INFORMATION WARFARE

DOI: 10.20535/2411-1031.2018.6.2.153489
UDC 004.056.53

OKSANA TSURKAN,
ROSTYSLAV HERASYMOV

DETECTION OF VULNERABILITIES OF THE COMPUTER SYSTEMS AND NETWORKS USING SOCIAL ENGINEERING TECHNIQUES

Information protection in computer systems and networks is focused on preserving its confidentiality properties of, integrity and availability from various inherently adverse impacts. Potentially possible adverse effects are interpreted as a threat. To prevent or complicate the possibility of realizing threats and reducing potential losses, a system of information protection measures is created and maintained in a healthy state. Such a system includes a computing system, physical environment, staff, and information. One of the most vulnerable elements of such system is staff. Within the framework of the socio-engineering approach, staff vulnerability is interpreted as its weaknesses, needs, mania (passions), hobbies. Manipulating them allows one to gain unauthorized access to information without destroying and distorting its main system-forming qualities. This is reflected in such forms as fraud, deception, scam, intrigue, hoax, provocation. The use of each of these manipulation forms is preceded by the determination of its content by careful planning, organization, and control. These actions are the basis of social engineering methods. Their use is aimed at imitating the actions of the information security violator, which are aimed at staff. This allows to assess the level of staff skills in the information security field and, as a result, to identify information vulnerabilities in computer systems and networks. The methods of social engineering used for this are divided into two groups, in particular, remote social engineering and personal contact. Methods of remote social engineering are implemented by means of modern telecommunications. In addition, the second group of methods involves the establishment of personal contact with the object of influence. In the end, it becomes possible not only to identify, neutralize, but also to prevent information vulnerabilities in computer systems and networks with the introduction of social engineering methods. Therefore, firstly, its protection is ensured taking into account the requirements of the information security policy; secondly, the rules of conduct of the staff are established, regulated by the job descriptions; thirdly, training is held to increase the persistence of employees stereotypes of the organization.

Keywords: vulnerabilities, computer systems and networks, behavioural model, social engineering, social engineering techniques.

Introduction. Detection of information vulnerabilities involves the phase aimed at the collection of data on the investigated computer system and/or network, namely, the phase of social engineering. The phase is included in the audit of the collection and information analysis from the outdoor environment. In view of the high probability of the human factor, the social engineering techniques are successfully carried out at this phase. To successfully accomplish the planned actions, a social engineer coordinates his work with a system administrator. The affirmative actions of a social engineer include the following: learning and analysis the content of the computer system and/or network, searching for vulnerabilities and development of the actions scheme [1] - [4].

Analysis of recent researches and publications. Using the social engineering techniques to simulate cybersecurity intruder actions, aimed at information system users of an organization, allows evaluating the qualification level of users in the cybersecurity ensuring area and a possibility of social engineering attacks realization [5] - [9].

When required data getting on an information system, a social engineer may regard as an input data, the data received from the public sources, contact information, family names and positions of the employees. It is necessary to highlight from the collected information the pieces in a computer system and/or network, which are vulnerable against the social engineering attacks, for their further use.

The social engineering techniques are based on the following [5]:

- characteristic features which control a human conscience;
- audience or actions field of an intruder;
- incompetence of an audience as regards the terms in the cybersecurity area;
- instability of the person's psychological features which characterize habitual stereotypes.

They may be used for a cautious manipulation (expressed through basic needs, weakness, propensity, wishes, ideals).

The article goal is analysis socio-engineering approach to the identification of computer systems and networks vulnerabilities.

The main material research. Within the framework of the socio-engineering approach, staff vulnerability is explained like its weaknesses, needs, mania (passions), hobbies. Manipulating them allows one to gain unauthorized access to information without destroying and distorting the main system-forming qualities (integrity, development). As a result, this leads to a new model of staff behavior, the favorable creation conditions for the information security threats realization and, as a result, a reduction in the ability of the information protection system to counteract their influence (see fig. 1). This is reflected in such forms as, for example, [4] - [8], fraud, deception, scam, intrigue, hoax, provocation. The use of these manipulation forms is preceded by the determination of its content by careful planning, organization, and control.

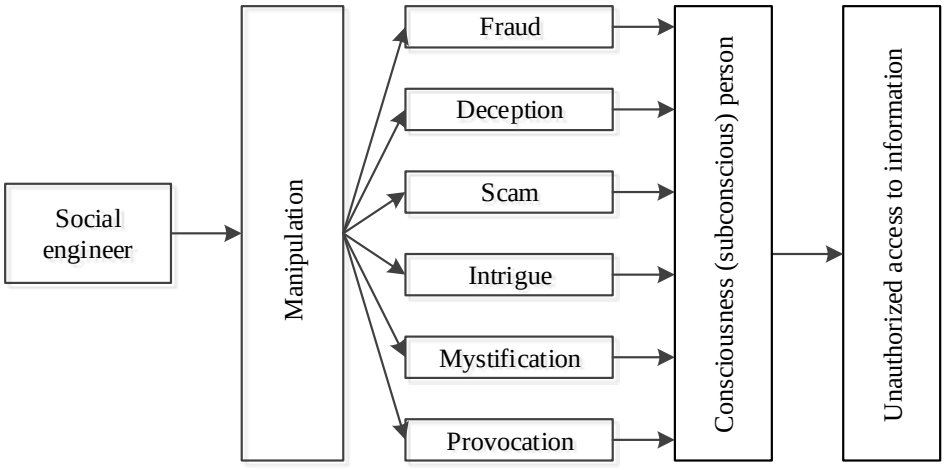

Figure 1 – Use of socio-engineering approach

Considering the fig. 1, the use of a socio-engineering approach to assessing the information security in computer systems involves a targeted impact on the consciousness (subconsciousness) of staff against their will, but with consent. Such an impact allows controlling the behavior of administration, administrator, users through weaknesses, interests, needs, inclinations, beliefs, habits, mental and emotional state. Therefore, manipulating these vulnerabilities is expressed in such forms as fraud, deception, scam, intrigue, hoax, and provocation. At the same time, the use of these manipulation forms is preceded by the determination of their essence through careful planning, organization, and control.

The forms of staff manipulation in assessing information security in computer systems vary depending on the type of social engineering attacks, namely [2] - [7]:

1. Phishing – a mass mailing to the large group of recipients. Acquaintance with e-mails encourages them to, for example, the opening of attachments to the letter, clicking on a link to a web page. Its purpose is to entice personal data from a trusting or inattentive computer system staff.

2. Pharming – redirect users to fraudulent sites to get their username and password. This is achieved through the spread of e-mail among users, for example, social networks, online banking, mail web services.

3. Pretext – receiving information or prompting to commit certain actions by deceit based on a pre-compiled scenario or creating a fictitious situation. Applied by phone and requires preliminary research to gain confidence.

4. Smishing – receiving information by sending mass SMS messages with a link to web resources or with details of organizations (for example, financial). As a result, appropriate actions are carried out, for example, a call to the bank to check the account status with an indication of confidential data: card number, expiration date.

5. Vishing – receiving information by entering into the trust during a conversation via IP-phone. At the same time, in violation of confidentiality, a statement is requested, in a message, to call a specific city number. For example, enter the card number, passwords, PIN codes, access codes, or other information.

6. Spear Phishing – sending an e-mail to a specific addressee (for example, a manager, administrator, user), which prompts him to make a mandatory view and replies to the received letter.

7. Whaling – sending an e-mail to a representative of the organization's management prompts him to make a mandatory review and replies to the received letter.

Obtaining unauthorized access to information (see table) with the help of phishing, pharming, smishing, vishing, spear phishing, whaling is carried out using such forms of manipulative influence as fraud and deception. Whereas the basis for creating fictitious situations when attaching is a scam, intrigue, mystification, and provocation.

Table – Forms of manipulative influence in socio-engineering attacks

№	Varieties of social engineering attacks	Forms of manipulative effects					
		Fraud	Deception	Scam	Intrigue	Hoax	Provocation
1.	Phishing	+	+	–	–	–	–
2.	Pharming	+	+	–	–	–	–
3.	Pretext	+	+	+	+	+	+
4.	Smishing	+	+	–	–	–	–
5.	Vishing	+	+	–	–	–	–
6.	Spear phishing	+	+	–	–	–	–
7.	Whaling	+	+	–	–	–	–

Therefore, when assessing the information security in computer systems by the socio-engineering approach, it is advisable to take into account the forms of manipulative influence.

Most social engineers operate using identical or cognate templates. This is why learning of their techniques allows identifying the following levels of interaction with the effect object: domination, manipulation, rivalry, partnership, and concord.

1. Social engineering techniques

All social engineering techniques can be divided into two groups [3] - [8]:

1. Remote social engineering is realized using the modern means of telecommunication:

1.1. Telephone

Using telephony features a social engineer may stay anonymous and have direct contact with the target object. The latter is important since the direct contact does not give an interlocutor a

chance to think over the situation and weigh all pros and cons. It is necessary to decide immediately and under the pressure of the social engineer. Since they exchange only audio information in the telephone conversation, to make a decision intonation and voice of the interlocutor are very important. These characteristics are selected in accordance with the behavioral model of the social engineer to obtain information on the effect object. For example:

1) boss – a person who is used to give orders, values his time and reaches out objectives. The conversation manner should be tough and impatient. Full confidence in himself and slight (or full) ignorance of non-management employees. The tone shows that the referred matter is a slight discrepancy that should be considered as soon as possible. No requests – only demands and orders. In response to suspicious and checking on words, only indignation and intimidation are possible.

2) secretary – a girl (in most cases) with a pleasant voice. The task is to fulfill a specific boss's errand sticking to business. She has information about her boss and some business of his and, on the side, drops true facts (or not true, which are impossible to check). The conversation is mild with a slight erotic implication (if interlocutor is a man). Reaction to reluctance to cooperate is a stormy regret and complaint that the boss would punish.

3) technical employee – an employee in the organization who is characterized as gracious and friendly to clients. The objective is very simple that of to fix troubleshooting and get both sides rid of a headache. It is underlined by a specific terminology competence. Reluctance to cooperate is met by surprise as cooperation is beneficial, primarily, for the client. No persuading, just showing that his reluctance may result in negative consequences.

4) user – an employee who fulfills his duties and is scared by an unexpected problem. A clear expressed motivation is to fix all problems as soon as possible and come back to routine duties. No awareness of the problem character, only interest to fix it. Character of communication: to show hopelessness of the situation and readiness to surrender to an expert.

1.2. Global Internet network

The most frequent social engineering techniques using the Internet are the following:

- carrying out social engineering via e-mailing;
- carrying out social engineering via the message exchange systems (Skype, Viber);
- social engineering at fora, in chats and blogs.
- successful realization of social engineering in those cases is stipulated by a correctly developed communication scenario.

2. Personal contact is the most labour consuming and dangerous social engineering technique. Beside above mentioned requirements to the communication scenario and behavioural model, a social engineer should pay proper attention to his appearance and manners of "in live" communication. For a proper visual perception it is necessary to correctly select the following:

- colours of clothes and shoes;
- manners and gestures during the conversation;
- communication distance.

Also, when using the social engineering techniques, it is necessary to characterize interlocutor. By voice or appearance it is necessary to find out his weakness and use it to reach out objective. The basic weaknesses of a person, which working jointly with properly selected behavioural model and conversation scenario allow reach out expected objective, are the following:

- credulity;
- fear;
- greed;
- sympathy;
- superiority;
- charity.

The main reasons of effect the social engineer object are: personal feeling of dignity, his aspiration to success, material benefits, getting satisfaction, comfort, wish to be healthy, having a well-to do and secured family.

Using the techniques of covered and direct manipulation of a person gives possibility to a social engineer to find out and use in the future this useful information for profit.

Conclusion. As a result, it becomes necessary not only to prevent, detect, account, and neutralize the root causes of emerging information vulnerabilities in computer systems and networks using the social engineering techniques, but also, firstly, ensuring its security in view of the requirements of the information security policy, secondly, establishment of the rules of conduct for the employees based on the job descriptions, thirdly, conduct trainings aimed at sustainability of stereotypes of the employees.

REFERENCE

[1] International Standards Office. *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements* [Online]. Available: https://www.iso.org/standard/54534.html.

[2] International Standards Office. *ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity* [Online]. Available: https://www.iso.org/standard/44375.html.

[3] P. Singh, "Robust Security System for Critical Computers", *International Journal of Computer Network and Information Security*, vol. 4, no. 6, pp. 24-29, 2012. doi: 10.5815/ijitcs.2012.06.04.

[4] V. Mokhor, O. Tsurkan, V. Tsurkan, and R. Herasymov, "Information Security Assessment of the Computer Systems by Socioengineering Approach", *Selected Papers of the XVII International Scientific and Practical Conference "Information Technologies and Security"*. Kyiv, 2017, pp. 1-6 [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf.

[5] S. Hasani, and N. Modiri, "Criteria Specifications for the Comparison and Evaluation of Access Control Models", *International Journal of Computer Network and Information Security*, vol. 5, no. 5, pp. 19-29, 2013. doi: 10.5815/ijcnis.2013.05.03.

[6] O. Tsurkan, and V. Mokhor, "Analysis of social engineering attacks on a person in cyberspace", *in Proc. 14th International conference: information technologies and security: principles of information security*. Kyiv, 2014, pp. 100-102.

[7] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", *Journal of information security and applications*, vol. 22, pp. 113-122, 2015. doi: 10.1016/j.jisa.2014.09.005.

[8] F. Mouton, L. Leenen, and H.Venter, "Social engineering attack examples, templates and scenarios", *Computers & Security*, vol. 59, pp. 186-209, 2016. doi: 10.1016/j.cose.2016.03.004

[9] W. Fan, K. Lwakatare, and R. Rong, "Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations", *International Journal of Computer Network and Information Security*, vol. 9, no.1, pp. 1-11, 2017. doi: 10.5815/ijcnis.2017.01.01.

The article was received September 16, 2018.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] International Standards Office. *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements* [Online]. Available: https://www.iso.org/standard/54534.html.

[2] International Standards Office. *ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity* [Online]. Available: https://www.iso.org/standard/44375.html.

[3] P. Singh, “Robust Security System for Critical Computers”, *International Journal of Computer Network and Information Security*, vol. 4, no. 6, pp. 24-29, 2012. doi: 10.5815/ijitcs.2012.06.04.

[4] В. Мохор, О. Цуркан, В. Цуркан, та Р. Герасимов, “Оцінювання захищеності інформації в комп’ютерних системах за соціоінженерним підходом”, *Selected Papers of the XVII International Scientific and Practical Conference “Information Technologies and Security”. Kyiv, 2017, pp. 1-6* [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf.

[5] S. Hasani, and N. Modiri, “Criteria Specifications for the Comparison and Evaluation of Access Control Models”, International Journal of Computer Network and Information Security, vol. 5, no. 5, pp. 19-29, 2013. doi: 10.5815/ijcnis.2013.05.03.

[6] О. Цуркан, та В. Мохор, “Аналіз соціоінженерних атак на людину в кіберпросторі”, на *14 Міжнародній конференції: інформаційні технології та безпека: принципи інформаційної безпеки*. Київ, 2014, с. 100-102.

[7] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks”, *Journal of information security and applications*, vol. 22, pp. 113-122, 2015. doi: 10.1016/j.jisa.2014.09.005.

[8] F. Mouton, L. Leenen, and H.Venter, “Social engineering attack examples, templates and scenarios”, *Computers & Security*, vol. 59, pp. 186-209, 2016. doi: 10.1016/j.cose.2016.03.004

[9] W. Fan, K. Lwakatare, and R. Rong, “Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations”, *International Journal of Computer Network and Information Security*, vol. 9, no.1, pp. 1-11, 2017. doi: 10.5815/ijcnis.2017.01.01.

ОКСАНА ЦУРКАН,
РОСТИСЛАВ ГЕРАСИМОВ,

ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ КОМП’ЮТЕРНИХ СИСТЕМ І МЕРЕЖ МЕТОДАМИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Захист інформації в комп’ютерних системах і мережах орієнтований на збереження її властивостей конфіденційності, цілісності та доступності від різноманітних за своєю сутністю несприятливих впливів. Потенційно можливі несприятливі впливи тлумачаться як загроза. Для запобігання або ускладнення можливості реалізацій загроз, зменшення потенційних збитків створюється та підтримується у дієздатному стані система заходів захисту інформації. Така система включає обчислювальну систему, фізичне середовище, персонал та інформацію. Одним із найбільш уразливих елементів такої системи є персонал. У рамках соціоінженерного підходу вразливості персоналу тлумачаться як його слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації без руйнування та перекручування головних для нього системоутворюючих якостей. Це відображається в таких формах як шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передує визначення її змісту шляхом ретельного планування, організування та контролювання. Означені дії є основою методів соціальної інженерії. Їх використання орієнтовано на імітування дій порушника інформаційної безпеки, що направлені на персонал. Це дозволяє оцінити рівень кваліфікації персоналу в області забезпечення інформаційної безпеки та, як наслідок, виявити вразливості інформації в комп’ютерних системах і мережах. Методи соціальної інженерії, що використовуються для цього, поділяються на дві групи. Зокрема, віддаленої соціальної інженерії та особистого контакту. Методи віддаленої соціальної інженерії реалізуються засобами сучасних телекомунікацій. Крім цього, друга група методів передбачає встановлення особистого контакту з об’єктом впливу. В кінцевому випадку, стає можливим не тільки вплив, нейтралізування, але й

запобігання уразливостям інформації в комп'ютерних системах і компонентах з використанням методів соціальної інженерії. Як наслідок, по-перше, забезпечується її захист з урахуванням вимог політики інформаційної безпеки; по-друге, встановлюються правила поведінки персоналу, що регламентуються посадовими інструкціями; по-третє, проводяться тренінги, що направлені на підвищення стікості стереотипів персоналу в організації.

Ключові слова: уразливість, комп'ютерні системи та компоненти, модель поведінки, соціальна інженерія, методи соціальної інеженерії.

ОКСАНА ЦУРКАН,
РОСТИСЛАВ ГЕРАСИМОВ,

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ КОМПЪЮТЕРНЫХ СИСТЕМ И СЕТЕЙ МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Защита информации в компъютерных системах и сетях ориентирована на сохранение ее свойств конфиденциальности, целосности и доступности от разнообразных по своей сути неблагоприятных влияний. Потенциально возможные неблагоприятные влияния толкуются как угроза. Для предотвращения или усложнения возможности реализации угроз, уменьшения потенциальных убытков создается и поддерживается в дееспособном состоянии система мероприятий защиты информации. Такая система включает вычеслительную систему, физическую среду, персонал и информаци. Одним из наиболее уязвимых елементов такой системы является персонал. В рамках социоинженерного подхода уязвимости персонала толкуются как его слабости, потребности, мании (пристрастия), увлечения. Манипулируя ними позволяет получить несанкционированые доступ к информации без разрушения и перекручивания главных для него системообразующих качеств. Это отображается в таких формах как мошенничество, обман, афера, интрига, мистификация, провокация. Использованию каждой из этих форм манипулирования предшедствует определение ее сущьности путем тщательного планирования, организации и контроля. Данные действия являются основой методов социальной инженерии. Их использование ориентировано на имитацию действий нарушителя информационной безопасности, которые направленны на перснал. Это позволяет оценить уровень квалификации персонала в области обеспечения информационной безопасности и, как следствие, выявить уязвимости информации в компьютерных системах и сетях. Используемые для этого методы социальной инженерии делятся на две группы, в частности, удаленной социальной инженерии и личного контакта. Методы удаленной социальной инженерии реализуется средствами современных телекоммуникаций. Кроме этого вторая группа методов предполагает установление личного контакта с объектом влияния. В конечном итоге, становится возможным не только выявление, нейтрализация, но и предотвращение уязвимостей информации в компьютерных системах и сетях с использованием методов социальной инженерии. Следовательно, во-первых, обеспечивается ее защита с учетом требований политики информационной безопасности; во-вторых, устанавливаются правила поведения персонала, регламентированные должностными инструкциями; в-третьих, проводятся тренинги направленные на повышение стойкости стереотипов сотрудников организации.

Ключевые слова: уязвимость, компъютерные системы и компоненты, модель поведения, социальная инженерия, методы социальной инеженерии.

Oksana Tsurkan, senior engineer, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
ORCID: 0000-0002-5524-8834.
E-mail: o.tsurkan24@gmail.com.
Rostyslav Herasymov, researcher, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
ORCID: 0000-0002-4115-8344.
E-mail: gerasimov.rostislav@gmail.com.

Оксана Володимирівна Цуркан, провідний інженер, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Ростислав Павлович Герасмов, науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Оксана Владимировна Цуркан, ведущий инженер, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Ростислав Павлович Герасимов, научный сотрудник, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.