DOI: https://doi.org/10.34069/AI/2021.38.02.11

Counteraction to methods of social engineering as one of the areas of information protection of organizations with varying degrees of state participation

Противодействие методам социальной инженерии как одно из направлений защиты информации организаций с различной степенью государственного участия

Received: February 25, 2021 Accepted: March 30, 2021

Written by:
Elena A. Ostanina[30]
https://orcid.org/0000-0001-8559-5362
https://www.elibrary.ru/author_profile.asp?id=822012

Abstract

The relevance of this topic is due to the constant improvement of technical means of transmission and processing of information, as well as the creation of new technologies for its processing and storage. At the same time, the growth in the value of information as a resource in the modern world and the transition to electronic document management in the activities of organizations is accompanied by the emergence of new methods of illegal access. The purpose of this study is to analyze the most relevant methods of influence and create a training program for staff that would minimize the risks associated with illegal access to information of organizations. The paper presents and analyzes data characterizing the share of the impact of social engineering methods on individuals and legal entities. The study has confirmed that the most effective way to protect against social engineering is to train workers. It is advisable to organize the process periodically in a distance format, adapting the program to the position occupied by the employee. Training, in addition to theoretical lessons on the study of methods of protection, should contain active methods, discussions on the analysis of current information security incidents and solution of case studies.

Key Words: distance learning of staff, information security, countermeasures, social engineering, security threat.

Аннотация

Актуальность данной темы обусловлена постоянным совершенствованием технических средств передачи и обработки информации, а также созданием новых технологий ее обработки и хранения. В то же время рост ценности информации как ресурса в современном мире, переход к электронному документообороту в деятельности организаций сопровождается появлением новых способов неправомерного доступа. Целью данного исследования является анализ наиболее актуальных методов воздействия и создание программы обучения персонала, которая позволила бы минимизировать риски, связанные с неправомерным доступом к информации организаций. В работе приведены и проанализированы данные, характеризующие долю воздействия методами социальной инженерии на физических и юридических лиц. Проведенное исследование подтвердило, что наиболее действенным способом защиты от социальной инженерии является обучение работников. Процесс целесообразно организовывать периодически в дистанционном формате, адаптируя программу к занимаемой сотрудником должности. Обучение, помимо теоретических занятий по изучению методов и способов защиты, должно содержать активные методы, дискуссии по разбору актуальных инцидентов информационной безопасности и решение кейсовых заданий.

Ключевые слова: дистанционное обучение персонала, информационная безопасность, методы противодействия, социальная инженерия, угроза безопасности.

[30] PhD in Pedagogical Sciences, Associate Professor, Moscow Aviation Institute (National Research University), Moscow, Russia.

Introduction

Information in our time is a key resource of almost any organization or community, company and even the state as a whole. It can reflect the personal data of a person, constitute a commercial secret of the company and affect its financial condition, as well as be classified as information constituting a state secret and determine the security, integrity and sometimes the existence of the state. Thus, the issues of ensuring the security of information resource all over the world come to key positions and require careful analysis, assessment and prompt response to modern challenges.

In organization, a breach of information security can be the result of an accidental or deliberate misconduct of an individual with respect to the organization's assets. As a result, use, processing of information by technical means and processes accompanying it in information systems can have negative consequences. Violation can be caused by erroneous actions of people, improper functioning of technical means of processing, storage or transmission, natural factors (for example, fire or flood), as well as deliberate actions of intruder, leading to a violation of confidentiality, integrity or availability.

Within the framework of this study, the analysis and assessment of the significance of the human factor in ensuring the information security of an organization was carried out. In the course of analyzing the publications of researchers on the issues of identifying information security vulnerabilities, it can be concluded that one of the most vulnerable components in the current conditions of the activities of organizations, financial companies and government structures is a person. The study examined such categories of information as information related to trade secrets and personal data in terms of information about employees and customers of organizations.

Industrial espionage has existed for a very long time, but nowadays it is acquiring a significant scale precisely in terms of "hunting" for information using a lot of means and methods.

It is noted that in the information society it has become easier to manipulate people. Interaction without direct contact via mobile Internet communication has greatly simplified this procedure. The constant improvement of information technologies and the technical means that provide them requires the employee to constantly improve his skills and abilities, however, quite often the employee simply does not have time to educate himself in all these areas. As a result, human interaction with the information system can pose a threat to the information security of an organization. Its implementation can be caused by a deliberate action of an employee and committed through ignorance (lack of qualifications), through inattention or negligence, as well as with outside influence on him by methods of social engineering, the basis of which is misleading a person.

Inadvertent actions of employees, as a rule, include the loss of information carriers, destruction or distortion of information through negligence, assistance to “wrong persons” as a result of exposure to them by social engineering methods, when the employee does not realize that his actions may lead to a violation of the security regime, while the one who asks him to do so is aware of the possible violation. As a result of such actions, information can become available without direct impact on the technical means of its transmission, processing and storage.

An attacker can try to get hold of information by hacking a database, intercepting messages or documents on the network, retrieving information from technical devices (monitors, keyboards, printers) and data transmission channels, as well as attempting to modify or destroy information. However, this article discusses in more detail a fairly effective method of obtaining confidential information and information containing commercial secrets, which is largely based on the use of weaknesses, prejudices and complexes of the organization's human resource.

Theoretical Basis

Social engineering is a method of obtaining the necessary access to information, based not on hacking an information system using hardware and software, but on the peculiarities of the psychology of employees of organizations. The main goal of social engineering is to gain access to confidential information, passwords, banking data and other secure systems.

In the current interpretation, the English term "social engineering" can be presented as an integral group of psychological and analytical methods of influencing employees in order to "push" them to take actions leading to a violation of the organization's information security.

Methods and means of information protection primarily include software and hardware, legislative, organizational and administrative methods (Kodeks, 2006).

Unforeseen or undesirable event that can disrupt the activities of an organization, in terms of information intra-organizational or external interaction or its information security in general, is usually called an information security incident. These include the following: ignoring policies or recommendations on information security; system failures and overloads uncontrolled system changes; software failures and hardware failures; loss of equipment or devices; user errors; violation of physical protective measures; violation of access rules (Kodeks, 2008).

A variant of the generalized attack scheme using social engineering can be represented by the following chain:

1. definition of goals;
2. choice of object;
3. collection of information about object;
4. assessment of possible methods of impact on object and determination of the most effective ones;
5. attraction;
6. coercion to desired action;
7. obtaining information / performing actions required by attacker.

At the same time, used methods are aimed at forming such a behavioral model of an employee that is beneficial to the attacker and carries a false idea of voluntariness and independence of its acceptance by the object of influence. Attraction is a concept that denotes the appearance, when a person is perceived by a person, of the attractiveness of one of them for another (Karpenko et al., 1998).

As a rule, all social engineering techniques are based on the personality traits of a person and take them into account when making decisions. No one can be protected from the scrutiny of intruders: neither top managers, nor administrative employees, contractors or interns. Even business partners can be used (without their consent and knowledge of this fact) to obtain confidential information and access networks. Even relatives, including children, studying remotely from March-April, 2020 and using the home network their parents worked through could be potential targets. The higher the position is occupied by a person exposed to an attack in an organization, and not only in management terms, but also in terms of the level of access to the organization's information resources, the more widespread the consequences of the attack can be. It is important to note that such methods are quite effective, simple and cheap to implement and also have a low degree of risk (Gridin, 2010).

Scammers rely on publicly available data to hack into the psychology of attack targets to create victim profiles. They are experts in the art of manipulating, influencing and creating decoys to deceive people. The purpose of these actions is to push people to disclose confidential data or provide access to networks of organizations or their facilities.

Fortinet experts identify the following options for attacks using social engineering (TAdviser, 2020).

Spearphishing is Email-based attacks targeting a specific person or an entire organization. The goal is to induce people to click on malicious links or to collect credentials. It is noted that local phishing targets a specific person through social networks and instant messengers (Itglobal.com, 2021).

Cheating on social media by creating fake profiles: the goal is to win the victim's trust, deceive him and force to provide confidential information or download malicious software to his device.

A plea under pretext attack involves a cybercriminal preparing a good pretext or a plausible story to convince the victim of the need to provide certain information.

WaterHolding involves collecting information about visits to websites from a target group (persons of a particular organization, industry or region) by an attacker. It searches for vulnerabilities on these resources and infests them with malicious software. As a result, when visiting these websites, malware infects employees' technical devices. However, it should be noted that this attack is not limited to social engineering and involves the complexity of using various methods.

Smashing is an attack using text phone messages, supposedly from a trusted sender. The goal is to download a virus or other malware to the victim's device.

Spoofing is an attack that involves faking the caller ID. In this case, the attacker calls, pretending to be a representative of some legitimate organization, for example, a bank, in order to "extract" confidential information (bank card details, etc.).

Separately, it is worth highlighting such a phenomenon as reverse social engineering, which implies an independent appeal of a person for “help” to an attacker (Mitnick & Simon, 2003). This is achieved by conducting advertising or sabotage operations, for example, creating a reversible problem on the victim's computer, followed by a recommendation (demonstration of a business card, advice from a good friend) to contact the attacker with such problems at the specified coordinates (Kuznetsov & Simdyanov, 2007).

This is not a complete list of possible life situations and involves constant monitoring of such incidents and the inclusion of their analysis in the training process on information security issues.

It is noted that 95% of all security breaches are currently caused by human factors. This is why it is imperative to train employees and continually deepen their knowledge of cybersecurity.

Methodology

In the course of an empirical study using methods of observation, analysis, interviewing employees of organizations and collecting data on information security incidents, an assessment was made of the percentage of respondents for whom social engineering methods were successfully applied (Algarni et al., 2017).

In Russia, social engineering methods have become widespread during the pandemic and the transition of employees to a distance work format. Compared to other countries, this problem “is growing at an explosive speed” (Alizar, 2019). In the reports of the Central Bank and in the comments of companies in the field of information security, two reasons for this growth are indicated: low cyber literacy of citizens and almost regular leaks of databases from government agencies and commercial organizations.

The primary target of most cyber-attacks is information theft. In attacks on legal entities and individuals, its share is 58% and 55%, respectively. Attackers pursue financial gains in attacks against these categories at 30% and 42%, respectively. The higher share of financially motivated attacks on individuals is explained by regular infections with malicious software, for example, when visiting questionable sites, personal computers and mobile devices of citizens. As a result, the threat of disseminating compromising information about a person with the aim of extortion is often realized (Positive Technologies, 2019).

When attacking legal entities, attackers are most often interested in personal data collected in companies' databases. These can be customer bases and databases containing employee credentials.

Considering social networks and numerous forums as a source of information, it should be noted that users do not always care about the security of their accounts, using simple and identical passwords, without checking the reliability of the resource, enter credentials and information that helps to guess the password. This explains the high share of stolen credentials (44%) in attacks on individuals (Positive Technologies, 2019).

Here there is the typification of stolen data in attacks: individuals and legal entities. So, when a legal entity (company) is attacked, accounts make up 27%, personal data 29%, payment card data 13%, information related to the category of trade secrets 12%, medical information 7%, customer databases 6%, personal correspondence 2% and other information 4%. At the same time, when an individual is attacked: 44% are credentials, 7% are personal data, 34% are payment card data, 9% are personal correspondence and 6% are other information (Positive Technologies, 2019).

The share of targeted attacks is constantly growing, with the most active attacks being carried out against government organizations (about 20%), industrial companies (10%) and medical and banking organizations.

When attacking government, industrial and medical institutions, cybercriminals prefer using malicious software and social engineering methods. Hacking, exploitation of web vulnerabilities and brute-force credentials are used much less often nowadays (Albladi & Weir, 2018).

Cybercriminals actively use, for example, a set of services Azure App Service for various types of fraud using social engineering methods. Users are prompted to fill out fake authentication

forms, log in through a fake form pre-hosted on the Azure Blob Storage platform, which allows for credential theft. Another way is data collection, when a small amount of money needs to be transferred under the pretext of address verification to receive a certain prize. Also, YouTube platform is often used when distributing malicious software, when the description under the video contains links that initiate the download of remote control programs, for example, njRAT, Qulab stealer and clipper and other malicious programs (Koyun & Al Janabi, 2017).

There is the susceptibility of people to social engineering, their interaction with the banking sector and the field of online shopping. The use of remote payment methods for goods and services by that part of the population that, prior to the introduction of restrictions in connection with the COVID-19 pandemic, purchased and paid for them directly at points of sale, led to an increase of almost 40% in the number of financial transactions carried out without the consent of users. Due to the lack of the necessary experience in countering attackers, a significant part of the citizens turned out to be vulnerable to social engineering. The share of transactions carried out without the consent of users using social engineering in 2019 and 2020 (Central Bank of Russia, 2020) is 5% for the remote banking service system for legal entities in the first quarter of 2019, 8% in the second quarter, and in 2020 the first quarter is already characterized by the share of operations with the use of social engineering 44%, the second quarter: 29%. For the remote banking system for individuals, the indicators for 2019 were 86% (first quarter) and 94% (second quarter), in 2020 they were 85% and * 7%, respectively. Payment for goods and services on the Internet without the consent of users was accompanied by social engineering methods in 2019 in 56% of cases in the first quarter and in 65% of cases in the second one, in 2020 these figures are 63% and 89%, respectively.

Thus, for a number of positions, the share of attacks using social engineering is significant and reaches 80-90%.

According to the security information portal SecurityLab.ru, the number of such attacks in 2020 increased by 147% (Securitylab.ru, 2020).

The third quarter of 2020, according to experts from the Central Bank of the Russian Federation, also showed growth in all types of attacks, with the exception of attacks using vulnerabilities in software.

In 2020, a lot of new schemes of fraud appeared (TAdviser, 2020). These include fraudulent schemes in Telegram, through infection through "presentations" of a product intended to be demonstrated in paid advertising and active parasitism on increased anxiety and insecurity of people during pandemic.

The use of empirical methods made it possible to establish a correlation between certain reactions of employees of various organizations and the use of social engineering methods in relation to them. The study revealed an increasing trend in the number of such incidents, as well as an increase in the percentage of employees exposed to the use of social engineering methods. The advantage of the observation method in this case is that the study of the object of study takes place in real time and in a natural setting simultaneously with the changes in society caused by COVID-19 pandemic and improvement of the methods of social engineering. In the course of the observation, a purposeful recording of the most effective areas of influence by social engineering methods on employees was carried out. Indicators, expressed in numerical form, quite fully reflect the range of methods used and the priority in their implementation. It should also be noted that there are no differences in the perception of the surrounding reality by the observed and the observer.

Results and discussion

As a rule, companies spend a lot of financial resources on ensuring information security using technical methods, while these technical means may be useless if employees do not know the measures to counter social engineering or simply neglect them (Ostanina, 2019). The main defense against social engineering, according to numerous claims by scientists and employers, is training. In this regard, a variable training program is proposed, taking into account the employee's job status.

As any process of training (professional development) of adults at the initial stage, the preparation of specialists to counter the methods of social engineering should include incoming control (Salahdine & Kaabouch, 2019). In the course of this control, it is necessary to find out the level of training of the employee in the field of legislation (protection of which data is

provided for by laws, what is the measure of responsibility for its disclosure), technical literacy (knowledge of the features of the transmission of information on the network and possibility of its interception by hardware and software) and personal characteristics through psychological tests (tendency to spontaneous actions, exposure to other people's influence) (Abass, 2018).

When training, it is advisable to provide up-to-date knowledge about potential threats and ways of obtaining confidential information by attackers, whether it is personal data or information classified as various categories of secrets and ways to prevent such actions (Sorenson, 2019).

The training process should also be based on case technologies, when an employee, through solving specific problems and on specific situations, learns methods of counteracting social engineering. The reverse method is also interesting, when a group of students is instructed to create a scenario of a situation that can lead to the disclosure of confidential data.

In the process of training, the attention should be paid to the obligation to follow the instructions of the companies. They, as a rule, prescribe issues affecting the information security of the company, how to (accurately, without errors) authenticate the interlocutor during telephone communication correctly, how to identify a person and determine his affiliation with the company's employees and how to accompany clients (Siadati et al., 2017).

The program should be adapted for a specific organization or group of companies, taking into account the specifics of their activities and experience in preventing incidents. It can be implemented using distance learning technologies.

As a result of a survey of employees of organizations, the following results were obtained:

- 78% of respondents neglect to follow instructions when using personal devices;
- 64% neglect measures of additional control over the identity of callers;
- 46% use personal e-mail and send official documents via unprotected communication channels;
- transition to unverified Internet resources when searching for information was carried out by about a quarter of respondents;
- 20% of respondents or their relatives fell for the tricks of fraudsters through social networks at least once.

As a result of solving the cases, it was found that 43% of employees made a mistake in identifying the attacker, considering him an employee of their organization. This was especially noted by respondents in large organizations during the transition to distance work.

Based on the obtained results, it can be concluded that the use of social engineering methods to illegally gain access to confidential data often leads an attacker to the desired results. As a result, the need is objectively created to take a series of consistent actions to counter such methods.

The results of this work allow updating the training process taking into account the current situation and the transition of employees to a remote format. The use of active teaching methods using distance technologies on a regular basis for the purpose of preventing information security incidents in organizations of different fields of activity has not been previously carried out.

At the same time, considering rapid development of technologies, their introduction into everyday life and further improvement of social engineering methods, it should be noted that the relevance of countering such methods will not decrease. In this regard, the controversial nature of issues related to countering unauthorized access to information will continue to persist.

Conclusions

Thus, ever-increasing value of information, transition to the widespread active use of information technologies and network resources, as well as the improvement of methods of illegal obtaining of information will require periodic additional training of employees in each organization. The organization of such training using distance technologies can bring an additional effect by bringing the training conditions closer to the real activities of employees in new conditions.

References

Abass, I. A. M. (2018). Social engineering threat and defense: a literature survey. Journal of Information Security, 9 (04), 257.

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social

engineering attacks in social networks. Human-centric Computing and Information Sciences, 8 (1), 1-24.

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal of Information Systems, 26(6), 661-687.

Alizar, A. (2019). Social engineering in Russia is more effective than in other countries. Habr. Retrieved March 04, 2021, from https://habr.com/ru/news/t/459278/

Central Bank of Russia (2020). Review of the reporting of information security incidents during the transfer of funds for the 1st and 2nd quarters of 2019 - 2020. Retrieved March 04, 2021, from https://cbr.ru/analytics/ib/review_1q_2q_2020/

Gridin, A. (2010). A brief introduction to social engineering. Habr. Retrieved March 04, 2021, from https://habr.com/ru/post/83415/

ITGLOBAL.COM. (2021). Information security in 2021. Threats, industry trends. Habr. Retrieved March 04, 2021, from https://habr.com/ru/company/itglobalcom/blog/540748/

Karpenko, L. A., Petrovsky, A. V., & Yaroshevsky M. G. (1998) A Brief Psychological Dictionary. Rostov-on-Don: Phoenix. Retrieved March 30, 2021, from http://lib.mgppu.ru/Opac Unicode/app/webroot/index.php?url=/notices/index/IdNotice:12641

Kodeks (2006) State Standart GOST R 50922-2006. Information security. Basic terms and definitions. Standardinform, Moscow, Russian Federation, February 01, 2008. http://docs.cntd.ru/document/gost-r-50922-2006

Kodeks (2008) State Standart GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. Standardinform, Moscow, Russian Federation, October 01, 2009. https://internet-law.ru/gosts/gost/48411/

Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. Journal of Multidisciplinary Engineering Science and Technology, 4(6), 7533-7538.

Kuznetsov, M. V., & Simdyanov, I. V. (2007). Social Engineering and Social Hackers. St. Petersburg: BHV-Petersburg.

Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. New York: John Wiley & Sons.

Ostanina, E. A. (2019). Information security in the implementation of the BYOD concept. Human capital, 12(132), 131-141.

Positive Technologies (2019). Research by Positive Technologies. Topical cyber threats Q2 2019. Retrieved March 04, 2021, from https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: a survey. Future Internet, 11(4), 89.

Securitylab.ru (2020). Social Engineering Attacks Increase 147% in 2020. Retrieved March 04, 2021, from https://www.securitylab.ru/news/515178.php

Siadati, H., Nguyen, T., Gupta, P., Jacobsson, M., & Memo, N. (2017). Monitor Your SMS: Mitigating Social Engineering with Second Factor Authentication. Computers and security, 65, 14-28.

Sorenson, J. (2019). Toward a pragmatic and social engineering ethics. Paladyn, Journal of Behavioral Robotics, 10 (1), 207-218.

Tadviser (2020). Social engineering. Retrieved March 04, 2021, from https://www.tadviser.ru/a/521580