The Threat of Social Engineering and The Safety of Companies

Barbora Kotkova
Tomas Bata University in Zlín
Zlin, Czech Republic
b_kotkova@utb.cz

Martin Hromada
Tomas Bata University in Zlín
Zlin, Czech Republic
hromada@utb.cz

***Abstract*— Social engineering is a method of attack aimed at the state, organization, or individual. It focuses on the weakest point in the use of information and communication technologies, specifically the human factor. The article deals with the issue of social engineering with a focus on the attack and the possibilities of defense against it in a commercial and manufacturing company. Several questionnaire studies were conducted, which found that only a small number of staff had been trained in the past against similar attacks. Companies still underestimate their protection, investing in new technologies, but already investing less in training employees who use them. At the same time, social engineering largely focuses on them. The article, therefore, identifies social engineering, its ways of carrying out the attack. Furthermore, the article briefly summarizes its threats as well as its history, along with an overview of the first attacks. For greater orientation in practice, the individual types of attackers, the progress of their attacks, and the relevant technical aspects are described here. An analysis of the current state of safety in the existing manufacturing and trading company was performed, namely, the specific directives that are currently in force. These were compared with current needs and appropriate measures were proposed. Based on this analysis, recommendations for improving the state of security against social engineering attacks in all companies, in general, are described at the end of the article. The most frequently used methods in practice are listed according to the survey, followed by the establishment of safety recommendations. Individual technologies are constantly evolving, newer applications are being launched on the market, and at the same time, more advanced methods for data protection need to be developed.**

Keywords— attacks, defence, information, human factor, manipulation, security, social engineering.

I. INTRODUCTION

Today, information is already considered one of the most valuable assets in companies. It is a farm that is needed in all areas and sections of society. Starting with purchasing, stock, production, and all the other indispensable components that make up the whole, a functioning company. Information is also commonly traded. As an example, we can choose a consulting company that currently offers one of the relevant professional analyzes as an information processing service. The output of their activities is only information or an information system. With the help of a set of information today, as an individual or an organization, we can gain an advantage over the competition and thus secure a good position in the market. Every day, thousands of transactions take place in each company, during which information is exchanged, obtained, or provided. However, not all information can be shared this way. The misuse of sensitive information can have devastating consequences for society. Whether in the form of disclosure of technology, the composition of important components, or misuse for purposes for which they were not developed. If companies do not want to lose sensitive information, they must eliminate the risk of its misuse or at least minimize it. Today, many companies regularly, and not exceptionally as usual in the past, invest significant resources from their budgets in security. These include various types of software and physical security against intrusion and theft. The information is still leaking. One of the main reasons is still the human factor, which plays a very important role in security. Social security uses this security gap. Thus, the goal of an attack by social engineers is not always material good, but also very valuable information. These attacks are a very current problem today, and with the growing importance and price of information, they will become more and more important and necessary. The number of ways to get into the organization is increasing - for example, due to the Covid pandemic by allowing work from home. Many companies are still not sufficiently informed about these threats and do not place the necessary and sufficient emphasis on information security. They usually start solving this only after the successful implementation of this attack, when the cost of the necessary investment reaches high amounts.

Social engineering can be defined in several ways. Much literature and interesting articles have been written on the subject of social engineering. These include Hadnagy and Ekman's title Unmasking the social engineer: the human element of security, Gulati's book The Threat of Social Engineering and Your Defense Against It, and Allsopp's title - Unauthorized access: physical penetration testing for IT security teams. Hadnagy's titles will be used in this article. Influence the psychology of persuasion. Another interesting work would include Cialdini's Influence on the psychology of persuasion. Especially from the author Hadnagy and his titles will be further cited. The Institute of Sociology of the Czech Republic defines it as a social science discipline based on multidisciplinary scientific knowledge, with which it creates recommendations and a system of guidelines for practice to achieve change in a targeted way, for example in a group or individual behavior. In the field of information technology, however, the term social engineering is used for the style of psychologically led manipulation. Another definition is given by Hadnagy [1], which is: “The act of manipulating a person to a certain action, which may or may not be in his interest. It may involve obtaining information, access, or an activity. ”According to Watson, Mason, and Ackroyd [2], social engineering involves various ways of manipulating an individual to obtain certain information or perform an activity. These manipulations, therefore, focus on the often weakest link in the information system, which is a person. Attacks are usually conducted over the Internet or by telephone. To a lesser extent, social engineering methods are also used by other media, such as regular mail or personal contact. This article discusses attacks that are conducted using information

and communication technologies. They, therefore, present social engineering as manipulation of people, in order to obtain the necessary information. People who are manipulated are not aware of this and therefore there is a high risk of providing sensitive information. Therefore, for the purposes of this work, the definition of social engineering according to Watson, Mason, and Ackroyd [2] as various ways of manipulating an individual in order to obtain certain information or perform certain activity is decisive.

There are not many books in the Czech Republic that deal with this concept of social engineering. One of the available current sources is the publication of Jan Kolouch Cybercrime. From abroad, the book The Art of Deception, which was translated from the English original The Art of Deception by Kevin Mitnick. This book contains many useful recommendations to increase security against social engineering attacks, especially in companies.

We can understand the issues of social engineering and the degree of threat from the methods and techniques described by social engineers in the introduction to the article. It is dedicated to the psychological, technological, and other necessary skills that social engineers use in their attacks. He also mentions several cases that took place in real companies. The list of all methods and methods is not entirely exhaustive or complete, as the individual uses of techniques and procedures may be combined and composed. The article continues with an analysis of the state of information security in a particular commercial manufacturing company and proposes certain security recommendations leading to increased protection. Specific safety guidelines, audits, and other documents from the analyzed company are used to analyze the current situation. The conclusions of this analysis and specific recommendations can be used to improve the security situation in other companies that are aware of the need for these measures.

II. History of Social Engineering

The first case of social engineering skills was recorded in Greek mythology and the Trojan War. Odysseus, who commanded the Greek army, pretended to defend the Trojan defenders. As proof of the armistice, he dedicated a large wooden horse to the city of Troy. We know from history that it was the trap that destroyed Troy. Therefore, today the term "Trojan horse" refers to software that at first glance seems harmless and beneficial. [3] The term Trojan, therefore, refers to a program that further contains hidden functions. The user is usually not familiar with these functions or does not agree with their use. these functions can then be potentially dangerous for the further operation of the system.

Briefly, around 1920, Charles Ponzi's deception, now known as the Pyramids, became known. He promised the first investors a 100% profit within 90 days. He then paid off this money, which he obtained from new investors, part of which he kept. He is believed to have illegally enriched himself by $ 250,000 from at least 40,000 investors. [1] His deception became very well known. In the world, similar machinations are described as performed according to the "Ponzi scheme". A Ponzi scheme means fraudulent investment operations. Investors entrust money to the founder or operator of the fund for their interest. However, he does not further invest the entrusted money, retains it for his enrichment, and pays out the fund's resources as a profit to the initial investors.

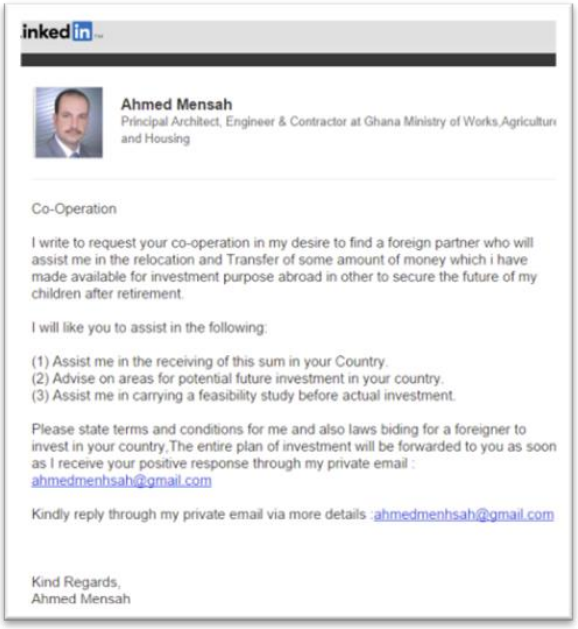

Figure 1 Fraudulent social engineering email [4]

As the picture above shows, the most famous of the present is the scam The 419 Scam, more precisely it is variant Nigerian Scam. The essence was to send a letter (now an email), which is sent by the fraudster to potential victims. It is usually about pretending to be a very rich person, very often a Nigerian prince. He offers his victims a very advantageous offer, where a large reward will be paid for providing a small financial amount. If the victim responds to this offer and sends the amount, he will usually immediately receive information about the complications that have occurred and the need to send another amount. This process is repeated indefinitely, with the person still sending small amounts under the promise of even greater rewards. Of course, the victim will never see his money again. There are currently several variants of fraud, with different stories. [5]

In the second half of the 1920s, two major attacks were recorded, also caused by two social engineers. The first was Frank Abagnale, who, at the age of 20, illegally obtained at least $ 2.5 million through several fake identities (a masterpiece of today's successful Catch Me If You Can Do It with Leonard DiCaprio) when he successfully pretended to be a doctor, lawyer or airline pilot. . The second is Kevin Mitnick, who at the time was the most wanted person to commit a computer crime. At the age of twelve, he received passwords from various corporations with just one phone call. For example, he obtained passwords from Motorola and Nokia. He was later arrested and, after serving his sentence, began working as a security consultant for Mitnick Security Consulting LLC. [5]

Nowadays, it is much easier to carry out any variant of previous attacks. With the help of the Internet and communication technologies, large groups of people are available to reach, and there is no need for a personal meeting or closer interaction. Thanks to new information and communication technologies, attacks can be carried out in a much more sophisticated and large way. It is a well-known fact that each new technology with its pros also brings new threats and, if successful, also the difficulty of detecting

attackers. In this way, any state institution, company, or individual can easily be attacked. [5]

III. ATTACKS USING SOCIAL ENGINEERING

The changing nature of social engineering does not allow us to describe exactly and simply how its attacks work. It is not an exact science, but a set of most of the principles that make attacks successful. Psychological principles are used here, as well as influencing the reactions of the environment. Even in professional literature, the description is very often simplified and vague. For better identification, it is necessary to set the criteria that define the attack.

A. Classification of attacks

Security attacks can be divided according to Vyskoč using the following 1 or 2 aspects:

1. Whether or not the user is involved in the attack:

- Autonomous - attacks implemented completely within the computer and communication structure. They do not require any user intervention (eg DDOS, SQL injection).
- Cognitive - requires some change in the user's behavior, caused by manipulation of his perception. The user's action or inaction is key in the attack (eg sending an infected e-mail that the user must open).

2. The aspect focuses on the form of implementation:

- Physical - a classic attack on physical components (eg keylogger connection, hardware theft).
- Syntactic - an attempt to eliminate the syntactic (operational) logic of a network or system and its subsequent disabling (eg DDOS, SQL injection).
- Semantic - producing or inserting false or misleading information to a user (or machine) to act in a certain way. [6]

According to these aspects, the attack of social engineering can be classified as a cognitive semantic attack. However, it should be borne in mind that an attack may consist of several procedures and techniques for achieving the attacker's target, and therefore there may be classification exceptions.

According to Mouton and others, we can also divide the attack of social engineering into 1 or 2 main categories:

1. Direct attack - This is an incident where two or more people are involved in a direct conversation. This conversation is either one-sided or multi-sided. We divide this into a direct attack with a two-way conversation, where each party consists of an individual, a group of individuals, or an organization. Furthermore, in a direct attack with a one-way conversation here the social engineer communicates with the target, but the target cannot establish a conversation with the attacker. It is done using communication media such as bulk emails or SMS.
2. Indirect attack - An indirect attack is performed by a third party, usually USB, websites, and more.

B. Types of attackers

In the case of obtaining the information needed for a credible start to communication, attackers are very useful websites of companies. Here the attacker finds out both the structure of individual companies, but also the names of the responsible employees. According to the names, they will check these, for example, on Facebook and other networks, when they will already obtain relatively comprehensive information. [7]

According to Hanagy, the attacker focuses on the following information:

- the victim's employment and type of classification
- what is his position, colleagues
- where the victim lives,
- whether the company offers new jobs,
- company structure, corporate jargon

The attacker must find out a large amount of detail and information to persuade the victim and to prevent checks or inquiries. Because technology and computer technology do not require personal contact, these attacks are often successful.

It follows from the above that anyone who has the talent to manipulate people and acts in a trustworthy manner can become a social engineer. However, about today, it can be stated that it is most often used to obtain information, passwords, and access to corporate networks. The article will focus on these in particular.

- Criminals - this is a large group that chooses individuals or organizations - hackers, fraudsters, and organized groups.
- Penetration testers - these are groups of information-savvy people who test their information systems security for their clients.
- Traders - using influencing and persuasion techniques that are part of social engineering, they negotiate with their clients and successfully close deals. [8]
- Doctors - positive manipulation motivates people to better life and overall behavior.
- Ordinary people - it is part of people's lives to influence their surroundings with the fact that their decision is beneficial for them. Often they may not even be aware of this manipulation. [1]

IV. ATTACK ANALISIS

No attack can be considered so simple that it can be carried out in a single step. It always consists of several, which follow one another:

1. obtaining information,
2. planning and preparation of the attack,
3. attack,
4. victim's response - obtaining information,

5. recovery of information - the peak of the attack.

The first step is to obtain information about the victim, her surroundings, jobs, hobbies, and friends. Under these circumstances, an attack plan is created with several possible courses. An attacker must be prepared for any questions to avoid losing credibility. Then comes contacting the victim and trying to lure information. The completion is then the use of the obtained information. [9]

Another well-known model of social engineer's attack comes from Kevin Mitnick's so-called sociotechnical cycle. This cycle contains 4 phases:

1. survey (data retrieval

2. building relationships and trust,

3. use of trust,

4. use of information.

It also begins with obtaining information about the victim. It continues with the second phase when the attacker pretends to be someone else, mentioning the names of people known to the victim. In the end, he asks him for help or tries to give the impression of authority. Once trust is built, the attacker asks the victim to share information or take action. In some cases, a capable type of attacker will use manipulation means so that the victim himself requests cooperation. If the information obtained is only the next step in bringing the attacker closer to the target, it returns to the previous points of the cycle until it reaches its target. [10]

When comparing the above procedures of social attacks by Greitzer et al. and the socio-technical cycle from Mitnick we notice a considerable difference. Mitnick views this process as a repeating cycle as needed as a cycle. It assumes that the individual steps are used several times in a row. Only partial targets of the attack are achieved in them. And this cycle ends only when the attacker reaches the target.

Another look at the attack using soc. engineering provides the so-called ontological model of attack [10]. The difference is that it does not look at the attack as a whole in the process, but focuses on the individual elements of the attack. Each attack has its architect, the so-called social engineer or attacker. He is looking for a victim who is willing to help him achieve his goals using manipulation techniques, media, and some form of socio-technology. [7]

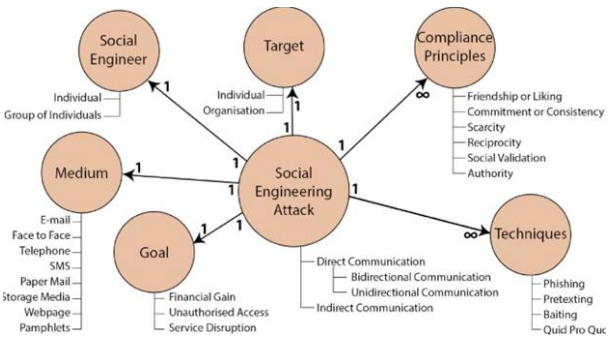

Figure 2 Attack ontology [11]

The procedures of individual attacks were mapped here and these were used to design this template of attacks. However, the individual indicators are also generalized to apply to different cases.

V. SOCIAL ENGINEERING TECHNIQUES

Just as there are several types of attacks and attackers, there are several techniques for performing attacks. Nowadays, the attack does not take place without technology. Social engineering mainly uses pretexting, pharming, baiting, phishing, vishing, smishing, and water holing. Currently, the most used and therefore the most developing are pretexting and phishing [10]

- Pretexting - it is a technique where an attacker impersonates someone else so that later, after building trust, he can use someone else's identity to obtain sensitive information. Both the script and the characters are created. These are composed and match the victim's surroundings to make it feel believable. The victim's environment, experience, description of the corporate environment are always mentioned so that the victim is more prone to cooperation and information. Typically, an attacker calls the organization and impersonates someone in management, requesting access to information from his or her authority. He argues about time pressure during a meeting or business meeting. The attacker must be prepared to be asked questions by the victim and therefore devotes himself to the thorough collection of information in advance.

- Pharming - the goal here is to obtain personal or private data, for example to bank accounts, using fake domains. This method attacks the DNS server and rewrites the IP address. The victim is then redirected to a fraudulent page created by the attacker. However, the browser shows that it is on the right web page, so pharming is difficult to detect.

- Baiting - this attack uses physical media such as floppy disks, CDs, or USB drives. An attacker leaves them infected with malicious code in clear and used places. It relies on the victim's curiosity. For example, an attacker creates a USB drive with the logo of a well-known company and inserts a top-secret inscription. An unsuspecting victim then inserts a USB disk into the computer and simply inserting this media into the computer starts the installation of the malicious program. This will give the attacker access not only to this computer but also to access to the entire corporate network.

- Phishing - a well-known technique for sending bulk email to as many users as possible. This may be a fraudulent email created from a well-known company website. Only during a more detailed study of eg, an email address is it found that the letters in the company name were accidentally changed, etc. The e-mail usually contains a hypertext link and asks the user to visit the website to update personal data. Usually passwords, bank card numbers, social security, and bank accounts. A website is a hoax created to steal user data. Another option is to attach an infected file, such as an "overdue invoice".

- Vishing - is a similar tactic to phishing, except that it is used by the phone to persuade the user to release private information.

- Smishing - it is similar to vishing and phishing. In this technique, an attacker uses SMS instead of a call or e-mail. Using an SMS message attracts the victim to certain behaviors. As with phishing, it can be a malicious hyperlink or lure information from the victim.
- Water Holing - this is a strategy where the attacker uses environments that victims regularly visit, such as websites. The victim is therefore attacked in a well-known environment. The process begins by gathering information about the websites that the victims are visiting. Then the vulnerability is tested, the code is entered. This can then infect the visitor system with malware. Code injection and malware are tailored to the selected target group and systems.

There are many other techniques and ways. In addition, these techniques can be combined, the credibility of the email can be supported by telephone contact and vice versa.

VI. PROTECTION AGAINST SOCIAL ENGINEERING IN A COMMERCIAL PRODUCTION COMPANY

In 2015, the security company Balabit conducted a survey to find out the 10 most commonly used methods in a hacker attack. 494 US security experts were interviewed. Phishing came first, breaking a weak password second. [12] It is therefore important that every company using information and communication technologies, regardless of its focus, ensures compliance with security standards and their continuous updating. Below is a picture of individual organizations and their protection - using artificial intelligence.

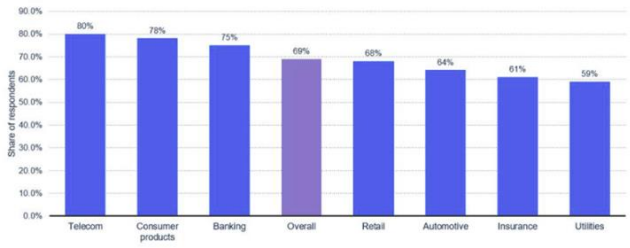

Figure 3 Share of organizations relying on artifical for Cybersecurity in selected countries as of 2019, in Industry [13]

For clarity, an analysis of the security of the information system in a commercial and production company against attacks by social engineering will be performed. From the results of this analysis, proposals will be made to increase safety over the current situation. The company uses an information system to ensure its operation, where information is collected, processed and stored. The smooth operation of this system is important for the overall operation of the company, but also for the protection of sensitive data. These relate to the company itself, its structure and personal data of employees. Furthermore, data on clients, suppliers and production processes are collected here. The system was introduced to support all sections of the company. That is, from the company's management through the accounting and sales department, to the department of the warehouse, shipping and production output. Data of customers, individual orders, materials up to the final invoice for goods and services are introduced here. The company has been attacked several times by social engineering at the stage of a failed attempt. There was no leakage of sensitive data or direct financial damage. However, before the system was restored and the attack completely averted, there were downtime of the company. It is therefore appropriate to check security, comply with security standards and update them here as well. Furthermore, as social engineering methods and techniques change and improve, further measures need to be considered. Sustainability is a strategy of the process of sustainable development. [14]

As part of the security analysis, we will focus on the following areas:

- Security policy
- Information security organization
- Personnel security
- Access control
- Traffic management
- Communication security
- Information security incident management

A. *Security Policy*

The creation and adoption of a company's security information policy should be ensured by its security management. After that, all employees, suppliers, and customers should be acquainted with it. The security policy should be a clear signal of the observed standard not only inside the company but also outwards. Once this policy is in place, it must be regularly reviewed and updated according to the situation. The currently surveyed company does not have a precisely defined safety policy according to international standards. They follow established guidelines, which are commented on by auditors every year. Information security is contained in the Information System Directive in the following points:

- basic security, anti-virus protection policies for users, protection against user abuse, protection against external attacks, security of assignment of access rights and authentication of authorized persons, security against unauthorized access, determination of the scope of access rights, allocation of emergency rights, and security procedure employees.

Company guidelines are available to all employees. However, they are not enough to cover all the critical points of society. It is not stated what attacks the company is exposed to, nor what attacks have been made on it in the past and how they have been dealt with. On the plus side, the guidelines are updated annually by auditing the most important points. The audit is performed internally and then control by external auditors. The allegations are recorded and a deadline is set for their correction, which is then subject to inspection.

Recommendation: To create a comprehensive information security policy according to the ISO / IEC 27002 standard and a separate directive only for information security, not as a small section of the Information System Operation Directive. The individual directives should be interconnected and cover all areas of society. Indicate the specific situations that may occur and how to solve them. To acquaint all employees and company partners with this. Not only employees are interested in the security of their data, but also customers and suppliers. Continue the annual review of the guidelines and their timeliness, followed by an axle check. If there are changes, it is advisable to inform employees about them.

B. Information security organization

Each safety function must be clearly defined and a person appointed to and from the sections covered by it. The different areas and the rights and obligations belonging to them should be separate. This will reduce the possibility of misuse of most of the company's assets. Today, a directive regulating the use of mobile devices in society should be a natural part of it.

Current state-security management and control fall under the IT department. This is managed by financial management. An employee of the IT department recommends and monitors the operation of information systems, the approval and purchase of which falls under financial management. They forge maintenance and updating of these systems, solve problems with external professional companies. By signing the guidelines, employees confirm compliance with the company's guidelines regarding work with the information system. The IT department checks its compliance and reports any negligence to the superiors of these employees.

Recommendations - there are no guidelines for the use of own and corporate mobile devices. It is therefore recommended to adopt a uniform company policy on their use, where their use for non-business purposes will be regulated. It should also prohibit the provision of any information by telephone or email relating to information security. In the past, the corporate network has been infected by connecting a private device, which should therefore be completely banned.

C. Personnel security

All new job seekers should have a personal check of the information provided in their CV. These are mainly references from previous jobs, verification of education, and a possible extract from the criminal record according to the starting position. When starting a new job, they should be trained in all areas of security, including information.

Current status - upon commencement of employment, proof of education is required. References from previous jobs are not collected. Technology skills are not tested and the new employee is not specially trained. The guidelines only define the penalty for a breach of a specific employee, not for a specific incident. Passwords and accesses are defined by the IT department employee on the order of the head of the department to which the new employee belongs. After his departure, the rights are revoked.

Recommendations - before starting, carry out an additional inspection of the new employee at the previous employer, check the data from the CV, and be required to extract the criminal record. The company does not receive any security training on information technology security. They are not informed about unwanted attacks, so they are not aware of current threats. Enter these responsibilities into the workload of IT staff, for example, send them by email.

D. Access control and passwords

Users should be assigned and granted only access to those parts of the system that they need in the exercise of their profession. These inputs should comply with all safety standards, at least those required by company safety guidelines.

Current status - when an employee joins, his account is created, to which passwords and email are assigned. He is also assigned a PC with a password, which also has an IT department. Approaches are determined by the job position and the head of the department. The login name and password cannot be changed by the employee. Computers stay online 24 hours a day, and employees do not log out of individual software products when they leave.

Recommendation - Disable leaving passwords typed near your computer as you often see. Disable a single login password for individual company software. It is necessary to completely change the policy of assigning passwords, the inability to change the password, and collective login. It is necessary to log out at the end of work from individual software, introduce this as a standard.

E. Traffic management

The company should not only set standards for safe walking but also detect their non-compliance and social engineering attacks. Precautions should be taken as well as continuous data backup, security program updates, and user review of newly installed software.

Current status - data, servers, and workstations are protected against malicious software. The antivirus program is set to install updates itself in the evenings when the computer is not being used by an employee. Employees are prohibited from setting any changes, however, they may make them secretly. Changes are not detected immediately by IT staff. However, they have the right to block individual employees from accessing the site. Which do not match their work focus. It is also the department responsible for backing up data to a central server. No records are kept of the performance of these backups.

Recommendations - using security software alone is not enough to secure your company's data. Here, too, it is necessary to train employees on new current threats, identification of malicious emails and attachments.

F. Communication security

Information security policy must include rules for the exchange of information not only within the company but also outwards. They must apply to all types of communication media and, if exchanged electronically, following all security rules.

Current status - most information transfer and communication takes place via Microsoft Outlook. Furthermore, via mobile phones and landlines, SMS messages are also used. The sales department communicates in all world languages via emails and their attachments, the production department in the Czech language. The company has no rules for electronic communication.

Recommendations - Establish a directive for working with means of communication and electronic mail. Inform employees about fraudulent mail and verification of suspicious attachments or personal identities.

G. Information security incident management

A security information incident management procedure should be developed in each company to ensure rapid and effective defense to minimize damage and information leakage. These incidents should be recorded and investigated.

Current status - the information security incident management process is not specified. No records are kept, individual attacks are in most cases not reported. Reporting is done by phone or email to IT staff. Everything is solved without a record, at most by reporting to the appropriate superior. The company is facing mass fraudulent emails, malicious attachments, and a case of ransomware.

Recommendations - the company should start keeping records of individual attacks and their solutions. Guide how to address them to employees. In addition, make traceable reporting of these incidents operational, for example in the form of a Helpdesk. Suspicious employee behavior should also be recorded.

VII. DISCUSSION

Information and communication technologies affect all areas and parts of every society. Each department must be in contact with others, receiving and passing information to them. Therefore, it is and will be extremely important that not only managers but also the most remote are informed about all the dangers and threats that can be realized with the help of these technologies. individual companies and institutions therefore create their own internal guidelines. These then correspond to the processes that take place in them. As follows from the above analysis of the guidelines of a particular trade and production company, the production processes are described in detail. However, this cannot be said about updating technology protection in companies where their protection and use is described very marginally. It is not updated according to the current situation in the cyber world.

The summary of the analysis of the current state of the above company is clear and after their implementation it is assumed that the monitored company will function better. It can be said that its current security is at a satisfactory level according to its current needs. However, the information security situation is changing every day and it is therefore necessary to either update the measures or create new ones, depending on the situation. The information security situation is changing every day, and it is therefore necessary to update the measures taken or create new ones, depending on the current situation. The company has not yet clashed and attacked directly. The Company is therefore encouraged to develop new guidelines and procedures in accordance with applicable standards and taking into account the Company's functional needs. Also, record each incident, the people involved, and their solutions. It is essential that the computer settings are correct to ensure secure user protection. [15] Raise employees' awareness of existing threats, implement training, and repeat these on an ongoing basis, especially adhering to basic information security principles:

Basics of protection when working with information and communication technologies:

- create a strong password in a combination of characters, uppercase and lowercase letters, preferably a fingerprint
- do not store credentials freely around the device
- enter the password secretly and lock it when leaving the device
- update device protection and software regularly
- technologies like Wifi and Bluetooth turn on only when needed
- portable devices such as USB and the like use encryption when storing data
- back up data to external devices
- do not connect any unknown devices (especially memory devices)
- turn off unwanted operating system services (such as location services)
- check the correctness of the name of the visited pages (due to possible redirection to malicious pages)
- the information on the Internet may not be true, so we verify from multiple sources.
- not to disclose any personal or sensitive information
- verification of identity with whom I communicate from multiple parties
- do not open phishing e-mails or suspicious attachments, immediately notify the IT department of their occurrence.
- not use online password strength control tools that can be passed to an attacker.

This article can serve as a guide for creating training for employees with individual needs, where its general points will be used as a basis. Each company must adapt further details according to its industry and focus. A study of the growing number of attacks by social technicians clearly shows that these attacks will continue to escalate. Companies that have not yet considered it a priority to respond to these facts must therefore include information security among their priorities. All measures do not require extreme investment or intervention by an external company. Many recommendations, especially the basic ones, are given on the Internet and in professional books. This information may also be gathered by IT staff and relevant departments may require the establishment and implementation of appropriate training. It is also possible to create instructions and records that respond to and map individual security incidents. The fact remains that the cost of prevention is much lower than the cost of dealing with side effects.

Information and communication technologies affect all areas and sections of every society. Each department must be in contact with others, receiving and passing information to them. Therefore, it is and will be extremely important that not only managers but also the most remote are informed about all the dangers and threats that can be realized with the help of these technologies. All employees must be constantly aware of possible attacks, their types and methods of execution. Indeed, social engineering poses a serious danger to anyone, from individuals to smaller and larger companies to the largest government corporations. Social engineering is a global problem for which adequate protection and early prevention are the best protection.

VIII. Acknowledgment

This research was based on the support of the Internal Grant Agency of Tomas Bata University in Zlín, the IGA / FAI / 2021/002 project and the Institute of Safety Engineering, Faculty of Applied Informatics.

References

[1] HADNAGY, Ch. 2011. Social engineering: the art of human hacking. Indianapolis: Wiley Publishing. ISBN 978-0-470-63953-5.

[2] WATSON, G .; MASON A .; ACKROYD, R. 2014. Social Engineering Penetration Testing Executing Social Engineering Pen Test, Assessments and Defense, Syngrey.

[3] STUART, Nathaniel. Commissum.com. The History and Evolution of Social Engineering Attacks. [Online] 24. 5 2018. [cit. 4/14/2019.]. Available from: https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks.

[4] https://365tipu.cz/2017/03/07/tip737-co-je-to-nigerijsky-spam-proc-mi-nekdo-pise-ze-jsem-zdedil-miliony/

[5] CONHEADY, Sharon. Social Engineering in IT Security Tools, Tactics, and Techniques. [online] New York: McGraw-Hill Education, 2014. ISBN 978-0-07-181847-6.

[6] VYSKOČ, J. 2004. Hacking is not like hacking. DSM - Data Security Management.)

[7] MOUTON, F .; LEENEN, L .; VENTER, H. S. 2016. Social engineering attack examples, templates and scenarios. Comput. Secur. 59, 186–209. Available from: https://doi.org/10.1016/j.cose.2016.03.004)

[8] MALWAREBYTES. malwarebytes.com. Malware. [Online] [cit. 19.3.2019.] Available from: https://www.malwarebytes.com/malware/.

[9] GREITZER, FL; STROZER, JR; COHEN S .; MOORE, AP; MUNDIE, D .; COWLEY, J. 2014. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In : 2014 IEEE Security and Privacy Workshops: 2014 IEEE Security and Privacy Workshops [online]. Pp. 236– 250. Available from: doi: 10.1109 / SPW.2014.39)

[10] MITNICK, K .; SIMON W. 2003. The Art of Deception. B.m .: Helion S.A. ISBN 83-7361-210-6.

[11] https://www.sciencedirect.com/science/article/pii/S0167404816300268

[12] BALABIT. infopoint-security.de. Balabit CSI report. [Online] 2015. [cit. 2/26/2019.]. Available from: https://www.infopoint-security.de/medien/balabit-top-10-hacks.pdf.

[13] https://www.statista.com/statistics/1028762/worldwide-reliance-ai-respond-to-cyber-attacks-by-industry/

[14] Alena Kocmanová, Jana Hornungová, Marie Docekalová, Interakce mezi environmentálními, sociálními, podnikovými správami a ekonomickými ukazateli, Int. J. of Applied Mathematics, Computational Science and Systems Engineering, Volume 2, 2020, pp 113-121.

[15] MCCARTHY, Linda and Denise WELDON-SIVIY. Be the master of your space: how to protect yourself and your stuff when you are online. Prague: CZ.NIC, 2013. ISBN 978-80-904248-6-9.