls to counter potential security threats. (Mitnick, 2002).
In an article released by Cisco, they list some important factors that should be included while developing a security policy. (Cisco).

- Password Management: Guidelines such as the number and type of characters that each password must include, how often a password must be changed, and even a simple declaration that employees should not disclose passwords to anyone (even if they believe they are speaking with someone at the corporate help desk) will help secure information assets.
- Two-Factor Authentication: Authentication for high-risk network services such as modem pools and VPNs should use two-factor authentication rather than fixed passwords.
- Anti-Virus/Anti-Phishing Defences: Multiple layers of anti-virus defences, such as at mail gateways and end-user desktops, can minimize the threat of phishing and other social-engineering attacks.
- Change Management: A documented change-management process is more secure than an ad-hoc process, which is more easily exploited by an attacker who claims to be in a crisis.
- Information Classification: A classification policy should clearly describe what information is considered sensitive and how to label and handle it.
- Document Handling and Destruction: Sensitive documents and media must be securely disposed of and not simply thrown out with the regular office trash.
- Physical Security: The organization should have effective physical security controls such as visitor logs, escort requirements, and background checks.

Microsoft points out the fact that security is a journey rather than a destination and the policies must be continuously revaluated. "*Each incident provides new input for an ongoing review of security within the incident response model, which is shown in the following figure 2.1.*". (Microsoft, 2006).

Figure 2: Incident response model (Microsoft, 2006)

Audits

Chris Hadnagy (2011) compares an audit to a rehab meeting with a doctor after an injury. As the doctor rehabilitates you, he might perform stress testing to the injury. This allows the doctor to analyse if there is still some weakness that needs strengthening. The same concept applies to organisations. Audits are a form of stress-test for your company before a breach occurs. His explanation is as follows: "*In the most basic terms a social engineering audit is where a security professional is hired to test the people, policies, and physical perimeter of a company by simulating the same attacks that a malicious social engineer would use."* (Hadnagy, 2011).

According to a paper written by Christopher Jones (2004) for SANS Institute, the most trusted and by far the largest source for information security training and security certification in the world, there are two major questions that needs to be dealt with, namely:

- What is the use of implementing strong information controls or in-depth training if they are not taken seriously or possibly even ignored?
- How can we know that the actions that have been taken to protect the company are adequate?

To properly answer these questions, the company can make use of audits. (Jones, 2004).

"*Because social engineering defence is largely based upon the strength of the security policy, it only makes sense that regular security audits be performed to identify weaknesses and to better improve the policy itself."* (Jones, 2004).

He also lists four different methods/stages you can use to perform audits. (Jones, 2004).

- Intelligence Gathering Phase - Gathering information about the company, its practices, culture and employees, and identifying potential weaknesses is the goal
- Physical Entry Phase - While the social engineer will generally attempt to accomplish his mission without ever physically stepping foot on company property, sometimes it is necessary to gain physical access to gather further information.
- Shoulder Surfing and Eavesdropping - After gaining physical access, there are several options open to the social engineer. He may attempt to find an open network port to gain unprotected access to the company network, he may target a specific individual's machine in order to steal sensitive documents, install Trojan horse software or even shoulder surf passwords from employees.
- Telephone Based Auditing -The telephone is a very important tool for the social engineer. It allows the attacker to remain relatively anonymous and opens up almost every employee to possible exploitation by the attacker.

2.4.3 Acceptance

It is essential that senior management buy into and strongly support the necessity of developing security policies and an information security program. As with any other corporate program, if a security program is to succeed, management must do more than merely provide an endorsement, it must demonstrate a commitment by personal example. Employees need to be aware that management strongly subscribes to the belief that information security is vital to the company's operation, that protection of company business information is essential for the company to remain in business, and that every employee's job may depend on the success of the program. (Mitnick, 2002).

2.4.4 Accessing the threat

In an educational paper written by Microsoft called "How to Protect Insiders from Social Engineering Threats", they state that "*All security requires you to assess the level of risk that an attack presents to your company."* You identify the risk, asses the likelihood of it occurring, calculate the cost of potential mitigation and decide whether or not the cost is justifiable. (Microsoft, 2006).

In a Security Risk Assessment Handbook written by Douglas Landoll (2006) who has over 20 years of experience in working with Information Security, he says that a security risk assessment program is meant as a tool of senior management that will give them an effective measurement of their security controls as well as an indication of how well their assets are being protected. He lists the four stages of risk assessment as follows: Risk Assessment, Test & Review, Risk Mitigation and Operational Security. (Landoll, 2006).

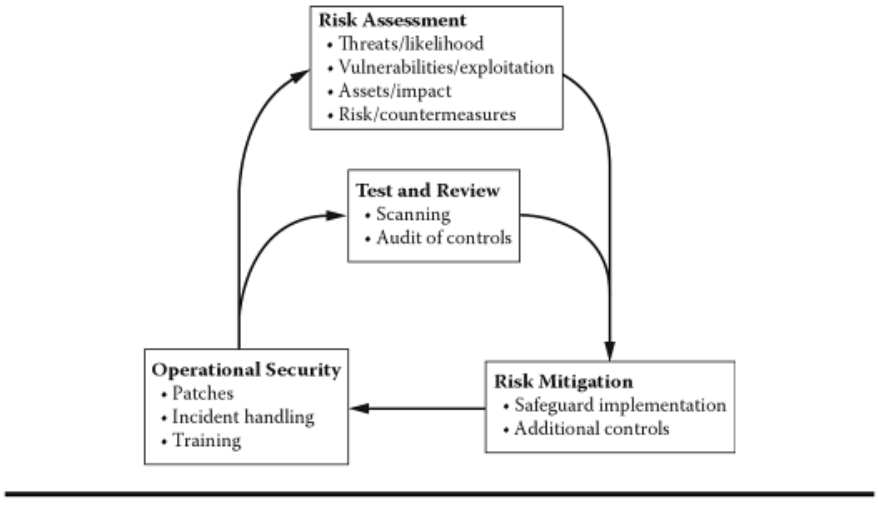

Figure 3: The role of the security risk assessment model (Landoll, 2006)

3 Scientific Method

The material used for this study was collected from three qualitative interviews with relevant IT security experts working for small and large production companies in Skåne, Sweden. The material used in the research framework section has been gathered from various studies in the field of IT security. The studies that we have used were selected due to their similarity in focus to our study and researchers who are experts in this specific field have produced them.

3.1 Choice of method

When performing a scientific study, there are two different approaches to collecting empirical data; a qualitative approach or a quantitative approach (Denscombe, 2000). The most appropriate approach is determined by what the study is about. We used a detailed qualitative approach since we wanted a deep and thorough understanding of how Swedish Production Companies perceive and work with Social Engineering.
We also wanted to compare the obtained data against our research model to see if the measures we found most relevant corresponded with the factors the respondents highlighted. In order to perform a more detailed analysis, we aimed to create a sense of openness to encourage free discussion with the respondents. A quantitative approach does not allow for follow-up questions, which could have a negative impact on the result. For this reason, we chose a semi-structured interview, also recommended by Bryman (2002).
This type of interview allows the respondent to talk freely about the subject and by doing so, cover more aspects. Bryman (2002) says that this might lead to new information, which the respondent might have overlooked. The answers are often more comprehensive with a semi-structured interview than when doing a questionnaire survey (ibid). The interviewers have the possibility to ask follow-up questions to the respondents which allows for far more comprehensive answers. (Bryman, 2002).

3.2 Selection of respondents

According to Jacobsen (2002), the point of a survey is to reach an understanding regarding the subject in question. Jacobsen (2002) says that there will always be some limitation when performing a survey; you rarely get in touch with all the respondents you want to interview. Only a small part of the whole picture is being examined. This will be reflected in the result and the validity of the survey (ibid).
A proper delimitation reflecting the scope of the study is therefore important. It is important to select respondents properly suited for the survey so the data you obtain is guaranteed to be detailed and valuable.

We decided to focus on production companies, not only because we believe they have important information that needs to be protected and that is highly valuable, but also because of the recent attention corporate espionage has received in the media. (Massimo, 2014). All of the companies that participated in the study are located in Skåne. This choice was made out of convenience as we are all living in Skåne and we preferred physical interviews rather than to perform them via other media such as email. This because we felt that the respondents might be more willing to talk to someone face to face rather than over, for example a phone and we would also be in a better position to understand the respondents reactions. (Ryen, 2004, 77-78).

We focused on employees that had vast experience in the industry and had a managing position in the IT-department of Swedish production companies. We wanted them to have good knowledge regarding Awareness, Measures, Threat Assessment and Acceptance. Jacobsen (2002) calls this knowledge criterion.
Our initial approach to acquiring interviews was to send out emails to all the companies we knew of, from the news, advertising or contacts. We also searched the Internet using keywords such as “Swedish production companies” or “Production companies located in Skåne”.

The email that we sent to the selected companies contained a description of us; how we perceive social engineering and what our research hopefully will result in. The email is provided in the appendix section. These emails were sent to around 30 different companies. However, the emails failed to yield any interviews and we only got one reply, which was a company who declined to participate without any explanation.
At this point, we decided to change our tactics and started to call all the companies we had tried to email before. This did not yield any better results as we were diverted to phones where no one answered or we were simply met by a voice recording. In the end, we did acquire three interviews using personal contacts. So, in the end, we had to use a convenience selection. Since the respondents decided to keep themselves and their companies anonymous we have decided to present a short explanation and description of each of the companies and of the respondents in order to bring some context.

Company A
Company A is a global company within the production industry with over 16 000 employees in over 35 different countries.

Respondent A
Respondent A has an engineering degree in Computer Science and the respondent has over 25 years of industry experience. The respondents' background is rather technically oriented but over time, the respondents' focus has drifted from the technical aspects to the "soft parts", i.e policies, education and guidelines.
When the respondent began his work for Company A, the concept of information security was basically non-existent and the respondent was given the assignment to create a defence system. The respondent has been involved in building all the soft parts of the enterprise security system. The respondents' current role in the company is Head of IT-Security management.

Company B
Company B is a regional company with over 100 employees. The company is involved in the production of printing solutions.

Respondent B
Respondent B has worked in the industry for as long as he can remember. Respondent B has always worked with IT but lately, the respondent has drifted more towards IT-security specifically. The respondents' duties include both the soft parts and more technical tasks, like penetration testing and implementations. The respondent is CISSP-certified and has worked with IT-security & Information Security education for several years.

Company C
Company C is a global company with over 64 000 employees and currently operates in 90 countries worldwide. The company produces products such as chemicals and plastics among a wide range of other products.

Respondent C
Respondent C is head of IT-security management. The respondent's main focus is maintaining the IT-infrastructure, which is done mainly by working with the soft parts of Information Security.

3.3 Performing the interview

Prior to the interview, the respondents were informed about the nature of the study, what the obtained data would be used for and they were given the questions beforehand. The respondents were informed about their right to anonymity as well. We felt that this was important to allow the respondents to talk freely, without risk of compromising their own security systems at work.

To ensure the convenience of the respondents, we conducted all of the interviews at the respondent's workplace. We also felt that the respondents were more likely to feel comfortable and at ease when being in their own facilities. Jacobsen (2002) says that a physical interview is preferable since body language and facial expressions can be observed which might lead to a different interpretation of the answer provided.
Another benefit with physical interviews is that the response time is dramatically reduced compared to e-mail or a phone interview. (Denscombe, 2000)
The interviews took between 45 and 70 minutes and were all performed within a span of one month.

In order for us to capture the data of the interviews correctly all of the interviews were recorded using Samsung Voice Recorder, a free application on one of our mobile telephones. The respondents were informed that the interview was recorded and they all agreed to it. We asked the respondents for at least one hour of their time in order to perform the interview but in neither case did the interview become rushed, even though the time often went beyond the time agreed. This was important to us, as we wanted to fully capture every essence of the interview.

3.3.1 Interview Guide

A good structure is required to simplify the analysis and categorization of the empirical data. (Kvale, 1997). However, too much structure might result in a reclusive respondent and, as a result, lackluster answers. Therefore, you should always aim for balance in the interview structure. The interview is used to collect empirical data, which will help us answer the research question. In order to reach that goal, the interview questions need to be well written and dynamic. This is because the research-questions are often defined by the theory related to the research model, which is often thematically designed. This leads a high level of abstraction. (Ibid)

We designed an interview guide in order to obtain homogenous data from the respondents. (Appendix 1) We categorized the questions based on the themes we selected for our research model. The interview guide consists of 12 questions with some spontaneous supplementary questions depending on the answers of the respondents. The following section will describe our interview guide, explain the questions connection to our research model and clarify some of the keywords.

1: Tell us about yourself; your background within the field, within the company and specifically what duties and responsibilities you have within your current position.
This was our initial question, which had several purposes. First and foremost, it is good practice to initiate a discussion with some formal presentation and some generic questions. Secondly, we wanted to establish their formal position in the organization and their background in order for us to create a comprehensive presentation of the respondents without giving up their anonymity. Lastly, we wanted to validate that the respondent really met our criteria.

Question 2: What is your definition of social engineering?
This question was also meant for our validation; we wanted to make sure that the respondent shared the same perception of social engineering as we did.

Question 3: How is your company working to prevent social engineering?
This question is probably the most holistic question that we have as it pretty much covers every theme of our research model. This allowed for the respondent to explain their companies' defense freely. The generic nature of the question also served a second purpose. The respondents' answers were similar, more or less, but every respondent put different emphasis on different aspects. This, in an inconspicuous way, revealed what controls the respondents companies had prioritized.
This question was sometimes followed by additional questions, depending on the respondents' willingness to talk.

Question 4: How are you received at work? Do you get support from the leadership? Do you get support from the employees?

We wanted to examine if the respondent felt acceptance and support, both from management and fellow employees when carrying out their work. Our research model considers acceptance as an important factor in a social engineering defence. Acceptance can only be achieved when management understands why security is a priority and the information security department also understands the values and goals of the management. We wanted to examine the respondents' opinion on the matter.

Question 5: Does your company work with threat metrics? If you do, how?
This is related to the factor Assessing the threat, which is part of our research model. We examine if the companies work with any threat assessment or risk analysis tools and how they incorporate them in their security work.

Question 6: If you work with awareness of social engineering, how do you do it?
This question is related to the awareness factor which is a part of our research model. The question investigates how the organizations work to achieve awareness amongst their employees and if they consider awareness to be as important as our research model has shown.

Question 7: Do you perceive the threat to your company by IT attacks is greater today than when you started working here? If yes, why do you think that is?
This question is also related to assessing the threat. In our perception, the threat is bigger today than it ever was which would lead to a greater need for threat assessments today. We want to know if the respondents shared our view of the matter.

Question 9: Say you were to receive unlimited resources, how would you have used the money to increase security?
This question was almost our favourite. Even though it is not covered by our research model, it reveals what parts the respondent would prioritize if given an extended budget and should reflect what specific measures are prioritized by the companies, something we considered to be very interesting.

Question 11: Do you keep some kind of record or statistics of the number of technical or social attacks that are committed against your company?
This question is also related to assessing the threat. In order to do a proper threat assessment, there must be access to statistics regarding attacks. However, social attacks are hard to keep statistics of since the victims often are not aware that they are being attacked. We wanted to investigate how the respondents dealt with this matter.
Question 12: Have you heard of audits? Does your company use them? Do you think they are/could be effective?
We deemed this question to be very important. From our research, we have found audits to be one of the more effective measures against social engineering. This question covers several parts of our research model; both Measures, Acceptance and Awareness. We were interested if Swedish companies used audits and if they did; were there any problems related to them being performed?

3.4 Quality of the interview

To ensure the quality of our interviews, they were designed based on our research model. When designing the interview guide we also made sure that the structure was in line with the examples of interviews mentioned by Jacobsen (2002).

The interview guide was approved by our mentor and sent out in advance to the respondents in order to allow them to prepare themselves prior to the interviews being conducted.

3.4.1 Ethics

The empirical material collected in this study is based on interviews conducted with voluntary informants, which according to Jacobsen (2002) and Denscombe (2000) is one of the basic conditions. It is important that the interviewed respondents are well aware what the information collected will be used for and its purpose.
Prior to every interview, the respondent was informed about our research questions and the purpose of our study. In the same nature, all the respondents have participated by their own free will.

The respondents have been given the opportunity to approve or disapprove the transcribed material. A document with the transcribed material was sent to the respondent via email a few days after the interview, this was influenced by the time we had to transcribe the recordings. Two of the respondents required being anonymous to partake in the study. In order to be consistent, we decided to keep all respondents anonymous. We believe that our empirical material validity is not affected by the anonymity. The presentation of the companies and respondents provide sufficient insight. We have contacted several companies that for various reasons have chosen not to participate in our study. We respected their choice and instead, we continued with companies that were willing to take part. No one has been pressured to participate.

3.4.2 Validity and reliability

It is of the utmost importance that the results of our study are reliable, credible and properly validated. This implies that the study has been based on the problem area to secure that the content of the study is relevant. Validity means that the chosen subject investigated in the study is the one that is relevant for the context and therefore, the one that should be measured. (Jacobsen, 2002).

When performing a scientific study with a qualitative research approach, it is often easier to ensure validity since the authors often have a stronger personal contact with the respondent compared to a quantitative study. (Jacobsen, 2002)
However, the personal contact can also have an impact on the respondents' answers. The respondent might, consciously or unconsciously, answer falsely in order to meet the expectations of the author. To avoid this problem and to strengthen the validity of the study, we have used open questions and we have asked the questions from a neutral point of view. We have used the same approach and asked the same questions in all the interviews to ensure reliability.

Our three interviews, performed at three different production companies, has offered us different perspectives. This results in an increase in the generalizability of the study which contributes to added credibility. (Jacobsen, 2002).
According to Jacobsen (2002), obtained empirical data should always be analysed from a critical perspective.

Consequently, we have been critical during our analysis of the collected empirical data. The analysis was later evaluated and compared to previous literature and articles which we presented in our research model The validity of the study is increased due to the fact that all three authors of the study were been present during the interviews. This ensures that the answers are interpreted, not from just one single perspective. To ensure validity, we offered the respondents to review the transcribed interviews and revise anything they felt had been misinterpreted, something that they did take advantage off.

3.5 Collecting and analysing interview data

To achieve an adequate result, Jacobsen (2002) claims that structure and reductions of the empirical data is necessary. The analysis consists of three stages; description, systematization and categorization as well as combination. This is done in an iterative process. (Jacobsen, 2002).

The description consists of the interviews adequately summarized. (Jacobsen, 2002).
The transcribed data comes with line numbers to enable a more detailed navigation in the transcribed material. Every interview starts on a line number and is separated from the others due to the individual naming convention of the respondents, i.e. Respondent A, Respondent B, Respondent C in accordance with Denscombe (2000).

By categorizing the empirical data, we quickly identified associations between the interview responses and our research model. The data was categorized in line with our research model. The data is presented in the empirical results section.
The combination phase involves pointing out the similarities and the discrepancies' that we identified from our empirical study and our research model. This will be presented in the discussion. To make the study unified, we have divided both our empirical analysis and our discussion into identical topics, the same topics that our research model consists of.

4 Empirical Study Results

In this section, we will present the results from the three interviews that we performed. The results are divided by questions and the answers are formulated in keywords which is described in the scientific method section.

Question 1: Tell us about yourself; your background within the field, within the company and specifically what duties and responsibilities you have within your current position.

Respondent A	Respondent B	Respondent c
Global Company 16.000 Employees Head of IT-Security	Scandinavian Company 150 employees InfoSec Manager	Global Company 70.000 Employees Head of IT-management

Question 2: What is your definition of social engineering?

Respondent A	Respondent B	Respondent C
People, not technology Not completely mitigatable by technical controls The art of Conning	Manipulating people Stealing information Hurtful for the organization	Get information through communication Taking advantage of human kindness Create a sense of trust

Question 3: How is your company working to prevent social engineering?

Respondent A	Respondent B	Respondent C
Awareness E-learning Technical controls	Awareness Continuous education, once a year Policies/principles/procedures /standard	Awareness Security theme month Technical controls

Question 4: How is your work received? Do you feel support from management? Do you feel support from other employees?

Respondent A	Respondent B	Respondent C
Constant resistance Mostly from employees Budget-question	White-noise resistance[1] Social skills help Consequences Reason Measures	Acceptance From both employees and management Mutual understanding

Question 5: Does your company work with threat metrics? If you do, how?

Respondent A	Respondent B	Respondent C
No Too many attacks Hard to know when you're attacked PLM/IDP[2] It's the future	Yes Threat matrix Workshops	Yes Ongoing project Do it to stay alert Risk assessment templates List all threats and classify them

Question 6: If you work with awareness of social engineering, how do you do it?

Respondent A	Respondent B	Respondent C
E-learning Big-brother sees you Posters Core relevance	Continuous education Audits Policies	Policies Theme month Posters Core relevance

Question 7: Do you perceive the threat to your company by IT attacks is greater today than when you started working here? If yes, why do you think that is?

Respondent A	Respondent B	Respondent C
Bigger threat today Money talks	Up and down World conflicts affects	Goes up and down Less spam today Doesn't know why

Question 8: Do you feel that there is a conflict between seamless access/communication and security in your company? If you do, how do you deal with it?

Respondent A	Respondent B	Respondent C
Yes, very much Communication between management and IT-security How much is our information really worth?	Internal struggle Correct information classification Pro Seamless Access	Yes and no There must always be a balance but I wouldn't call it struggle

Question 9: Say you were to receive unlimited resources; how would you use the money to increase security?

Respondent A	Respondent B	Respondent C
Making E-learning fun Right information to the right person	Open infrastructure Awareness Involving the employees Protect core information	Formal & Informal Education Create awareness

Question 11: Do you keep some kind of record or statistics of the number of technical or social attacks that are committed against your company?

Respondent A	Respondent B	Respondent C
No Almost impossible to measure social attacks	As much as possible Hard to measure social attacks	Yes Incident reports

Question 12: Have you heard of audits? Does your company use them? Do you think they are/could be effective?

Respondent A	Respondent B	Respondent C
Not working with them Have heard of them Colleagues talking fondly of them Maybe in the future No privacy issues	Sometimes Both physical and technical Intrusive Explain the reason in order to gain acceptance	Yes Welcome activity ce the reason is explained Creates awareness No privacy issues

[1] White Noise Resistance – Resistance that can be easily overcome
[2] Product Lifecycle Manager/Intrusion Detection Prevention

5 Analysis

In the following section, we will present the empirical data that we collected when performing our interviews with the IT security managers. The data is presented from a holistic perspective where our goal is to distinguish patterns that will help us achieve the goal of our study and answer the questions of how aware Swedish companies are of social engineering and what measures they use to protect themselves from the threat.

5.1 Awareness

"Social manipulation is to manipulate someone into believing you have good intentions, allowing you to gain information or gain access to systems."
(Translated, Respondent B, Appendix 4, Row.63)

When asked how they would define social engineering, all three of the interviewed companies produced a similar explanation. They were obviously all aware of what social engineer is, however, their thoughts on what the consequences of a successful social engineering attack would result in differed. Where company A and B thought that a social engineering attack could result in real and severe damage, company C downplayed the threat. The respondent from company C felt that social engineering would not lead to sensitive product information being compromised and he believed that large scale technical attacks were the threat to focus on when it comes to real damage potential.

Even though we did not speak to any employees in the companies except the IT security managers, there seemed to be a consensus that personnel in Swedish production companies were very aware of the threat of social engineering. This is handled via security measures, such as education and awareness programs, which will be highlighted in the next section. However, the respondent from company A did mention that even though personnel in their Asia division were aware of social engineering they had encountered a problem which conflicted with implementing security measures.

"For example, in Asia there is another problem, seniority. You do not say no to someone who is older."
(Translated, Respondent A, Appendix 3, Row.60)

However, as we have chosen to focus on Swedish companies, we continue the analysis with a pure focus on strategies in a Swedish context.

5.2 Measures

"I usually say that at least 50% of information security in a company lies with the employees. You cannot remove it or mitigate it by technical means. It's just not possible."
(Translated, Respondent A, Appendix 3, Row.19)

All of the respondents interviewed agreed that, even though technical controls has a place in IT security, it cannot be the sole solution to handling a problem that is first and foremost of human nature. Rather, the respondents felt that, to tackle this problem, there was need for several security controls to work in conjunction. The security measures that the respondents emphasised was education, awareness programs, technical mechanisms, audits and policies. These security controls are of both formal and technical nature, where formal focus on rules and responsibility like policies and the technical are for example firewalls. Even though all the respondents we spoke with felt that there was a need for both formal and technical controls, respondent B mentioned that when companies are downsizing and firing project managers, the technicians were usually the ones that got to keep their jobs. This might result in security measures taking a technical approach rather than the softer version, which could explain why security standards like PCI DSS (Payment Card Industry Data Security Standard) and the threats identified in OWASP (Open Web Application Security Project) are of mainly a technical aspect.

"See something, say something."
(Respondent C, Appendix 5, Row.25)

Awareness of what social engineering is and the ability to spot suspicious behaviour is something that all of the interviewed companies felt was a key essence in tackling social engineering. Being the main focus of the company's strategy for security measures also simulated this. All three of the interviewed companies applied a basic education program that is mandatory for all new employees. These education programs are not focused on social engineering specifically but social engineering was definitely a part of them. Respondent B also stresses the need for continuous training in IT security as an important part of the security and he feels that a basic training is not enough. The employees of company B had to attend an education in IT security at least once a year. Company A had a similar approach where the IT department pushed for E-learning which is performed via their website. Company C did not have continuous education in that sense but instead, they made use of monthly newsletters detailing security risks. They also had a security month each year in September where bulk emails are sent out to employees and informative posters are made and posted in the offices. There is also another big difference between the company A, B and company C. Both company A and B had a follow up control that checked whether the employees had taken part in the education or not. Company C had no such follow up and rather trusted that the employees made sure to stay informed. This can be put in contrast to company A's control that not only checked if an employee had taken part in the E-learning but also timed how long the employee had attended the course.

We were shown some statistics from the latest test and it was clear to us that some employees, even though they had attended the course, had skipped the information. This was obvious from the time the education had taken. Where some employees had used 15 minutes to complete the course, some employees had completed it in mere seconds.

They all have comprehensive policies that determine how the employees should work. Company A and company B had their policy disassembled into several detailed policies to make the information more comprehendible while Company C did not.

"In that case I would have had opened it all up, all the firewalls and everything."
(Translated, Respondent B, Appendix 4, Row.393)

The reply from respondent B to our question of what they would do if they were given unlimited resources can be put into stark contrast compared to how company A and C wanted to deal with their technical security. Company A and company C rather focused on locking down the systems with firewalls and layered protection. However, at this point, all three companies use firewalls to protect their systems and servers. All three companies points to the importance of encrypting the information on hard drives and servers. Though as respondent B puts it, only the computers that are deemed to have valuable information gets their hard drives encrypted, seeing it is a question of economics as well. When it comes to technical perimeter protection, the companies differ somewhat. Company B was the most extreme case where. In order to tackle tailgating, not only did you need a key tag to get into their building but you also needed to have used your key tag to enter. Otherwise, the tag wouldn't grant access when trying to leave. People who did not work in the building had to be let in by an employee attending the door. Company A had a system where you needed a key tag to get into the building and people who did not work there had to enter via a special door where an employee had to let them in. Company C had a somewhat more relaxed technical perimeter protection but also used a key tag to enter the building.

In order to access the internal systems and networks employees of company A and B had to use a certificate. Company A used a TPM-chip (Trusted Platform Module) and company C used a certificate stored on a USB drive that once you inserted it into your computer you had access. The access was still limited to authorization levels as mentioned in the policy section.

"We have looked at it, we do it, and we do it from time to time."
(Translated, Respondent B Appendix 4, Row.282)

When asked about if the company performed audits or so called white hat attacks, we perceived that the all of the respondents tensed up somewhat. Two out of three of the companies did admit that they were performing audits on their employees while the third expressed his interest in it, though he felt that his company currently did not have the funds to go ahead with it. When asked if they felt that the employees experienced discomfort or anger about being targeted by these simulated attacks, both of the respondents who admitted to using them said that the employees had few or no problems with it, at least when its purpose

was properly explained. Respondent C did mention that it was important that the simulated attacks did not occur too often, lest they would interrupt the normal work flow which is something respondent B felt was important as well.

5.3 Acceptance

"I'm sure there are photos of me out there which they use to throw darts at."
(Translated, Respondent A, Appendix 3, Row.49)

The respondent from company A felt that there were definitely a resistance against the IT security department and what he was trying to do. As his company uses filters that the employees have to get through in order to access websites, some employees are angered that they do not get access. The respondent from company B felt that, even though there were resistance towards the IT security department, the respondent still felt that he was quite able to convince the employees of the benefits of the security and its greater purpose.

5.4 Accessing the Threat

"When there is a new virus threat we often know about it before the FBI does."
(Translated, Respondent C, Appendix 5, Row.136)

When it comes to evaluating the threat, two out of the three interviewed companies mentioned that they used threat metrics. These metrics are not limited to the threat of social engineering but threat in general. The idea of a threat metric is to assign a number, for example from 1 to 3 to the risk of something happening that would have a negative impact on the company. You when then assign a number illustrating how severe the consequences would be if that risk would be realized. And finally, you would assign a number depicting how hard it would be to minimize that risk. This would provide a base on how to properly perceive a threat. Even though one of the three companies did not currently work with threat metrics, the respondent informed us that they intended to implement it soon. Respondent C also emphasized that the IT security organization that is located in the US works intensively to spot new virus threats.

6 Discussion

In this section, we will discuss our empirical results and compare it to the studies we have highlighted in the research framework section.

6.1 Awareness

The study conducted by Dimensional Research (2011), which we discuss in our research model, stated that the awareness towards social engineering amongst IT-personnel was very high.
Our findings were in accordance with this. In all of our interviews, we questioned the respondents about their perception of social engineering. We deemed that every respondent had a good idea of what social engineering is based on the definition we highlighted in the theoretical chapter. However, their perception of its possible impacts and consequences varied. In our opinion, the companies that were well aware of the possible impact were more inclined to build a solid defence while the company that underestimated the possible impact was far less dedicated in building their defence. Our conclusion from this is that a good awareness, not only about social engineering itself but its' potential impact goes hand in hand with the quality of the companies security measures.

But, it is not enough to have awareness in the management, or even in the IT-department for that matter. The whole organization must be aware of the threat that is social engineering. The study performed by Bullée, et al (2015) showed that awareness has a significant positive effect and in their experiment, respondents that were not subjected to extra awareness training were 2.84 times more likely to be subject of a social engineering attack compared to those who were subjected to extra training
.
Our empirical study results also showed that Swedish production companies consider awareness to be the foundation to a good social engineering defence. However, the means to reach awareness are many and how companies decide to work differs. In the next section, we will discuss the different measures that a company can take against the threat of social engineering.

6.2 Measures

As we established early during our research, technical measures are not specifically a part of a social engineering defence, even though they are needed for information security. The respondents' agreed with this and said that technical controls could not be the sole solution to handling a problem that was first and foremost of human nature.
Chris Hagnady (2010), cofounder of Social-Engineer.com and author of several social engineering books, stated in an interview that the first mitigation against hackers employing social engineering techniques was security through education. Our study agrees with this and our respondents held education as a high contributor in achieving awareness in their companies. Even though every respondent agreed with the importance of education, their actual education varied quite a bit. Every company had some form of education but while one of the companies had continuous education made available online in the form of E-learning and proper monitoring of the employees' results, another company only offered a basic security tutorial for new recruits which briefly touched the social engineering subject and offered neither continuous education nor did they monitor the results. This would have made sense to us if it was directly connected to the size of the company but this wasn't the case. It was actually the largest company that offered least education which is suprising.

When it comes to policies, our findings correlate fairly well to what our research showed us. Policies are as Mitnick (2002) said, a vital building block in developing effective controls to counter potential security threats and all the respondents agreed with this statement. The only difference we detected in their policies was the fact that two companies had their policies separated into smaller, comprehensive sub policies while the third company had one general policy that covered all of the parts. Company A's reasoning behind the separation of policies was that they wanted the information the employee had to take part of to be of core relevance. This is when the information is specified for the employee, so he does not have to read about rules that do not affect him. Company A tried to incorporate core relevant information in all of their educations and policies and the respondent even talked about creating interactive web tutorials which asked a set of questions to identify the employee's work role and customize the policy in line with the answers given. We found this very interesting and we believe that this way of working could have a great impact in creating an aware workforce. The honest truth is that no employees are happy if they are forced to do assignments that go beyond their everyday tasks. This issue is more or less avoided, at least information wise, when you work with core relevance. This should improve the willingness of the employees to actually read the information that is sent out to them which inevitably will lead to a more conscious workforce.

Another interesting discovery was the difference in attitudes towards audits. All of the companies we interviewed claimed that there was little resistance or anger affiliated with using audits or simulated attacks on the employees. However the studies we found on prior research in that field pointed to the opposite. There was allot of resistance to what was felt as an invasion of privacy. During the study of phishing by Jacatic et al. (2007) the research blog

was forced to shut down due to users writing offensive messages and demanding the researchers to be fired from the University. The students who unknowingly participated in the audit clearly objected to what they felt was an invasion of their privacy. (Jagatic et al., 2007, p.99). The use of audits to perform penetration testing is likely to be a hot topic in the future, especially since privacy is something people value highly in the west. Not least since the revelations of former NSA employee Edward Snowden and Bradley Manning from the Pentagon. Yet, the companies we interviewed see no problem in the use of audits as long as they are not performed to frequently, as that would have an impact on the daily workflow (Interview Respondent C).
The security measures that the companies we interview applied were the same as is recommended in allot of the studies we found.

6.3 Acceptance

According to Mitnick (2002), acceptance and support from senior management is essential if the security program is to succeed. All of our respondents felt strong support from management. Regarding support from the other employees, the respondents admitted that there was some minor fuss, usually regarding denied access to certain websites or services. Everyone agreed however that this was a problem that was easy to handle and when the complaints actually reached the respondents, they were often easily solved.

All the respondents mentioned that the IT-security department is often considered to be regressive and they are almost seen as an obstacle. This seems to be an issue in most business and is sort of understandable since IT-security's' main objective is to restrict access and make the employees follow rules. However, the respondents believed that the employees deep down understood why IT-security is important and even though they might not always like it, they did accept it.

6.4 Assessing the threat

The fact that there was a difference in how the companies perceived the potential impact and consequence of a successful social engineering attack is interesting. This shows that, even though all the three companies understood what social engineering was, they did not necessarily agree on its' potential impact.

7 Conclusion

Through our study, we established that the Swedish production companies we interviewed are aware of social engineering and that they have well established strategies of how to protect themselves from the threat. However we found that their view of the threat differed, as did their view of the potential impact.

All the companies worked with both technical controls as well as "soft" measures like policies, education and awareness programs. However, the quality of the training varied, something that was directly related to how serious of a threat the companies perceived social engineering.
The same patterns were visible for policies. Every company made use of policies but the company that took the social engineering threat most seriously had the most developed policies and worked with core relevant information. When it comes to technical controls, we decided to put less focus on them in the study since it was apparent that the respondents did not feel it was the major factor in fighting social engineering. Technical controls are indeed a necessity when working with information security and the respondents' agreed to this but, we consider the informal and formal aspects more important.

Only two of the companies used audits as a continuous measure but the third company was aware of the measure and they are planning on using audits in the future. What we found after performing our theoretical research was that audits was a measure that is increasingly being used and the empirical study only enhanced this impression. When performing the interviews, we questioned if there could be any privacy issues when performing the audits. The respondents all argued that this was not a problem but we definitely noticed some hesitation and unwillingness to talk too much about the subject. This leads us to the conclusion that audits are definitely a good measure that, when used correctly, can improve the awareness. However, we believe that employees could potentially be displeased or feel that their privacy was violated by their own company if targeted by audits.
Furthermore, audits will inevitably create pressure on the employees as it will create an atmosphere where the company is watching you and testing you to see how well you perform. Moderation is the key however, as the measure in itself will lead to employees thinking twice before doing something they should not, though if the measure is applied to often it will likely lead to the employees losing confidence in the IT management.

Two of the three interviewed companies worked with establishing and analysing different threats as well as calculating the risk should any identified risk come into realization. The main reason for using these risk and threat calculations is to be able to show statistics to the management when making decisions about security. One of the respondents explained that it was easy to gain acceptance from both management and other staff members when you are well informed and have figures to back up your statements.

Summary:

- Swedish production companies are very aware of what social engineering is.
- Swedish production companies have several well established methods of countering social engineering vulnerabilities.
    - The formal controls they are using are the spreading of awareness, using emails and posters. They also use education as a tool to ensure that the employees know how to spot a social engineer and how to avoid his or her attack. They also use policies to regulate how the employees use valuable information. There is also clear directions of ownership of data of which the owner is responsible for.
    - The informal controls are the end result of the formal controls. The use of an open culture and the emphasis on not persecuting someone who has been subjected to social engineering helps to counter attacks.
    - The technical controls used are firewalls, certificates and encryption.
- Swedish production companies put their focus on formal measures of protection rather than on the technical when dealing with the threat of social engineering.
- Swedish production companies have identified audits as a useful way to enhance protection but realizes that there are complications related to the practice.

8 Further Research

As this study has focused solely on production companies there is room for further investigation into companies in a broader term, it might be interesting to see if there are differences between different types of companies and also what areas they are based in.

As we noticed in our interview with company A there was an aspect concentrated only to Asia which could have a serious impact on the defence against social engineering. What the respondent mentioned was seniority. It might be interesting to investigate what kind of problems might be geographically oriented.

Due to our chosen scope only IT managers were chosen to be interviewed which means that there is room for further studies into how aware the employees are in the companies and how they perceive the threat of social engineering.

As we have identified auditing to likely be a procedure that more companies will use in the future, studies that further investigate what impact these simulated attacks will have on private privacy and how the employees will feel about it seem highly valuable.

9 References

Bryman, A. (2002): Samhällsvetenskapliga metoder. Malmö: Liber.

Bullée, Jan-Willem H.; Montoya, Lorena; Pieters, Wolter; Junger, Marianne; Hartel, Pieter H.. *The persuasion and security awareness experiment: reducing the success of social engineering attacks.* Springer Science, Business Media Dordecht. January 20, 2015.

Burns, Tom; Nora Machado. Social Rule System Theory: Universal Interaction Grammars. *Centro De Investigacao e Estudos de Sociologia* 2014 http://www.cies.iscte.pt/np4/?newsId=453&fileName=CIES_WP175_Burns_Machado.pdf (Accessed 2015-05-03).

Calabresi, Massimo. US Charges Chinese Government Officials With Cyber Espionage. *Time.* May 19, 2014. http://time.com/104508/u-s-charges-chinese-government-officials-with-cyber-espionage/ (Accessed 2015-03-28).

CNN International. A convicted hacker debunks some myths. *CNN*. October 13, 2005. http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/ (Accessed 2015-05-03).

Cook, James. "FBI Director: China Has Hacked Every Big US Company,". *Business Insider*. October 6, 2014. http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 (Accessed 2015-04-06).

Denscombe, M. (2000). Forskningshandboken – för småskaliga forskningsprojekt inom samhällsvetenskaperna. Lund: Studentlitteratur.

Dimensional Research. The risk of Social Engineering on Information Security: A Survey of IT-Professionals. September, 2011 http://www.greycastlesecurity.com/resources/documents/The_Risk_of_Social_Engineering_on_Information_Security_09-11.pdf

(Accessed 2015-03-24).

Eneroth, Bo. (1989). *Hur mäter man "vackert"? - grundbok i kvalitativ metod*. Göteborg: Natur och Kultur.

Federal Trade Commission. June, 2003. http://www.ftc.gov/os/2003/guessanalysis.htm (Accessed 2015-04-15).

Fehr, Ernst; Gächter, Simon. Fairness and Retaliation: The Economics of Reciprocity. *Journal of Economic Perspectives* 14 (3). Summer, 2000. http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.14.3.159 (Accessed 2015-05-08).

Hadnagy, Cristopher. (2011). Social Engineering:*The Art of Human Hacking*. Indianpolis: Wiley Publishing, Inc.

Jagatic, Tom N.; Johnson, Nathaniel A.; Jakobsson, Markus; Menczer, Filippo. Social phishing. *Communications of the ACM*. Vol. 50 No. 10. October, 2007. http://cacm.acm.org/magazines/2007/10/5556-social-phishing/fulltext (Accessed 2015-05-05).

Johansson, Tommy K. Polis-trojanen som låser din datorn och hotar om böter. *TkJ.se.* March 14, 2012. http://blogg.tkj.se/polisen-boter-bedragier-it-brott/ (Accessed 2015-05-06).

Landoll, Douglas. (2006). The Security Risk Assessment Handbook – A complete guide to performing Security Risk Assessments New York: Auerbach Publications

Long, Johnny. (2008). No Tech Hacking - *A guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Burlington: Syngress Publishing Inc.

Manske, Kurt. An Introduction to Social Engineering. *Information Systems Security*. December 21, 2006. http://www.tandfonline.com/doi/pdf/10.1201/1086/43312.9.5.20001112/31378.10 (Accessed 2015-04-28).

McDowell, Mindi. Avoiding Social Engineering and Phishing Attacks. *United States Computer Emergency Readiness Team.* February 06, 2013. https://www.us-cert.gov/ncas/tips/ST04-014
(Accessed 2015-05-03).

Microsoft. (2006). *How to Protect Insiders from Social Engineering Threats* *https://msdn.microsoft.com/en-us/library/cc875841.aspx*
(Accessed 2015-04-28).

Mitnick, Kevin. (2002). *The Art of Deception.* Hoboken: John Wiley & Sons.

Olavsrud, Thor. (2010). 9 Best Defences Against Social Engineering Attacks
http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm
(Accessed 2015-04-28).

OWASP, The Open Web Application Security Project.
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
(Accessed 2015-04-06).

Rouse, Margaret. Pretexting. *TechTarget*. May, 2011.
http://searchcio.techtarget.com/definition/pretexting
(Accessed 2015-05-03).

Ryen, Anne. (2004). *Kvalitativ intervju - från vetenskapsteori till fältstudier*. Malmö: Liber.

Stanley, Milgram. Behavioural Study of Obedience. 1963.
http://www.holah.karoo.net/milgramstudy.htm
(Accessed 2015-05-07).

Stasiukonis, Steve. Social Engineering, the USB way. *Dark Reading*. June 7, 2006.
http://web.archive.org/web/20060713134051/http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1
(Accessed 2015-05-06).

Thornburgh, Tim. Social Engineering: The "Dark Art". *InfoSecCD Conference'04*. October 8, 2004.

Valentin, Jesse. How to Plan a Social Engineering Assessment. February 3, 2014. Infotec Institute http://resources.infosecinstitute.com/plan-social-engineering-assessment/ (Accessed 2015-05-03).

Walters, Riley. Cyber Attacks on U.S. Companies in 2014. *The Heritage Foundation*. October 27, 2014. http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014 (Accessed 2015-04-06).

Wikipedia. Internet of Things. May 8, 2015. http://en.wikipedia.org/wiki/Internet_of_Things (Accessed 2015-05-12).

Workman, Michael. Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security.* December 19, 2007. http://www.tandfonline.com/doi/full/10.1080/10658980701788165 (Accessed 2015-04-08).

Appendix 1

- Berätta lite om dig själv; Din bakgrund inom branschen, inom företaget och specifikt vilka arbetsuppgifter du har i din nuvarande arbetsroll

---

- Vad är social engineering enligt dig?

- Hur arbetar ni med social engineering i företaget? Utbildning/Policies/Tekniska lösningar

---

- Hur känner du att du blir bemött i ditt arbete? Stöd från ledning? Stöd från andra anställda?

- Har ni arbetat för att fastställa hotbilden mot ert företag, i så fall hur?

- Hur ser ert aktiva arbete ut för att skapa awareness för social engineering bland de anställda?

- Upplever du hotbilden mot ert företag som större eller mindre idag än när du började arbeta för företaget? Vad tror du det beror på?

- Känner du av kampen mellan seamless access/kommunikation i företaget & att ha ett så säkert företag som möjligt? Hur hanterar ni det?

- Om du i dagsläget hade fått ett betydande tillskott till din säkerhetsbudget, vart hade de pengarna gått?

_____

- Arbetar ni med riskanalyser på något plan?

_____

- För ni någon statistik på antal tekniska/sociala attacker utförda mot ert företag?

_____

- Arbetar ni med/har du hört talas om s.k. audits? D.v.s. när man simulerar en attack på sitt eget företag för att testa personalen! Om inte, är det något du tror hade kunnat fungera för ert företag?

_____

Appendix 2

Hej X!
Jag heter Björn Kronberg och fick den här adressen av X!
Jag tänkte kolla med dig om du skulle tycka det var okej att ställa upp på en intervju om IT säkerhet. En kort introduktion först. Jag läser sista terminen på Systemvetenskap på Lunds Universitet och skriver just nu min kandidatuppsats om social engineering. För att förklara vår definition av vad social engineering är så kommer här ett citat.

"Social engineering is the art of manipulating people into doing things, particularly security-related-such as giving away computer access or revealing confidential information. Rather than breaking into computer networks or systems, social engineers use psychological tricks on humans."

Jag och mina två gruppmedlemmar försöker utreda företags medvetenhet om vad social engineering är och hur man kan skydda sig mot det. Vi har valt att inrikta oss mot produktionsföretag i Skåne där vi redan fått intervju med bland annat X och nu hoppas vi på att få chansen att träffa er på X med! Målet med studien är att skapa ett ramverk som företag kan använda för att öka sitt IT-skydd.

Som deltagare i studien kommer du att få tillgång till alla resultat och kommer att få uppsatsen skickad till dig. Du kommer även att vara helt anonym.

Våra frågor till dig kommer att avhandla dina tankar om företagets:

Formella Åtgärder för IT säkerhet - Företagspolicys
Informella Åtgärder - Allmän företagskultur
Tekniska Åtgärder - Brandvägg, Passerkort, Antivirus, Auktorisering/Tillstånd etc.

Vi kommer även att prata om ditt företags syn på social engineering, hur ni utbildar er personal och vilka åtgärder ni har satt in för att motverka detta samt hur ni motiverar de kostnader ni har i samband med er IT säkerhet. Vi vill även ha lite synpunkter på vilka åtgärder du hade tagit om du hade haft obegränsad budget.

Intervjun kommer att vara semistrukturerad men det är en diskussionsintervju vilket innebär att vi vill skapa en dialog mellan den som intervjuar och respondenten.
Jag hoppas att detta har gett dig en lite tydligare bild av vad vi är ute efter.

Tack för din tid!
Mvh Björn Kronberg

Appendix 3

Björn: Vi är en studentgrupp från Lunds Universitet, Systemvetenskap, och vi håller på att skriva vår kandidatuppsats i social engineering. Vad vi då har inriktat oss på är; Vad gör företag för att skydda sig mot social engineering, är det något man är medveten om och finns det möjlighet till att skapa någon sorts ramverk till hur man kan förbättra sin säkerhet mot det.

Respondent A: Jag är respondent A, Informationssäkerhetsansvarig i koncernen company A. Det finns ju egentligen bara jag så, jag är lite one man show. Jag sysslar med alla delar, både informationssäkerhetspolicies, guidelines och implementationer. Social engineering awareness framför allt då. Min bakgrund är Civilingenjör från D-linjen, Lund. 1990 gick jag ut. Bakgrunden är egentligen teknisk så jag har jobbat mycket på annat företag. Totalt 25 år inom company A. Bott några år i Singapore. Ganska bred bakgrund egentligen.
Informationssäkerhet har inte varit väldigt utvecklat i ett såhär gammalt industribolag så att jag klagade väldigt mycket på att det inte fanns någon. För fem år sedan när vi gjorde en omorganisation så fick jag den rollen så jag har byggt det från grunden, det som finns i bolaget.
Då menar jag inte det tekniska som jag var ansvarig för tidigare utan mer den mjuka delen, policys etc.
Jag brukar säga att åtminstone 50 % av informationssäkerheten i ett företag sitter egentligen hos de anställda. Man kan inte bygga bort/mitigera det med tekniska åtgärder. Det går inte. Det är misstag, det är social engineering, att de blir övertygade om att de ska ge ut information och det är direkt, by intent så att de verkligen vill göra det. Det är väl lite ingångsförutsättningarna från min sida när jag tittar på det. Men, ni kanske har 1 miljon frågor? Så kan vi bolla idéer fram och tillbaka och jag kan visa lite data på saker som vi gjort.

Jocke: Vi var väl till och börja med intresserade av din kunskap om social engineering då vi har haft svårt att bilda oss en uppfattning huruvida företag idag är medvetna om social engineering eller inte. Men, det låter på dig som det är ett ämne ni arbetar mycket med.

Respondent A: Njae, det beror på vilken kontext du pratar om. Om det gäller att ändra folks beteende så är det ju som att ändra en supertanks riktning; det tar liksom 49 sjömil innan de ens börjar att flytta på sig. Sedan slutar folk och så börjar det ny personal och så kommer de nya in blanka. Det är rätt svårt i en organisation som company A, där man har 250 sajter och flera av de anställda inte kan engelska. Det är en evig kamp skulle man kunna säga, när det gäller folks hjärnor och hur de tänker och vad de går- och inte går med på. Samtidigt blir de ju duktiga efter hand tycker jag, att meddela när saker och ting händer och villiga att skydda information. Samtidigt som de är helt hejdlöst vilda när det kommer till access:a saker på internet så, det går åt båda håll. Vi gör tekniska controls för att minimera exponeringen när

det gäller internet och trojaner och liknande skräp i vår miljö. Men, även där möter vi motstånd.

Björn: Hur kan det motståndet te sig?

Paul: Vi har satt en lösning på plats. Tidigare hade vi s.k. brickor som var tidskontrollerade så att när man loggade på skulle man ange en kod och den har vi då tagit bort så att vi certifikat till maskinerna istället. Så fort man kopplar upp sig mot internet på en PC från company A så är du inne i tunneln. Det gör att det går via filters som finns hos oss. De kommer inte åt Svenska Spel, de kommer inte åt Netflix etc. Där öppnas tickets hela tiden på att det är för jävligt och att storebror ser oss syndromet. Jag är säker på att det finns foton på mig runt om i världen där de kastar pil på mig. Då gäller det att stå fast och verkligen vara säker på sin ståndpunkt. Datorn är ju ett arbetsredskap och ingen privat. I så fall får de ta med en egen padda eller liknande.

Jocke: Hur pass medvetna tycker du att personalen är om den sociala hotbilden när du kommer ut och informerar om det?

Respondent A: Jag/Corporate IT är ju egentligen väldigt lite ute på bolagen. Mycket kommunikation via webb. Jag är ute en hel del eftersom jag gör internrevisioner också. Nästa vecka ska jag till England och då passar jag ju på och informerar. Men, det är väldigt varierande, det beror på kultur. Tillexempel i Asien finns det en annan problematik, “seniority”. Man säger inte nej till en äldre. Vilket kan bli ett problem när det gäller företagets informationstillgångar. Det finns ingen annan stans, det är bara i den Asiatiska kontexten. Mycket auktoritet, man trampar inte någon på fötterna. Och det är något man måste jobba med, att de anställda förstår att företagets hemligheter tillhör företaget, inte de anställdas.

Björn: Har ni någon speciell strategi i just Asien då?

Respondent A: De är en del av den E-learning vi har gjort för social engineering. Jag har två stycken E-learnings just nu. Den första är en grund, informationssäkerhet, och den andra är en social engineering. Där har jag då även gjort Portugisiska /Polska/Kinesiska/Koreanska subtitles. De förstår ju inte vad de lyssnar på när det är på engelska. Sedan hålls det classroom-sessions som jag har gjort parallella i PowerPoint så att de kan översätta till sina språk men i samma kontext. Sedan är company A speciella då vi äger 20-30 bolag som egentligen är våra direkta konkurrenter. De är inte en del av company A men de ägs utav company A och ska därför följa våra corporate policies. Där är också ett problem då de inte har E-learning eftersom de inte har tillgång till vår "portal". Och det är också en utmaning då vi ska nå ut till de företagen också. Vi kan ju inte påverka de bolagen alls förutom när det gäller policies.

Jocke: Denna E-learningen ni har via portalen; är det något frivilligt eller är det något alla måste genomföra?

Respondent A: Alla ska genomföra den utbildningen inklusive ”blue-collars” och de har ju inga datorer så där skickar de in listor med underskrifter. Det är ett stort jobb faktiskt. Vi är uppe i 16 000 deltagare. Jag har ju pushat Vd:arna runt om i världen om att detta måste göras. Jag har en repository här på min dator full med rapporter och mail skickade till alla VDs. Jag har haft ett Excel-ark där jag kan se exakt vilka som är gröna/gula/röda som jag direkt kan pusha till VDs.

Jocke: Då kan man med andra ord påstå att det finns en väldig medvetenhet om social engineering i företaget?

Respondent A: Ja, det tycker jag. Sen sker det såklart misstag, det går ju inte att kunna undan. Den mänskliga faktorn kommer alltid att finnas. Senast igår gick vi ut med en ny policy vid namn "Acceptable Use" där vi säger att vi har rätten att monitorera och de har rätt att använda internet tillexempel. Sen är där då en lång lista med not acceptable use. Det finns relaterade policys som hjälper folk med deras beteende och att de lite grann känner "storebror ser" känsla så att de inte kan fuska hur mycket som helst utan att det sker någon åtgärd. Och vi har möjligheter till det. Verktygen finns ju. Men, vi gör det inte då det skulle kräva alldeles för mycket diskutrymme. Man kommunicerar ju bara delmängder av det till de anställda, need-to-know basis.

Jocke: I Sverige pratar man mycket om personlig integritet, finns det någon problematik med övervakning i Sverige?

Respondent A: Extremfallen är Tyskland på ena sidan som är privacy mässigt med högst krav av alla länder. Tittar man på andra sidan där man inte ens får göra någon business, som exempelvis Iran. Där är andra sidan av spektrat. Sen finns det ju allt där mittemellan. Jag hade en fråga igår från Indien där man ville ta ut alla mail för hela den asiatiska avdelningen för alla anställda. Då sa jag att man måste gå till varje advokat i varje land och höra vad deras privacy är. I vissa fall i Venezuela kan de stämma företaget på ganska mycket pengar om man bara gör det. Du måste få ett godkännande av rätt person först.

Jocke: Det är med andra ord ett väldigt stort arbete att hålla dessa policys i ett globalt företag med tanke på att det finns olika regler i de olika länderna?

Respondent A: Precis. Det blir en lokal kontext. Policy-mässigt är det inte speciellt svårt. Operationellt är det däremot svårt. Det är den operationella delen vi inte riktigt har koll på. Det blir ju land för land.

Jocke: Social engineering vs phishing; vad säger du då?

Respondent A: Jag ser väl ingen större skillnad på de två.

Björn: Det är ju en del av social engineering.

Respondent A: Jag håller med! Phishing-attacker är ju en form av social engineering då de har lurat dig att klicka på någonting du inte borde klicka på och sen är det ju kopplat till malicious code, t.ex. trojaner etc.

Björn: Hur värderar du riskbilden? Är det de tekniska eller de sociala aspekterna av social engineering du ser som mest problematisk?

Respondent A: Mest problematisk är ju egentligen intellectual property, d.v.s. att våra kronjuveler inte ska exponeras. Det görs ju via en phishing attack då de kan få tillgång till en keylogger eller liknande på en PC som då kan kommunicera ut information som inte alls borde läcka.
Vad jag har gjort, som är satt på plats nu 2014 är ett system där vi har fyra olika klasser; Public, Internal, Confidential & Strictly Confidential. Vi säger att information är 100 %. 20 % är då strictly confidential - adresserar management som då är vår ledning. Jag intervjuade alla dessa. De fick komma med sina åsikter om vad det var. Vad är det i form av RaD (Research and Development?), vad är det i form av patent? Och ut kommer det då en infotyp kan man väl säg som i sin tur blir cirka 400 anställda.
Då ska man tänka av 16-17 000. De 400 anställda här ska då ha ett sätt att skydda "detta"! Då är det viktigt att kunna skydda dem på rätt sätt så vad vi har gjort är att vi har en programvara som heter PGP från Symantec som då ligger på en PC-klient. Det är en folder egentligen bara. Det är helt transparent.
Du har en folder på en file-server. Inte på SharePoint men på en file-server. Kopplat till detta då har vi då något som ni kanske känner till, nämligen en active directory. En active directory är ett övergripande bibliotek där anställdas lösenord förvaras.
Så det finns olika roller i detta. Vi har då ungefär 60 personer eller resurser i världen som kan lägga till sig i vilken grupp som helst då de har så höga rättigheter, t.ex. i de här krypteringsgrupperna. Genom att göra detta kan de då få access till den information som vi försökte skydda, de 20 % vi pratade om förut. Vad vi då har satt på plats är en logglösning så alla förändringar som sker här resulterar i ett e-mail till mig.
Det måste jag sedan kolla upp för att se vem det är som har lagt till sig i den specifika gruppen. Det fungerar som en sorts survailance.
Dessutom har dessa PC-klienter samma sak. Är det någon som tar över en session, t.ex. en keylogger eller malicious code eller en "sånhär?" där det finns mjukvara för att köra remote controller där du bara tar över sessionen. Du agerar alltså som dom(syftar på admins).
Och kan du agera som de 400 så kommer du ju åt den krypterade informationen. Då är den inte skyddad längre. Skulle man få in någonting som börjar kommunicera utåt så kommer vi att fånga det via denna logglösning. Så, på något sätt finns det survailence på PC-klienten.
Men det är en svår grej, hur skyddar vi egentligen de här bitarna? För det kan ju vara t.ex. vår koncernchef Mr.X som har surfat *ohörbart ord* som har installerat någonting på PC-klienten som antingen ligger och vilar och samlar data eller kan detektera att det finns hemlig information och kommunicera ut den informationen. Men, då kan vi ju iallafall fånga utropet och se hotbilden och få KPI:er och upptäcka att det försvinner ut information.

Detta är ju en rent teknisk lösning som inte handlar om deras beteende. Även om det i grund och botten handlar om deras beteende då den här typen av detekteringar strävar ju till att öka awareness hos ledningen. Och det är där man börjar någonstans. T.ex. denna E-learningen, den gick jag upp med till koncernchefen och påpekade att han inte hade genomfört den. Och då gjorde han den direkt. Det är viktigt att ledningen leder skeppet, att de visar ett gott exempel. Det tror jag är det viktigaste egentligen om man ska ändra folks beteende, att ledningen står bakom dom. För om du inte har ledningen med dig är du ganska rökt. Tycker inte de att det är viktigt så kommer du aldrig få de anställda med dig.
Det är egentligen ett fundament för att kunna skapa en företagskultur. Och genom denna lösning inser de ju en viss hotbild och kan jag då rapportera till de exakt vad som har hänt så skapar jag en medvetenhet hos ledningen som kanske hade varit svår att uppnå annars. Så, samhället hjälper oss lite på traven där med social engineering awareness.

Björn: Rent statistisk, om man kollar på antal attacker ni blir utsatta för, har de ökat med tiden sen du började här?

Respondent A: Ja, det har det definitivt. Vi ser en tydlig ökning av antal attacker. Det är ju en business. Både de tekniska och de sociala hoten ökar årligen. Det är ett resultat av att exempelvis en civilingenjör i vissa länder tjänar mer på den svarta sidan än på den vita. Det är inte svårare än så egentligen; Money talks! Det är beställningsjobb och de kan ta sig in på alla möjliga sätt såsom städare på företag och komma åt vårt interna nätverk på det hållet.

Och det är ju andra bitar som rent tekniskt inte har hängt ihop perfekt, d.v.s. parameterskyddet på insidan. Vi har ju ett platt nätverk med alla dessa 250 sajter där alla resurser kan adressera alla resurser. Det räcker att man kopplar in sig på en av dessa sajter så kan du adressera hela nätverket. Jag åkte ner till en av våra anläggningar i Indien och såg att där satt ett uttag ute vid hissen i ett sådant företagskomplex med ett antal företag. Det är ju bara att ha med sig en bärbar dator och en nätverkskabel så är du inne på koncernens nätverk. Inte så att du genast kommer åt våra system men du har ju access till den begränsade säkerheten som är på insidan och skyddet kanske är lite lägre än vad det är i det yttre skalskydden. Så, min dröm som säkerhetsnörd är faktiskt att inte ha ett intranät. Det vill jag ha bort helt. Man ska skydda resurserna där de finns. För, vart är fienden? Den är utspridd. Och idag kan man inte riktigt se vart company A finns längre då vi är så utspridda. Skulle vi inte ha ett intranät måste de komma hit för att kunna göra intrång och här har vi mycket bättre förutsättningar att kunna övervaka och skydda.

Björn: Jag läste en intressant sak igår faktiskt. Nu går jag lite off topic men; Det var en kinesisk hackergrupp som har lyckats hacka ett nät som inte har någon koppling till internet. Jag vet inte riktigt hur det gick till men, de hade lyckats med det iallafall.

Respondent A: Det räcker att du har din PC kopplat till ditt intranät och så har du samtidigt en GSM-koppling via t.ex. en mobiltelefon kopplat till internet. Då kan du agera brygga med din PC och då har du en koppling till insidan. Så, har du bara kompromitterat en PC som ibland kopplar upp sig till internet, då har du en gateway. Då kan man ha en trojan som

samlar den information du vill ha på insidan som sedan kommunicerar ut den informationen så fort gateway:en öppnas. De flesta företag har ju någon form av koppling till internet någonstans, det är svårt att undvika. Så var det inte förr, då var man helt rabiata. På Tetra-Pak tiden så hade vi disketter vi tog saker från internet till insidan, det var vår gateway. Vi var väldigt försiktiga med det där internetet.

Jocke: Ja, och det där är ju ett problem. För att maximera säkerheten vill man ju inte ha internet och som du sa förut, gärna inget intranät heller. Den som sitter på andra sidan och analyserar företaget ur ett effektivitetsperspektiv snarare än ett säkerhetsperspektiv håller ju nog inte med dig dock. De vill ha ett seamless intranät så att varje anställd kan utföra maximalt antal uppgifter utan att behöva använda sig av någon annan. Där är en balansgång som kan vara ganska knepig, eller?

Respondent A: Ja, det är ju ett problem. De förstår inte riktigt att konceptet seamlesness och den enkelhet och vilja att göra business som det skapar, att det även skapar en hotbild. Vi anses ju då vara bakåtsträvande och jobbiga typer som håller på och tjatar hela tiden. Det jag har fokuserat på de senaste två åren är väl egentligen att definiera risk ägandet i företaget. Vem är det egentligen som äger risken? För det är inte IT-avdelningen. IT ska aldrig äga risk, förutom infrastrukturen då. Och, vad är riskaptiten? Var ligger den någonstans? Desto högre säkerhet, desto mindre frihetsgrad. Det måste definieras på ett tydligt sätt och det är en intressant mänskligt beteende. När man tvingar individer/arbetsroller att äga risk istället för grupper som äger en risk, då är man helt plötsligt väldigt försiktig. Då är man utpekad som individ. Då är man plötsligt beredd att göra lite mer än om en grupp på sju personer äger risken gemensamt. Kollektivt risk ägande är inte riskägarskap egentligen. Detta har jag arbetat med för att återigen öka awareness inom ledningen. De ska vara medvetna. De ska kunna hoppa in i min helikopter, jag ska kunna ta de på en tur och visa riskerna varpå de därefter kan ta ett beslut. Sedan är det inte min sak vilket beslut de tar men då har jag gjort de medvetna om riskerna.

Jocke: Du säger att IT-säkerhetsavdelningen ofta bemöts som en bakåtsträvande och lite tråkig avdelning, som mest förhindrar och ställer till för andra. Samtidigt poängterar du vikten av att ha med företagsledningen på ett projekt som detta. Hur känner du personligen att du har det på company A när du har försökt genomföra dina säkerhetsreformer? Har du haft ledningens stöd eller har det varit lite knorrande fram och tillbaka?

Respondent A: Både och, skulle jag vilja säga. I ert mail ställde ni frågan "Vad hade du gjort om du hade haft obegränsad budget?". Mitt svar på den frågan är "Hur många timmar har ni på er?". Det är ju så, att med hur mycket pengar som helst så hade jag kunnat göra massor av grejer. Men, oftast är det inte värt investeringen och det är ju ledningens beslut att ta, d.v.s. hur värt är det att skydda vår information?
Vi bygger ju en elefant i väldigt väldigt små steg. Så, vi har ju visionen av en elefant men hittills är vi bara på höger fot liksom. Den byggs ju ur ett perspektiv där vi inte haft någonting på plats från början. Så, det är ett Work-In-Progress.

Jocke: Okej, vi förstår. Men, om vi försöker koncentrera oss på det mest akuta istället. Ponera att du hade fått ett betydande tillskott i din budget detta år. Tror du att du hade lagt de pengarna på att utveckla tekniska eller sociala lösningar?

Respondent A: En kombination av de två, tror jag faktiskt.

Björn: Är det något specifikt du hade velat introducera?

Respondent A: Jag har ju en del projekt jag arbetar med för tillfället. Exempelvis har jag skapat sajter där denna information finns lätt tillgänglig och jag har försökt göra informationen visuellt tilltalande. Jag har gjort två stycken E-learnings och sedan har jag gjort en med posters där det är informationsklassifiering. Tanken med den är att de ska tejpa upp det på platser såsom kök, toalett etc. där det finns ledig yta och de ändå inte har något annat för sig för tillfället. Då kan de iallafall sitta och läsa informationen och utnyttja tiden till något.

Detta (visar på datorn) är en animerad bit för att göra reklam för min acceptable-use policy. Jag har jobbat med vår... vi distribuerar ju patcher med jämna mellanrum för att uppdatera våra PCs runt om i världen. Vi har tagit den logistiken, gjort om den och satt en Alfa Laval logga och skapat en pop-up som gick ut igår. Där får alla våra användare i hela världen samtidigt upp en pop-up som säger "Det här är den nya policyn, du kan läsa mer på intranätet. Vill du se klippet nu? Ja/Nej?". Den har jag fått både positiva, negativa och undrande reaktioner på då inte ens vissa IT-ansvariga visste att den skulle lanseras.

---- *Filmen visas - spridda kommentarer och skämt angående filmen, inget av värde!* ----

Respondent A: Detta är ju för att göra det lite roligare att ta in informationen. Det är mer konsumerbart än en vägg av text. I dagsläget finns den endast på vårt interna intranät och det är ett litet problem då vi även har ett antal IT-konsulter som arbetar för oss. I framtiden vill jag även att de ska se filmen och skriva under att de har gjort det. De är ju ett minst lika stort problem som dessutom är IT-proffs så, de är nästan ett ännu större problem.

---- *Vi går igenom deras Acceptable Use Policy* ----

Respondent A: Vi har reasonable personal use. Det är kort sammanfattat typ att "Det ska inte ha någon konsekvens för deras företags målupfyllelse" osv. Sedan har vi not acceptable use och den är som ni ser väldigt långt. Här är allt från barnpornografi till rent praktiska problematiker som exempelvis att man inte får ändra i system settings på datorerna. Skulle man göra det så slutar den s.k. seamless accessen att fungera. För att låsa upp den behöver man nycklar som är 40-tecken långa. Så, det är rent operationella bitar som är inlagda här också. Men, det är väldigt mycket som täcks av detta. Även e-mail och social media & bloggning. Fail to comply är ganska tydlig, det kan resultera i terminering. Det är lite att gå ut och skrika varg, d.v.s. vi måste hota med något allvarligt för att folk ska respektera policyn. Det gäller i grunden att de ska ta på sig Alfa Laval hatten. I min grundutbildning där jag

pratar precis i början. Där tar jag på mig den s.k. company A hatten. Det gjorde jag för att alla ska känna att de är en del av säkerhetsteamet och det är egentligen målet med denna.

Sättet jag jobbar på då där jag skulle välja att lägga budgettillskottet är att jag har skapat en sajt. Tanken med sajten är att kunna kommunicera de policys som finns på ett sätt som gör de konsumerbara för individerna i bolaget. De läser inte policys. De finns ju där men det är ingen som direkt tittar på dom. Och varför skulle man göra det egentligen?
Jag vill skapa mer interaktiva policys, som kanske ställer användaren lite frågor om hans roll, vad han hanterar för data etc. Detta ska sedan leda till att bara de policys som verkligen berör användaren ska visas och allt "white-noise" ska filtreras bort.
De här posterna som vi pratade om innan, de är ju egentligen bara en bild. Men de hjälper användaren att tänka. Med både dessa posters och med E-learningen försöker jag att kontextualisera det hela. Nu när jag acceptable use policyn kommer skulle jag vilja lägga en del av budgettilskottet på att smeta ut den informationen. Får du en PC för första gången i Alfa Laval ska du kunna klicka på sajten och så ska den se till så att du får veta det du behöver. Inte mer, inte mindre utan precis det DU behöver veta!
Relevant konsumerar kontextuell information. Det handlar om att skapa awareness i grundtanken, i sättet vi jobbar. Sedan lägger jag ju otroligt mycket tid på tekniska controls i kombination och i alla projekt finns det checklistor för informationssäkerhet och alla avtal vi skriver ska täckas osv. Men här hade jag velat lägga mycket av krutet i en obegränsad budget. Här är mycket att tänka på.

Björn: En annan sak vi är lite nyfikna på är huruvida ni har gjort någon sort riskkalkyl/threat-metrics?

Respondent A: Nej, det är någonting vi precis har börjat jobba med, dvs riskanalyser. Fast vi har börjat jobba på programnivå. Sales eller PLM(Product Lifecycle Management) exempelvis. Så vi adresserar det egentligen risk register eller något liknande på plats idag. Vad jag har på min karta för året är att se in i världen av IDS/IPS (Intrution Detection Prevention), Malicious Code Analyser, Vulnerability analys osv. Då ska jag titta lite mer på tjänstesidan av det.

Björn:Jag ser att ni använder BitLocker. Det är något vi använder på företaget jag arbetar på också!

Respondent A: Ja, det kör vi. Det är ju en kombination av Seamless Acess & Bitlocker. Utan en Seamless Acess där du har certifikat kopplat till ett TPM-chip (Trusted Platform Module) i datorn utan Bitlocker så är det lite farligt eftersom om man kan gå runt admin lösenordet på PC:n så är du ju automatiskt inne på company A nätverk. Det är det Bitlocker är till för. Det ser till så att du inte kan göra just det.

---- Här visar Respondent A rapporter på hans dator som visar antal attacker mot company A ----

Respondent A: En sådan här rapport får jag var dag. Som ni kan se är där ju lite att ta i. Detta är antal virus inom company A en dag, 380st. Det har vi ju skapat processer för hur man ska jobba i det här men det räcker inte enligt mig. Vi har skapat ett workflow för hur man ska arbeta med varje individuell PC för att lösa problemen. Man måste ju nästan ner till alla de 380 PC för att se vart det kom ifrån, hur det gick till och hur vi ska hantera det. Problemet är att vi inte riktigt har en klar hotbild. Vad är det för något? Är det farligt? Vad är det vi tittar på? Den typen av analysinstrument kommer jag att titta på under året. Där är det viktigt att få rätt fokus. Det är det absolut viktigaste så att man fokuserar på rätt saker. Så vi inte lägger en massa onödig tid på att försöka skydda information som kanske inte är värd att skyddas. Däremot, om man inte vet måste man ta reda på det. Det är likadant med sårbarhet. Låt oss säga att det är något som går End-of-life TLS/SSL eller någonting och så har vi instanser implementerade som utgör ett hot. Hur vet vi det? Den analysmöjligheten har vi inte riktigt idag.

De flesta av attackerna blir omhändertagna tidigt av virusskyddet. Då är det på något sätt hanterat. Men, man ser typen av virus som kommer in. Och, då är frågan, de här Zero-Day attacks som kommer innan virusskyddet är uppdaterat och det som kan komma in utan att det upptäcks överhuvudtaget. Den fångas inte riktigt. Men, bara det här är ju ganska intressant att titta på. Vi är ju otvivelaktigen utsatta för attacker på en daglig basis. Och, det mesta hade gått att lösa med en högre awareness. De flesta virus som kommer in kommer via USB-minnen, surf till externa sajter, bifogade filer och andra "onödiga" sätt.

Björn: Dessa attacker är ju dock tekniska. Hur ser den sociala biten ut? Finns det något sätt att mäta antalet sociala attacker? Blir ni utsatta för sådant?

Respondent A: Nja. Det är ju inte så värst många som lyckas angripa oss vad jag vet. Däremot har vi ju en KPI (Nyckeltal) på hur ofta vi blir utsatta. Det rapporteras till mig när en social attack har utförts. Sociala attacker är ju ett väldigt brett begrepp. Det kan innefatta allt från att inställningsordrar till domstol skickas över E-mail, vilket är lätt att komma över. Till andra som verkligen vet vad de riktar in sig på, som finanschefer runt om i världen där de skickar att koncernchefen snabbt behöver ha flyttat lite pengar. Det kan se väldigt legitimt ut, som att det verkligen kommer från oss, men det gör det då inte. Det kan vara svårt att avgöra och då hör de av sig till mig. Ibland lyckas de ju dock. Vi har haft några man in the middle attacker där vi inte haft nödvändig säkerhet på plats och då har attackeraren lyckats med sitt uppsåt.

Björn: Har ni några exakta siffror på hur många sociala attacker ni utsätts för? Vi håller det såklart anonymt i vår rapport

Respondent A: Nä, det kan jag inte direkt säga att jag har. Det är otroligt svårt att mäta det då vi dagligen får in misstänksamma telefonsamtal. Det är ofta samtal till våra anställda där de påstår att de ringer från servicedesk och behöver ens lösenord för att ändra något. Och det är ju en big No-No, det bör alla anställda veta och det är det som är awareness. Problemet är när våra legitima enheter som hanterar supporten begär klassificerad info över telefon. Då har vi

ett problem. Det kan ju vara t.ex. ett utbyte av personal för våra konsultfirmor i andra delar av världen. Då är awarenessen lägre. Så, jag kan tycka att de externa parterna är ett minst lika stor problem som våra egna anställda. För egentligen önskar vi ju att de parterna också kunde vara inne i vårat seamless acess flöde men de är ju svårare att adressera. De skriver ju såklart under ett NDA(Non-Disclosure Agreement) men det betyder ju bara att de inte kan gå iväg med information från company A. Då kan vi åtala dem. Men de andra bitarna med deras beteende på fritid är omöjligt att ha uppföljning på.

Björn: Skulle du vara intresserad av något sorts verktyg som kan ta statistik på detta?

Respondent A: Absolut. Nyckeltal & statistik är alltid bra att ha. Det är speciellt bra när man försöker sälja in idéer till ledning. Och det är något jag saknar, definitivt. Det blir ju utifrån ett händelseperspektiv. Problemet är att man måste koka soppa när den ska kokas. Det lever ju bara en väldigt kort tid i medvetandet när det är en katastrof. När det stjäls ett antal PC-klienter från oss så skapas det direkt en hög medvetenhet/awareness. Men, den medvetenheten försvinner snabbt när allt är som vanligt igen.

Vi vet att det läcker mer i vissa länder än i andra. Vi går inte mot en DLP-lösning (Data-Loss Prevention) där man kan kontrollera all data då det kräver en väldig massa administrativa resurser. Men vi vet samtidigt vart det läcker, mer eller mindre.

Jocke: Jag läste i någon intervju med Kevin Mitnick att på den amerikanska sidan arbetar de mycket med något de kallar för audits, där man utför egna attacker mot sitt företag för att testa sina anställda och öka medvetenheten i företaget. Är det något ni har arbetat med eller hört talas om?

Respondent A: Nej, det är inget vi arbetar med i dagsläget. Däremot pratas det om det hos mina branschkollegor. Vi har bara inte haft resurserna att utföra det i dagsläget.

Jocke: Okej. Det har inget med Sveriges sekretesslagar att göra? Personlig integritet osv?

Respondent A: Nä, det tror jag inte direkt. Möjligtvis hade man fått en hel del sura kommentarer och blickar av de anställda i företaget men jag tror inte att det hade varit några problem att genomföra det rent regelmässigt. Jag har sett, i ett mejlflöde mellan högre uppsatta IT-säkerhetspersonal i Sverige, att de diskuterar awarenessbiten och en stor svensk aktör(10x större än company A) är inne på att utföra intern phishing för att testa sin personal. Vi på company A har inte riktigt tänkt i de banorna än men det är ju ingen omöjlighet att det kommer i framtiden. Det kan vara väldigt bra för att öka awareness. Det är ytterligare ett sätt.

Jocke: Ja, och dessutom spär man på den "Storebror-Ser-Dig" känslan vi pratade om innan, som kan vara nyttig i rätt mängd.

Respondent A: Exakt. Och social engineering är ju nyttigt för en även privat. Det tror jag faktiskt, att folk har blivit mer medvetna om det i vardagen. Dessa E-learnings vi har gjort är

inte speciellt väl utvecklade mot vad de kunde ha varit. Andra stora industribolag tillexempel har ju en budget som är väsentligt större än vår.

---- *Här visar* Respondent A *deras E-learning video för oss* ----

Denna har jag skickat ut till mina koordinatorer. Jag har pekat ut 8-10st globalt. De får informationen och sen skickar de ut det till lämplig plats, förmodligen på deras sajter.

Jocke: Detta kanske är lite off-topic men, när du gick din ingenjörsutbildning; trodde du då att du skulle jobba med IT-säkerhet i framtiden?

Respondent A: Nej! Jag började att jobba med minidatorer. Då var ett diskkabinett lika stort som ett rum. Så, jag var mer på systemsidan. Sedan gick jag vidare till nätverk och egentligen nätövervakning. Efter det fick jag rollen Globalt Kommunikationsansvarig på company A och IT-säkerhet ur ett tekniskt perspektiv för att sen glida över mer åt den mjukare delen med policys etc. Så, det har aldrig varit någon tanke bakom det men detta passar min personlighet & mina intressen bättre än var jag började. Jag är inte så väldigt tekniskt intresserad egentligen. Men det är bra att ha med sig i bagaget. Det är bra att kunna ta dialog med en tekniker och faktiskt förstå kontexten. Kombinationen är bra.

Min How-We-Work sajt är min kronjuvel. Den gör det attraktivt för läsarna. Och det så man når dom. Man kan göra det via compliance som jag gör idag och trycka ut det men det är inte den mest optimala lösningen.

Appendix 4

Respondent B: Har ni färdiga frågor eller är det en diskussion?

Björn: Alltså vi tänker oss att det skall vara rätt så öppet så vi har frågor men ser gärna att vi pratar om allt möjligt.

Respondent B: Vi kör på.

Jocke: Ja, men då börjar vi väl att frågar första frågan då.

Björn: Vi kan börja presentera oss.

Jocke: Ja vi kan presentera oss ja precis, Jocke Svanlund heter jag.

Björn: Björn Kronberg

Hampus: Hampus Jeppsson

Respondent B: Och vad har ni för bakgrund?

Björn: Vi är systemvetare, vi går ju nu sista biten det är bara kandidatuppsatsen vi håller på med nu.

Jocke: Skriver då om ämnet social engineering, åh vad var det nu titeln var på?

Björn: Vi bestämde “a study in awareness and measures”.

Respondent B: Okej.

Björn: Så vi är ute efter, är företag medvetna om vad social engineering är, vad hotet är, vad konsekvenserna kan vara och vad dom gör för att skydda sig,

Jocke: Perfekt då kör vi igång då. Du kan väl börja berätta lite om dig själv, din bakgrund i branschen, vad du gör här på företaget, dina arbetsuppgifter och lite sådant.

Respondent B: Min bakgrund är att jag har jobbat med IT i princip sen långt tillbaks och där har jag ju mer och mer glidit in på IT-säkerhet egentligen brett, så det handlar ju både om faktiskt, både om social engineering ända ner till kryptologi och hantera olika typer av kod, genomföra penetrationstester och riskanalyser. Titta på risker och försöka göra dom mätbara och omsätta dem i pengar, framförallt. Och sen hitta åtgärder som inte kostar mer än, en

åtgärd ska ju inte kosta mer än vad det kostar att skapa själva en produkt till exempel eller skapa en form av information då har man ju gjort en dålig affär, ni köper ju inte, ni ligger ju inte och betalar för dyra licenser på backup till programvaran av era maskiner där hemma, det skulle bli för dyrt, det är ett dåligt exempel kanske men ni förstår. så från att ha gått från många år tillbaks från att vara en Windows ad tekniker så har jag rullat igenom Linux träsket, nä jag ska inte säga träsk för jag älskar Linux, rullat igenom Linux världen och sen har jag hållit på med en del utveckling och hostat webbtjänster och jobbat i konsultbranschen för att sen landa här vilket är otroligt spännande och roligt, så där är min bakgrund.

Jocke: Vad är din utbildning?

Respondent B: Jag har ingen utbildning, jag har bara utbildat och då har jag utbildat i hela MCSC träsket höll jag på att säga, Windows bitarna, Microsofts, i flera olika spår, när det gäller serverhantering, SharePoint och webbutveckling, ingen utveckling då men mer, vad ska man säg, design av infrastruktur runt webtjänster och sen säkerhet kring det. I övrigt så är jag CISSP-certifierad och där ska du ju egentligen ha validerat dig att du har jobbat inom olika säkerhetsdomäner under 5 års tid tillbaks minst ska du kunna visa cv på från olika arbetsgivare. Så det är det, där har du min bakgrund och utbildning, och jag har kört mycket IT-säkerhet och informationssäkerhetsutbildningar på både KY och även rent mot företag.

Jocke: Då går vi vidare då, om vi säger begreppet social engineering, vad betyder det för dig? Vad är social engineering enligt dig?

Respondent B: Social manipulation är ju precis att du manipulerar någon att tro att du har goda avsikter och därmed så kan du ju lura dig till både information och lura dig till access in i system. och lura dig till, både avsiktligt och oavsiktligt få folk att göra saker som inte gynnar verksamheten.

Jocke: Precis, det stämmer väldigt väl överens med den uppfattningen vi har om det.

Björn: alltså är ni inom företaget medvetna om det eller känner du att det är med du som får ta den delen eller är alla i företaget medvetna om social engineering.

Respondent B: Vi bedriver security awareness training, vi försöker utbilda alla kontinuerligt inom IT-säkerhet och då går vi på dom klassiska fyra grejerna, konfidentiellt, integrity, availability och traceability. För att ha kontroller på detta så har vi även kontroller, en av kontrollerna är en förebyggande regulatorisk kontroll att du ser till att folk är medvetna och om risker att du inte ska sprida viss typ av information, eller berätta om t.ex. ett lösenord eller kanske öppna en viss typ av mail eller faktiskt också att bli lurad att starta applikationer eller exekverbar kod vilket också är en typ av social manipulation. Så vi har fortgående utbildningar hela tiden på det och minst en gång om året skall alla på företaget gå en sådan utbildning.

Björn: Har ni någon sorts kontroll att folk verkligen gör det, alltså går utbildningen?

Respondent B: Det är jag som sköter det och jag har kontroll. Jag har namnlistor och då jobbar jag ju nära HR, Personalavdelningen, för att följa upp den kontrollen. Så vi mäter, vi har KPI:er på också, vi sätter mätvärden; har vi lyckats med detta? nä bra, ny aktivitet på igen. Vilken avdelning har inte gått nu? Hur många procent har gått och sen så styr vi efter det.

Jocke: Ja nyckelvärden är viktigt. Om vi går vidare från utbildningen, policys osv, Hur ser det ut med det? Har ni mycket policys om hur de anställda arbetar för att?

Respondent B: Ja jag förstår. Vi har ju en policystruktur som är ganska strikt. Vi har en huvudpolicy, den är väldigt enkel, vi ska tjäna pengar. Higher management har satt den policyn, sen nästa steg under det finns det ju policys som skall leva på denna och där har vi ju då olika typer av policys som sedan mynna ut, vi kör ju konceptet policys, standard procedurers och principals kan man väl säg. Där man har policys högt upp sen neråt så har du principer, dom är inte lika hårda som policys men det kan ju vraa att du måste följa en viss princip. En princip kan vara mer föränderlig, alltså du ändrar ju den oftare än vad du gör med policys. Och sen har du standarder som t.ex. sätter din standard på vilken typ av antivirusprogram, vissa beteenden är standardiserade och vissa flöden är standardiserade. Vad sa jag nu? policy, princip, standard och sen har vi en till vad är det nu vi kallar den för. Ja i princip, så det är ett ganska standardiserat sätt att ha sina policys, vi har ganska mycket policys, de policys som gäller social engineering försöker vi har väldigt kortfattade och begripliga för annars blir det ett brus av information som slutanvändaren inte kan ta åt sig och då kommer det bli för mycket att hålla reda på om vi skulle t.ex. sätta en viss typ av mig mail får man absolut inte öppna, vissa får man kanske öppna, vissa måste man rapportera in. Då sitter du och håller på med mailboxen på ett felaktigt sätt. Den policyn kan ju vara så att vi har en princip som berättar att vi har antivirus eller anti malware, antispamkontroll som hjälper oss att inte få in skitmailen som dom inte skall öppna osv. Så att vi försöker hitta kontroller på alla olika plan för att minska den onödiga arbetsbördan för slutanvändaren. Var det svar på frågan? det blev ett långt svar.

Björn: det var svar på frågan. Det är någon sorts konvention av tekniska och formella och informella också?

Respondent B: Ja absolut.

Jocke: Dom här policyn, var finns dom att hitta? Har ni någon site som dom anställda kan gå in på? Eller sitter dom uppe på väggen någonstans? Eller skrivs dom ut och ges till dom eller var läser dom?

Respondent B: Dom sitter på en anslagstavla i pappersform nere på gågatan i landskrona?

Jocke: Mm, okej.

Respondent B: Nej det gör dom inte jag skojar med dig. Om vi säger såhär, all information är klassad och all information har en ägare, och information kan vara i lite olika skede, de kan vara konfidentiellt, det kan vara internt det innebär att alla får se det men inte sprida det eller så kan det vara så att det är publikt, det får inte ändras men det får lov att synas. Detta är inte publikt och det är inte helt konfidentiellt för alla ska ha tillgång till just dessa policys. Så dom finns på vårt, dom finns tillgängligt där folk söker och hämtar information.

Jocke: Skulle du vilja specificera lite mer hur ni jobbar med tekniska lösningar för att motverka social engineering eller social manipulation? Om ni arbetar med tekniska lösningar?

Respondent B: I min värld så kan man ha jättefräsiga security scanners och malware detectors och du kan ha penetrationsverktyg som pen-testar och ofta så kan man köpa dessa automatiska kontroller som går ut och scannar igenom nätet och dom är jätte fina och dom berättar precis vilka patchar du har missat och dom berättar att du har zero day threats i dina nätverk och du har allt möjligt. Men dom är byggda som robotar, vad dom skyddar dig emot är andra robotar som försöker ta sig in, lite grann en robot skyddar en robot. Men det är väldigt svårt att sätta en teknisk lösning som skyddar dig emot social engineering, en duktig människa på social engineering vet hur han ska lura sig förbi ett sådant system. Så vi har kontroller som är accepterade. visst man kan ju bygga jättestora dyra grejer, som data leakage protection t.ex. Det kan bli jättedyrt och det tar 2 år att implementera och kostnaden för det kosta mer än om skiten läckte ut. Därför när det gäller just social engineering med att folk ska lura sig in så handlar det om en medvetenhet ute hos slutanvändaren. När det gäller social engineering i form av att man försöker lura in exekverbar kod eller kanske få in mail eller någonting annat, då försöker vi ju ha kontroll på det med klassiska hjälpmedel som antivirus, anti maleware, antivirus botar i brandväggar finns också nu för tiden och, där du helt enkelt tittar på signaturer. Men eftersom ni också är i ämnet så vet ni ju också hur värt det är att titta på de här signaturerna. Det är väldigt lätt att skapa och gömma kod. Det finns gratisverktyg där du kan gå in och på bara ett par knapptryck så scramblar du den exekverbara koden så att den får en annan signatur, sen kan vem som helst exekvera den för antivirus hittar den inte. Och har du själv klickat på den har du själv godkänt en installation där du kanske till och med tar dig förbi någon sort säkerhetskontroll. Därför är det väldigt viktigt att vi hela tiden försöker hjälpa slutanvändaren här i organisationen att ha en medvetenhet.

Björn: Om en utsatt skulle bli utsatt för social engineering, har ni nått sort regelverk för vad den personen skall göra då, om den misstänker någonting?

Respondent B: Vi har dokumenterat hur du skall hantera vissa saker, det är sådant som, hur gör jag när jag har blivit av med min telefon eller dator, då finns det ju åtgärder för hur man hanterar det. Och även om någon misstänker att dom har blivit lurade eller om vi misstänker det, så är vi väldigt strikta med att ha en no blame culture här inne så att folk inte ska känna sig påhoppade om dom har blivit lurade. Tvärt om, dom ska känna att det är riktigt nice att gå till it avdelningen, vi håller dom om axlarna och trycker dom mot vårt bröst och tycker synd om dom. Vi lägger inte saker i bly, vi lägger dem i bomull, på det sättet skyddar vi om dom

faller. Lägger vi de i bly så pang, då kan ingen jobba. Vi försöker hjälpa individen, individen här är en asset, assets ska skyddas av organisationen. Alltså skyddar vi även individen och även försöker skydda dom hemma genom att göra dom medvetna om vilka risker dom kan bli utsatta för, och då är det även vårt ansvar att hjälpa till. Och detta speglar sig hela vägen in i organisationen så vi hjälper folk om dem blir utsatta för något så ska dom alltid känna att dom har hjälp. Rapportera in så fort dom bara kan, vi har vid vissa tillfällen till och med delat ut godispåsar när folk har kommit och bett om hjälp, bara såhär ploj-aktigt "rapportera det ni har så får ni en godispåse", alltså det är ju ett skämt men folk förstår budskapet med det, och det funkar jättebra! För ett tag sen hade vi stora lösenordsbytardagen, det är ett tag sen, den som har äldst lösenord får ett jumbopris, och folk kom och fick godis och någon fick jumbopris. Men vi fick bytt alla lösenorden istället för att alla "Jag pallar inte gå dit och få en utskällning", och det funka jättebra!

Jocke: Hur känner du att du bli bemött i ditt arbete när du kommer och vill öka säkerheten?

Respondent B: Det är såhär, jag måste vara duktig på social engineering, och med dom skills:en har jag inga problem att ta mig förbi dom sakerna i heller. Och det gör jag ju utan att luras men det handlar ju om att få någon att förstå på ett bra sätt. Som du säger social engineering, han lurar sig in han kan få folk att tro och förstå. Mitt jobb är att tro och förstå bara det att det faktiskt ligger en sanning bakom och att jag kan i efterhand ta upp ett papper och visa att det är såhär. Gör man på det sättet så är det inga problem att få igenom nått som är bra. Man måste alltid ha med sig 3 saker om man vill ha igenom nått, det är konsekvens, orsak och åtgärd. Konsekvensen kostar pengar, orsaken kanske inte kostar pengar för orsaken kan ju vara en bagatell eller något riktigt allvarligt, men sen åtgärden kostar också pengar. Sen har du ju vad skulle det kosta om risken exekveras, vad kostar det företaget? Då kan man ju räkna på dom här klassiska sätten i 3 steg. Sannolikhet att nått händer en 1a, det kan hända om ett år, en 2a det händer inom en månad, en 3a det händer imorgon eller har redan hänt och inte är åtgärdat. Där har vi sannolikheten. Konsekvensen det är ju, 1 är en jävligt jobbig dag på jobbet med spring i korridoren och folk skriker och arga chefer, en 2a och vi kanske till och med behöver betala vite till kunden för att vi inte har levererat det vi behöver, en 3a och kunden lämnar company B. Tar man då dom här väldigt enkla värdena sen kan du skala dom mycket mer. Har du någonting som kan hända imorgon eller har hänt utan åtgärd och om det är så illa att så att om det gör det så lämnar kunden company B, då har vi 3*3 det är en 9a, alla 9or ska åtgärdas. Kan jag få folk att förstå dom räkne exemplen, den matrisen på enkelt sätt och just det här matteexemplet är så enkelt mellan 1-3. Sen hur vi räknar i bakgrunden att vi kanske har skalat upp det ännu mer när vi gör riktiga riskanalyser, det behöver vi inte kanske berätta, men när vi har jätte jätte många frågor och det är en ledningsgrupp som skall sitta och lyssna på det också berättar man, tar man dom absolut värsta grejerna och tittar på det också kanske lite också såhär falling leaf, vilka grejer som vi kan bara fixa sådär utan att det kostar nått. Då har man ju samlat ihop riskerna, man presenterar dom på ett korrekt sätt och man får en acceptans om att gå vidare. Väldigt väldigt ofta är det en acceptans om man förklarar på rätt sätt.

Björn: Så ni jobbar med riskanalyser, threat metrics typ?

Respondent B: Ja.

Björn: Känner ni att ni har skapat någon sorts hotbild mot ert företag, är det någonting ni har jobbat med? Generella hot lixom?

Jocke: Var attackerna kan kommer ifrån och vad ni borde akta er för?

Respondent B: Ja.

Jocke: Är det något ni har arbetat mycket med är det något ni känner har varit värt att arbeta med?

Respondent B: Vissa saker är självklara, andra saker har vi fått jobba mer med och man förstår och det finns jätte många olika faktorer som det handlar ju dels om, typ konkurrens, missnöje, geopolitiska grejer, alla dom klassiska sakerna, när dom börjar göra riskanalyser tittar dom på hur allting ser ut, nära och långt bort och runt om dig och vilken verksamhet som bedrivs i en organisation. Man får sätta sig och workshoppa det här, så du gör det ju inte bara genom att knäppa med fingrarna utan du måste ju sätta dig ner och titta vad är faktiska risken och vem gynnas av att förstöra nånting för oss eller vem gynnas av att få ta del av det vi kan leverera. Tittar man bara snabbt så kan alla säkert fundera ut att det sitter fem snubbar liksom, tre fattiga studenter som går nått IT-program och vill tjäna pengar på att hacka oss för dom ska utpressa oss, ja det är en risk. Men det finns andra typer av hot också som är mycket mer komplicerade att förstå, och dom måste vi hitta. Och vi tittar så mycket som vi har möjlighet till på den typen av risker.

Björn: Upplever du att hotbilden mot ert företag är större nu än när du började jobba här?

Respondent B: Jag har inte jobbat här jättelänge, jag har varit anställt inte så länge. Jag har varit konsult här innan så vi har gått i omgångar. Men under den tiden som jag har varit här ungefär samma. Sen jag börja med IT-säkerhet har det gått upp och ner. Det som händer ute i världen påverkar väldigt mycket det finns sina konflikter här i världen på olika håll som påverkar. Men för fem år sen var det lite annorlunda konflikter och det var nästan lika mycket aktivitet då. För tio år sedan så var det, då fanns det bursts med attacker, och då visste ju inte folk och då fanns det ju sämre skydd dessutom. Så då behövde man ju inte köra social engineering då gick du ju in på security focus, ladda hem lite Linux kod, skicka det via nått ftp-kommando liksom bara i någon, till någon (*ohörbart ord*) FTP-server, pang så var du rakt inne i den och börja köra kommando. Och webbhotell som var tväröppna. Så folk har blitt mer aware nu så risken ser annorlunda ut. Jag tror det ökar, men samtidigt så ökar medvetenheten. Medvetenheten och tekniken hänger inte riktigt lika mycket med, så du har ju mer jobb nu, men mitt jobb e, jag kan ju faktiskt inte jobba mer än åtta timmar om dagen.

Björn: Har ni någon statistik över sociala och tekniska attacker?

Respondent B: Vi försöker så gott vi kan mäta sådana grejer, för det är det som vi har som underlag för vilken typ av skydd, och vilka typer av aktiviteter vi ska göra längre fram för att skapa rätt typ av kontroller och när jag pratar om kontroller så menar jag ju en policy är ju en typ av en kontroll, jag vet inte hur ni tänker där. Men kort sagt, ja vi försöker mäta det.

Björn: Tycker du att det är svårt med social engineering för då kanske man inte vet om det har hänt eller ej?

Respondent B: Precis det är svårt, otroligt intressant.

Björn: är det något ni funderar på hur man skulle kunna göra det bättre eller?

Respondent B: ja det gör vi ju alltid, alltid när vi gör någon större aktivitet så avslutas den aktiviteten med att titta på hur kan vi, alltså det finns ju en återkoppling där vi ser, hur känner vi att vi har lyckats, och det är litegrann det här med KPI:er, så att vi kan hitta rätt. Gjorde vi rätt här? Så det är ju dagligt jobb på en IT-avdelning att förbättra och jag sitter ju någonstans ganska nära IT-avdelningen eftersom jag jobbar med informationssäkerhet.

Jocke: Vi har läst en del om från Kevin Mitnick, och han talar varmt om audits, som dom har börjat med ganska mycket nu där man utför simulerade attacker mot sitt eget företag, bara för att testa, är det något ni har arbetat med? Eller är det något ni har tittat på? Om inte, varför?

Respondent B: Det har vi tittat på, vi gör det, vi gör det med mellanrum.

Björn: Hur upplever dom anställda det här?

Respondent B: Det kan kännas påträngande.

Björn: Har ni fått någon sorts kritik för det här?

Respondent B: inte när vi har förklarat syftet och av vad vi fick ut av det, då har det varit en positiv reaktion.

Jocke: Den påträngande känsla du prata om, den behöver inte bara vara negativ i heller, Jag kan tänka mig att det är bra att dom anställda har en liten "store bror ser mig känsla" i bakhuvudet, att det kan ske ett test när som helst.

Respondent B: Det är inte hela syftet, men en liten del av syftet är att skapa awarenes och att dom ska vara på hugget. Jag själv har t.ex. gick runt ett block i handen också hade jag en penna, också gick jag förbi någon, alla vet jag jobbar med så jag bara " vad har du för lösenord?". Och tror du jag fick det eller inte?

Jocke: Jag hoppas inte du fick det.

Respondent B: Vid ett tillfälle fick jag det, och vad jag sa då var "bra, du går genast ner och byter det", sen gick jag och han skratta. Men han lär aldrig göra om det, vi skrattade åt dem så de löste sig. men så enkla former mäter vi inte ens, det var bara jag som sprang och fick djävulshorn en dag.

Jocke: Men det är lite annorlunda sätt att skapa awarenes på och det måste man göra. Vad gör ni mer för att skapa awareness? Posters t.ex.?

Respondent B: Jag har använt posters på tidigare jobb, och jag kommer göra det. Det finns fräcka verktyg att använda för att skapa snygga posters.

Hampus: Känner du av kampen mellan seamless access och att allt skall vara säkert?

Respondent B: Jag är väldigt mycket för att information skall vara öppen om det är rätt typ av information så klart för vissa grejer kan ju skada människor. Och jag försöker ha den mentaliteten när jag går in och tittar på hur det fungerar i denna organisation, folk ska ha lätt för att jobba, och då kommer det här med availability, availability är att det fungerar och det fungerar inte när man har för hårda kontroller. Och det är där man skall hitta balansen, kommer den här kontrollen att hämma verksamheten? Eller kanske det är värt att ett visst system inte fungerar under en viss period för att folk kan i alla fall jobba jättemycket dom andra tiderna på året, och den balansen är jättesvår att hålla. Men ja det är en kamp, men jag har mer kampen inne i mitt eget huvud än vad jag har utåt mot organisationen.

Björn: Är det någon skillnad att få ledningen att skydda sig mot mjuka respektive tekniska hot?

Respondent B: Hoten är av olika karaktär oavsett om dem är mjuka eller hårda. Samma grej igen, kan jag presentera det på rätt sätt och relevansen, och det kan jag bara om jag kan en sak och det är om jag kan organisationen, då kan jag hitta relevansen och förklara varför vi bör göra det, också kan jag skriva ett business-case, och det är ett lätt fattat underlag där en högre ledning kan ta ett beslut, Kör! Det är nog det enda svar jag kan ge där.

Björn: Du nämnde det här CISSP, såg jag att det fanns på PCIDSS, det var en intressant del med det, det är att bara den sista av dom som dom listar där att du skulle följa i den standarden var av mjuk karaktär, det var policys. Sen alla dom andra var väldigt tekniska, och även OWASP, där är alla tekniska. Upplever du att det är någon sorts dissonans mellan vad hoten kan vara från social engineering och vad dom här påstår att det är.

Respondent B: Hela CISSP-konceptet är gjort av en organisation som heter ICS-2. Dom har funnits rätt länge och det är en stor oljetanker som är svår att vända som man brukar säga. Det är inte så många år sen dom höjde upp hela security awareness grejen mer, men sen ka du skriva om alla certifieringar och alla dom här domänerna som du ska kunna och det gör du inte i en handvändning. Hela det här med policys, är ju såhär följ dom här så kommer du fixa

allting, går du utanför dom så är du redan ute och tassar på fel ställen. Men ja, dom borde ha mer security awareness, absolut det skulle varit mer med det scopet.

Björn: Tror du att det kan vara för att det är svårare med social engineering än mer såhär tekniska grejer? Att det kan vara mycket svårare att skydda sig mot det?

Respondent B: Nej jag tror inte det handlar om det, jag tror det handlar om att det bara inte har behövts just för dom människorna som har varit målgrupp för den certifieringen, så mycket. Social engineering, är det en IT-fråga?

Björn: Vi tror absolut det.

Respondent B: Nej men frågan är om det inte är en informationsfråga, inte IT. Teknologin skyddar dig mot vissa exekverbara hot där du kan lura in filerna, men har någon lurat in filen, är det it eller är det någon annan som ska skydda mot dom här exekverbara filerna. Om du har rollbaserade rättigheter på rätt sätt i din organisation då kan du inte exekvera dom för då har du inte rättigheterna till det. Jag håller me jag skulle också vilja ha det på en IT-fråga, men en normal IT-avdelning där man har skurit ner på kostnader, det ryker några projektledare också sitter teknikerna kvar och dom teknikerna är tekniker.

Jocke: Vem äger risken, är det IT?

Respondent B: Jag säger såhär, det finns en informationsägare, informationsägaren äger informationen, äger klassningen av informationen, sätter bäst före datum på informationen, och ska delges risken om vad som händer om informationen blir kompromissad eller läcker ut eller blir förändrad eller vad som än händer. Och då bli det informationsägaren som i slutändan också ska förstå risken. IT bör vara en supportorganisation som hjälper resten av företaget. Alltså man beställer till it, vi vill ha en ny webservice, okej då kan vi bygga den i PHP vi lägger den på en sådan fräsig server, vi gör det här, tänk på att dom här riskerna finns, ska vi lägga såhär mycket pengar? Eller såhär mycket pengar? på att hantera detta. Lägger vi såhär mycket pengar, lite pengar så kan vi skapa koden och det blir en billig utvecklare som gör det. Han har ingen aning om OWASP. Vi kommer inte ha råd att penetrationstesta det eller göra en kodanalys osv. Om du har såhär dyr utveckling så kan du få in alla dom här bitarna, och vi får life cycle management och vi får kontroller och hela kittet men då blir det såhär dyrt. Då får ju den som äger den här webservicen också vara den som tar risken, vad har vi för budget på den här webservicen. Är det bara en kampanjsida, fine det kan läcka ut, den ligger på en Word press site ute på surftown och vi ska släcka den om en månad, men det kanske är en webservice där man kan komma åt information internt, koppla till databaser osv på nått sätt blir det en annan femma. Och då blir det ju, informationsägaren är den som äger risken och får hjälp av någon som är säkerhetschef, säkerhetschefen bör sen delegera till olika typer av säkerhet, om det är en HR-säkerhet eller en IT-fråga, så hoppas jag att det ska se ut på många ställen.

Björn: Vi har egentligen en stor fin fråga kvar, om du hade haft obegränsat med resurser, för det är ju alltid en pengafråga. Vad hade du velat göra extra skydd mässigt?

Respondent B: Då hade jag fullständigt öppnat allting, alla brandväggar och allting. Också hade jag stängt ner bara precis det som behövs. Så jag hade inte lagt skyddad som ett perimeterskydd med brandväggar och layerd security och allt möjligt, utan jag hade försökt ta mig så nära kärnan som möjligt, och skydda det lilla som ska skyddas med principle of least privilege, och separational of duties och alla sådana fräcka termer som man kan tänka sig. Allt annat skulle vara öppet och enkelt att hantera, och sen hade jag såklart tagit väldigt mycket tid och resurser på att få folk att förstå hotet med social engineering, få folk att skydda sin verksamhet och ta ansvar, och känna sig delaktiga.

Jocke: vill du berätta mer hur det tekniska ser ut? En av våra andra intervjurespondenter berättade att dom använde TPM-chip på sina datorer så det var trusted platform module där, vissa har haft inloggning, nyckelkort, sessionsbaserat. Det har sett lite olika ut och det är helt okej om du inte vill berätta.

Respondent B: Vi krypterar hårddiskar på vissa nyckelpersoner, ja på dom flesta men det finns ju vissa som är strunt samma för dom har ingen viktig information på sin dator. Så vi har krypterade diskar och vi har tvåfaktors (*obegripligt ord*), där det behövs. Och även till konsulter som skall in i känsliga system behöver två faktorer för att få tillgång. Så skyddar vi oss.

Jocke: Hur ser det ut när ni anlitar konsulter och extern personal, med E-Learning och utbildning? Är det nått dom ska göra? Kolla policys?

Respondent B: Vi går igenom de policys som är relevanta för den konsulten, need to know basis. Vi vill inte ha ut alla policys för vi vill inte berätta för alla hur vi gör och vilken typ av skydd vi har, och det är bättre lämnat. Sådan information som en konfidentiellt intern. Så dom får vad dom behöver också får dom skriva på sekretessavtal, och i vissa fall beroende på var dom ska in så göra vi även en poliskontroll, det gör i så fall säkerhetschefen, jag är inte säkerhetschef, jag jobbar bara parallellt med honom.

Appendix 5

Jocke: Då kör vi igång. Vill du börja med att berätta lite om dig själv?

Respondent C: Jag är IT-ansvarig för company C Sverige och man hanterar allting inom IT-säkerhet. Infrastruktur ska upprätthållas. Jag gör ingen support men jag ser till att vår IT-infrastruktur fungerar. Utöver detta är jag med i den Europeiska IT-organisationen. Vi gör mycket IT-projekt, både på regional & global nivå. Jag är certifierad projektledare, PMI/PMP. Jag är även IT-säkerhetsansvarig i Sverige. Vi har i vårat företag en IT-säkerhetsorganisation.

--- *Visar deras interna hemsida på datorn* ---

Här ser ni vår site. Här finns mycket policys, standards. Vi gör regelbundet användarna medvetna via kommunikation via mail och/eller muntligt. Vi har även årliga kampanjer gällande IT-säkerhet. Varje september är en IT-säkerhetsmånad.

Björn: Vad innebär den månaden mer specifikt?

Respondent C: Det innebär att vi dels skickar ut s.k. bulk-mail till samtliga. Vi sätter upp posters och vi har ett specifikt tema var år. Jag kan visa er ett exempel om ni vill?

--- *Visar information/bilder från IT-säkerhetsmånaden 2014* ---

Respondent C: Varje vecka skickar vi då ut ett mail och vi printar ut posters. Vi kan titta på postern för v.1 här. Här ser ni själva rubrikerna: Getting Physical, Securing your workspace, Security Post, See something - Say something (rapportera incidenter). Här ser ni då ett exempel på hur de kan se ut.

Björn: Är detta något ni skriver ut och sätter upp på arbetsplatsen då eller?

Respondent C: Precis. Säkerhetsorganisationen är lokaliserad i USA och där har vi de flesta anställda som ingår i den organisationen. Sedan, över resten av världen, har vi s.k. IT-säkerhets officierar. De är då ansvariga på respektive site och får då i uppdrag att kommunicera detta vidare, att printa ut och sätta upp posters på anslagstavlor. Dessutom brukar jag alltid ta upp detta på våra stormöten.

Jocke: Och det är då för att skapa awareness?

Respondent C: Exakt! Och det hjälper definitivt och är viktigt, något man måste jobba med ständigt. Alla vill ju ha seamless access och total frihet. Säkerheten ska vara någonstans runt omkring. Informationen ska vara säker men helst ska den anställda själv inte märka av det.

Björn: Dessa säkerhetsmånader ni har. Den informationen ni erbjuder där, är det ett krav att de anställda ska ta del av den? Gör ni någon sorts uppföljning?

Respondent C: Nej, det har vi väl egentligen inte. Vi har inget signeringssystem om vi säger så.

Jocke: Nu utgår vi från att vi gruppmedlemmar inte har någon koll på vad social engineering är för något. Vi vill då att du förklarar social engineering för oss, så som du ser på saken?

Respondent C: Social engineering är ett sätt att få information genom ett enkelt samtal. Vi är ganska vänliga av oss som människor och man kan få ut oerhört mycket information genom enkel kommunikation. Man ger ifrån sig information som man inte är medveten om. Ett vanligt samtal ger oerhört mycket. Dessutom är de vänliga, trevliga & inställsamma. Det kan räcka med en enkel telefonlista där man frågar något i förbigående. Man lämnar något namn för att skapa en förtroendekänsla eller något liknande. "Känner du henne/honom?". Sen är det väldigt lätt att gå vidare därifrån, när man väl har lite information att arbeta med. Igenkänningsfaktorn! Sedan är ju social engineering även regler etc. för hur man ska arbeta, vilken information som bör skyddas, vad man får sätta på anslagstavlan etc.

Jocke: Perfekt. Nu har vi pratat lite om de formella & informella delarna av ert Social Engineering skydd. Har ni, förutom policys, någon sorts internutbildning inom ämnet?

Respondent C: Som nyanställd får man alltid en introduktionsutbildning och där ingår även IT-säkerhet. Det är en grundutbildning. Där finns inte jättemycket om just social engineering men vi berör ändå ämnet. Den utbildningen ska alla nyanställda gå. Sedan är det kontinuerlig utbildning. IT-organisationen skickar ut nyhetsbrev med olika ämnen för den månaden, lite statistik på laptop-stölder och annat. "Man ska hålla utkik".

Hampus: Är det något som händer ofta? (läs laptopstöld)

Respondent C: Det händer lite då och då, definitivt. Vi kan se om jag inte har lite statistik på det

--- Tittar på nyhetsbrevet ---

Respondent C: Här kan komma alla möjliga ämnen. Någon säkerhetslucka eller något annat som är aktuellt, t.ex. tidningsrubriker eller Facebook. Då brukar man diskutera det i nyhetsbrevet och säga hur man bör agera. Någon statistik fanns här dock inte, det var jag som mindes fel. Det är ett antal sådana stölder per år dock. Det är ju ett stort företag med nästan 70 000 anställda så det är klart att det blir ett par hundra stölder per år. Tack vare detta ska

alla laptops vara krypterade. Det kravet finns inte med stationära PCs men alla laptops ska vara krypterade

Björn: Hårddiskarna då?

Respondent C: Exakt!

Jocke: Vad använder ni för kryptering då?

Respondent C: MacAfee.

Björn: Nu pratar vi en del om tekniska åtgärder. Vad har ni för andra tekniska åtgärder för att motverka social manipulation?

Respondent C: Brandväggar till att börja med. Man försöker göra det i olika skal, som en lök. Inte bara ett skydd vid internetgatewayen utan man måste skydda alla lager. På datornivå har vi ju sedan programvara som skyddar, såsom virusskydd, personlig brandvägg och kryptering.

Björn: Tailgating är något vi har hört/sett mycket av. Har ni några åtgärder för att motverka detta?

Respondent C: Ja, det har vi, en policy. På just denna anläggning har vi ju ingen reception utan här är det den som är värd till gästen som ansvarar för gästen personligen. Är det någon snickare eller målare så får de alltid en liten visitor-badge och så skrivs de in. Ska de vara här och arbeta under en längre tid och självständigt så får de en säkerhetsutbildning. Då är det inte IT-säkerhet specifikt utan mer generellt, d.v.s. hur man ska agera om brandlarmet går, att man inte får lägga sladdar på golvet, att man ska hålla i räcket när man går i trappan. Ja, ni förstår vad jag menar.

Björn: Du pratade om seamless access innan. Upplever du balansgången mellan seamless access VS säker information som ett stort problem?

Respondent C: Det kommer ju lite klagomål ibland när personer behöver logga in ett antal gånger bara för att kunna börja arbeta till exempel. Det går aldrig att komma ifrån. Men, i det stora hela är det inga problem. De flesta förstår varför vi gör detta och accepterar det. Däremot ses vår IT-organisation ibland som ett hinder för den anställdas produktivitet och vi anses vara tråkiga som bara skriver massa policys som vi måste följa.

Jocke: Det har vi hört även från andra håll, att IT-säkerhets avdelning ofta ses som bakåtsträvande och lite tråkiga.

Respondent C: Ja, och det stämmer väl till viss del. Men i det stora hela är det inget problem tycker jag.

Jocke: Om vi skiftar fokus från de andra anställdas acceptans och fokuserar mer på ledningen; hur känner du där? Har du stöd och förståelse från ledningen i ditt arbete?

Respondent C: Ja, definitivt. Det gör de.

Jocke: Har ni arbetat något med att försöka fastställa hotbilden mot ert företag?

Respondent C: Det är inget jag själv är inblandad i faktiskt men jag vet att vår IT-säkerhets organisation arbetar med det ständigt och kontinuerligt. De är väldigt på alerten. När det kommer nya virushot vet vi ofta det innan FBI vet om det ens.

Björn: Arbetar ni med riskanalys/threat metrics?

Respondent C: Ja, det gör vi. Vi har mallar för detta beroende på vad det är för något.

Björn: Är det mallar ni själva utvecklat?

Respondent C: Nej, även de kommer från vår IT-säkerhets organisation. När det gäller IT-säkerhet har vi en modell för det. Är det någon annan business så finns det en annan mall. Man skriver ner alla hot man kan komma på och sedan får man klassificera de.

Jocke: För ni någon statistik över antal attacker? KPI/Nyckeltal?

v: Ja, det förs statistik. Är det någon som drabbar dig själv så ska man göra en s.k. incidentrapportering och den statistiken samlas in.

Björn: Upplever du att det är svårare att använda sig av statistik vid sociala attacker gentemot tekniska attacker?

Respondent C: Dels får man tänka att alla ska rapportera in, vilket inte direkt görs. Däremot vet man att vi har haft s.k. white hat campaigns. Då har vi skickat ut fejkade mail som säger att "Du har ett paket att skåda. Följ paketets väg via länken."! På länken fanns då malicious software. Och, ungefär 20 % av de anställda klickade på länken. Men det har blivit bättre och jag tror att sådana kampanjer hjälper.

Hampus: Gör ni detta med fysiska attacker också?

Respondent C: Det kan jag faktiskt inte svara på!

Jocke: Okej. För, det var lite nästa fråga vi skulle komma till; Om ni arbetar med s.k. Audits, där man utsätter sin egen personal för en testattack för att öka deras medvetenhet. Men, det låter som det är något ni jobbar med

Respondent C: Ja, det stämmer!

Björn: Den andra sidan av myntet är då integritetsfrågan. När de anställda som utsätts för en simulerad attack får reda på att det var företaget som utförde attacken; möts ni av dåliga reaktioner?

Respondent C: Nej, det har jag inte direkt upplevt. Det tas emot ganska väl. De är mer glada över att det görs av oss, då det är ofarligt, och att de på så sätt får awareness. Sedan skickade vi också ut ett mail efteråt där vi förklarade vad vi gjorde och varför vi gjorde det. Så, min uppfattning är att det ses som en positiv sak.
Ibland så poppar det upp saker. En viss del av vår IT-verksamhet är outsourcad och ett av de företag vi har använt oss av då skickade mail för att samla in fakta om våra PC och våra laptops. Då var det många som upplevde detta som något skumt och kontaktade oss. Vi skötte detta ganska dåligt då vi borde informerat personalen bättre innan men, det fick ju en positiv konsekvens då vi såg att personalen faktiskt har social engineering awareness.

Björn: De externa konsulter ni använder er av, får de någon utbildning inom ämnet?

Respondent C: Det beror på. Ska de vara på själva företaget så kommer de behöva göra den vanliga fysiska säkerhetsutbildningen. Den måste alla ha. Ungefär en timmes genomgång. Sedan, när det gäller att ge konsulter acess till vårt system så måste det berörda företaget skriva under ett "Non-disclosure agreement", d.v.s. ett konfidentiellsavtal. Först därefter kan vi ge access och då får de ett konto till respektive system. Då förbinder de sig också att ha sin laptop krypterad, förberedd med rätt antivirusprogram osv. Men nej, de behöver inte gå någon regelrätt social engineering E-Learning.

Jocke: Om vi går tillbaka ett steg och pratar lite mer om era åtgärder, specifikt de tekniska åtgärderna: hur ser inloggningsfunktionaliteten ut för era anställda?

Respondent C: Vi har självklart en lösenordspolicy. Utöver det har vi certifikat. De sitter på en liten USB-sticka. Med hjälp av det mjuka certifikatet får du då access till våra system.

Jocke: Okej, så det är mer mjuk autentisering? Inga taggar eller nycklar eller magnetkort eller liknande?

Respondent C: Vi hade tidigare små dosor men det har vi gått ifrån nu. Nu måste man ha två-faktor autentisering, alltså att du ska ha något och du ska veta något för att kunna få access.

Björn: Hur kommer det sig att ni bytt system?

Respondent C: Vi gjorde en del andra större förändringar i företaget när det gäller mail-system och för att kunna upprätthålla säkerheten var vi tvungen att uppgradera oss. Den gamla lösningen hängde inte riktigt med helt enkelt. Man måste hela tiden anpassa sig till nya system.

Jocke: Jag antar att er data/information innehar olika klassificeringar? Har ni någon övervakning på konfidentiell information, d.v.s. att du får en notifikation av något slag när någon begär tillgång till skyddad data?

Respondent C: I de flesta fall har vi ingen övervakning utan har du access till filen kan du omärkt hämta ut informationen. Vi ger access enligt need-to-know basis. Sedan har vi, som du sa, olika klassificeringar på vår information. Public, internal, confidential & strictly confidential. Vi har s.k. secure vault servrar när det är riktiga företagshemligheter, d.v.s. strictly confidential.
Där finns det dessutom övervakning. Men inte på de andra klasserna. Det finns inte möjlighet för oss att ha mer övervakning, det hade tagit alldeles för mycket diskutrymme.

Jocke: Arbetar ni något med risk ägande? Vem äger risken? IT-avdelningen? Ledningen? Han som skrev informationen?

Respondent C: All data har en ägare. Har datan inte någon ägare så ska datan slängas, det är en policy vi har. Den som är ägare till datan är ansvarig för att upprätthålla säkerheten.

Jocke: Ligger det ansvaret på individnivå eller är det snarare arbetsrollerna som äger ansvaret?

Respondent C: Det är personerna i sig som äger risken.

Björn: Upplever du att antalet attacker mot företag har ökat eller minskat sedan du började arbeta för företaget?

Respondent C: Jag har inte riktigt tillgång till statistik över direkta intrång så, det är svårt att svara på. Det förs statistik över det men det är inte direkt något jag tittar på så ofta.
Jag ser ju statistik på spam och för ett par år sedan var det ett jätteproblem. Det steg hela tiden, explosionsartat. Men, det har klingat av, vilket är ganska märkligt. Vi förstod inte riktigt varför men det minskade definitivt. Sedan har vi såklart anti-spam filter som sorterar, kollar och tvättar mailen.

Jocke: Så, antalet attacker går lite upp och ner snarare än i en tydlig vinkel?

Respondent C: Exakt!

Björn: Då återstår vår favoritfråga då. Om du hade fått ett betydande tillskott i din budget detta år; vad är det första du hade lagt pengarna på? Var är behovet störst?

Respondent C: Jag tror inte riktigt att jag kan ge ett bra svar på den frågan i och med att jag inte jobbar aktivt i vår IT-säkerhetsorganisation.

Men, om vi bara utgår ifrån vårt behov här i Malmö så hade jag nog satsat på bättre utbildning och mer kontinuerlig utbildning.

Jocke: Du anser alltså att det snarare är de mjuka delarna än de hårda delarna som kan utvecklas ännu mer?

Respondent C: Definitivt. Det är väldigt viktigt att ha awareness och det kan vi bara få via information & utbildning. Hittar man ett USB-minne på parkeringen ska man inte stoppa in det i sin arbetsdator och det måste alla förstå utan att vi står och pekar med fingret hela tiden.

Jocke: Precis det du pratar om, med USB-stickor, hade respondenten vi pratade med igår utfört som en audit; d.v.s. att han planterade USB-stickor på företagets parkering för att se vem som skulle koppla in de i sin dator. Och, de flesta gjorde faktiskt det. Eller nästan alla.

Respondent C: Där ser man. Ja, det med USB-stickor är en ganska vanlig grej. Jag tror dock inte att det hade fungerat lika väl här. Eller, det hoppas jag inte iallafall.

Björn: Har ni en specifik kontaktperson man ska kontakta när man misstänker att man kanske blir utsatt för en social attack?

Respondent C: Det finns det definitivt. Det finns en hotline som det bara är att ringa eller maila. Om man får misstänka mail kan man även vidarebefordra mailet till oss så undersöker vi brevet. Annars kan man alltid kontakta den lokala IT-ansvariga.

Björn: Ni har ju genomfört audits på företaget, t.ex. de white hat du pratade om förut. Hur tyckte du att det fungerade? Är det något du tycker företag i allmänhet bör göra?

Respondent C: Ett bestämt nja på den frågan. Ja, det tycker jag, men inte för ofta, definitivt inte varje år. Kanske vartannat år är en lagom frekvens.

Jocke: Vad är risken om man gör det för ofta?

Respondent C: Det blir ett störningsmoment hos personalen! Vi vill inte avvika för mycket/för ofta från deras dagliga verksamhet.

Björn: När man ser på säkerhets-guider såsom OWASP, CISP etc. Nästan alla hot de listar är tekniska och nästan inga är sociala. Kan det vara ett problem? Kan man vaggas in lite i en falsk säkerhet? För, om man följer dessa guides till punkt och pricka får man säkerligen ett väldigt bra skydd mot tekniska attacker. Men, en kedja är inte starkare än sin svagaste punkt och om man inte är skyddad mot social manipulation kvittar det lite hur bra tekniskt skydd man än har. Vad säger du?

Respondent C: Nej. Jag tror att när det gäller företagsspionerі är det oftast på teknisk väg, man hackar sig in i systemen. Företag som ligger i frontlinjen när det gäller IT-utrustning

och/eller vapenindustrin är extremt utsatta för sådant här. Det beror lite på vilken typ av företag det handlar om. Men även vi här är en läkemedelsfirma som är duktiga på många saker och det finns säkerligen folk som vill komma åt våra hemligheter.

Jocke: Vi är bara lite överraskande då den slutsats vi kommit till är att den bästa åtgärden mot Social Engineering är Awareness. Är det inte då märkligt att dessa sidor, som ska agera guide till hur man skyddar sig, knappt tar upp de sociala hoten? Vore inte det ett ypperligt tillfälle att skapa awareness redan på en tidig nivå? Vi har ju märkt att det finns en väldig medvetenhet ute hos de svenska företagen idag så, det är ju inget problem i sig men ändå.

Respondent C: Ja, det gör det. Men vill du ha mer kunskap om en produkt får du inte det av social engineering. Det är ofta något land eller någon organisation som försöker hacka sig in i systemet på tekniskt sätt. Oavsett hur duktig en social manipulatör än är så hade vår VD aldrig läckt företagshemligheter till honom då han vet att den datan aldrig ska delas till NÅGON annan. Någon på Saab kommer liksom aldrig att visa dig en ritning till deras gripen-plan. Så är det. Så, Social Engineering "will only get you so far" men om man vill åt de riktiga godsakerna är det tekniska medel som gäller. Därför står det mest om de i alla guider. Tror jag iallafall.

Jocke: De andra företagen vi har intervjuat har aktivt försökt skapa en lite storebror ser dig känsla, så att de anställda lite ska tänka på vad de gör på jobbet då chefen faktiskt har möjlighet att övervaka ditt arbete. Är det något ni har lite av här också?

Respondent C: Det är ju en medvetenhet det handlar om. De anställda ska vara medveten om att de inte är helt anonyma. Och det ligger lite på en need to know basis där också. Vi har möjlighet att övervaka våra anställda. Det betyder inte att vi gör det. Men de behöver inte de veta.