Georgian Scientists

ქართველი მეცნიერები

Vol. 5 Issue 4, 2023

https://doi.org/10.52340/gs.2023.05.04.05

Planning and Automation of Information Security Awareness Training

Samkharadze Roman[1], Kiknadze Mzia[1], Sakhvadze Giorgi[2], Gachechiladze Lia[2], Acharadze Guram[2]

[1]Business and Technology University, Georgia, Tbilisi

[2]Department of Software Engineering, Georgian Technical University

Abstract

As is known, the goal of information security is to protect the confidentiality, integrity, and availability of information. Information security consists of three directions: confidentiality, integrity, and availability. Proper operation of these three directions ensures high information security in organizations.

In the article, an information security awareness training scheme for corporate networks is developed. Issues of its planning and automation are presented. A mechanism for conducting awareness training has been developed, which increases the general level of information security, which directly affects the process of safe data transfer. The necessity and importance of awareness raising training is justified and the ways of its implementation are suggested. Means of identifying types of attacks and ways to deal with them have been developed through awareness raising.

Keywords: information security, awareness training

The dependence of the successful activity of the organization on the corporate information security system is increasing every day. All this is caused by the increase in the volume of vital data processed in the corporate information system. Information systems are becoming more complex and the level of vulnerabilities found in them is also increasing. There is more than one way to detect vulnerabilities. They provide information on what kind of vulnerabilities exist on the systems and devices in the corporate network and how to fix them. This, on the one hand, helps the corporate network to have a high level of protection and, on the other hand, to improve and perfect its systems as much as possible through updates.

Security awareness and training activities involving the information security team should begin as soon as possible after personnel join the corporate network. Awareness-raising activities should then be continued at regular intervals to maintain a reasonable level of awareness.

Awareness can be raised in several ways [1]:

a. Provide the desired information to the employees by e-mail;

b. Make a presentation and make the employee more involved directly in the process;
c. Continuously provide information on global cyber-attacks in which human factors have been used;
d. Let the staff know about threats coming from social networks;
e. Continuously conduct tests to determine their readiness for the current challenges. The best practice is to use all these components regularly.

Human psychology must be taken into account in the process of raising awareness. When we try to provide information to a person, it is necessary to protect the golden mean so that there is no negative effect. If we provide a person with a lot of information at once, then the process of his perception, understanding, and learning will not be as efficient as when it is provided gradually. If organizations use such a platform that allows them to analyze the information about the effectiveness of the conducted tests and introduced news, then it will be much more fruitful to raise the awareness of the staff. In this process, some important points are highlighted, how and in what form we provide information to employees.

It is also important to prioritize this information as to which components are most important to raising awareness and which are less important. After determining the priorities, each component should be described in the program with a percentage that replaces the corresponding priority. After that, a test plan should be drawn up. Since most of the potential email attacks come from phishing, take advantage of this opportunity to send phishing emails to your employees. This will reveal how effective the use of existing training methods was for employees.

This process should be repeated several times during the year, and the results should be summarized and analyzed at the end of the year. It should be determined how much the threat decreased from the first test letter to the last test letter. Based on the current results, the next year should be planned, and this year, the number of priorities and important information should be adjusted to achieve higher efficiency compared to the previous year.

The best practice to combat insider threats is awareness. Raising awareness is possible through training, but a one-time training will not give us the best results. For this, it is necessary to plan the training and analyze all the components that are related to the training. The most important issue after conducting an awareness-raising course is the analysis of the results. Analysis helps organizations determine future actions. For example, if an introductory presentation was held as part of the awareness-raising course, it should be described in the corresponding program and assigned a corresponding priority, or the program should be able to do all this automatically. All actions taken should also be prioritized.

In general, the awareness-raising course includes three main directions:
a. Providing materials and introducing news to employees.
b. Conduct presentations and communicate directly with employees discussing cybersecurity news, challenges, and importance.
c. After the delivery of the material and the presentation, check the material's assimilation and knowledge. Knowledge testing is mainly done by sending phishing letters to e-mail, within the framework of which employees are checked to what extent they will go to the existing "infected" link.

The course is divided into two parts: in the first case, during the recruitment period, the employee is introduced to information, taught, and tested. In the second case, the above-mentioned actions of the

employee are already being analyzed. The frequency of training, testing, and delivery of materials during the year is determined by the program. Based on the entered data, the program automatically calculates the desired schedule and frequency for each employee [2].

The analytics module involves showing the advantages of three main directions. In our case, the initial data is provided to the program:

a. Getting to know the materials - priority 25%;

b. Conducting a presentation - priority 30%.

c. Exam - priority 45 %.

The employee who will pass this course must have a final result of at least 80%. For the awareness-raising course to be fruitful, it is necessary to introduce control mechanisms. This implies the involvement of the department manager in familiarization with the material, which confirms that the employees under his authority have received the existing materials and are familiar with them. During the presentation, a security engineer enters as a controller, whose duty it is to record the employees, to whom the presentation was made when, and what level of attendance it was. This can be viewed through the program, where the activity of employees is automatically noted. As with the presentation, during the exam, the security officer is the controller, whose duty it is to deliver phishing emails to all employees.

Data are generally measured every six months or at the end of the year by the program. After six months, the materials used during the three main directions can be changed. These will be introductory materials, presentation materials, and an email form to be sent during the exam. At the end of the year, it is necessary to summarize the events that happened during the year. The ability of employees to use the materials provided will be revealed and the next year's action plan will be planned.

It is necessary to analyze the issues that caused negative results for most of the employees. The mentioned issues will be displayed on a separate page by the program in terms of quantity and percentage. After that, mistakes made by employees should be analyzed and special attention should be paid to these components in the next year.

The security team should adjust each component with the help of the program with the results obtained during the year. Based on the modern challenges, the security engineer should determine if any direction has become a higher priority and accordingly make a percentage change of its priority in the program. The program automatically provides decision generation. Based on the results, he decides to increase or decrease the amount of work to be carried out.

The schedule that provides the company with information on the actions taken by the employees is drawn up by the program itself. When sending phishing e-mails, the e-mail must be properly composed. The components that were directly discussed during the training should be taken into account when compiling. If the employee of the company does not carefully observe the said letter, then he will not notice and will not be able to identify the real and fake addresses of the sender.

In awareness training, the greatest importance is given to the program itself and to the decision by means of which information is provided to employees, including training videos and phishing emails. The program itself should analyze all the components that directly determine the level of knowledge of employees.

It is desirable to allocate a special storage where all the text, graphics, audio, and video materials that should be provided to the employee will be placed. This storage should be connected to the program as an additional device, and employees should be connected to the necessary materials directly through the program.

Each employee must register and be assigned an individual username and password so that the program can identify those employees. The best option would be if the employees are authorized through e-mail. But we must not forget the main principles of security and a different password must be used when accessing the program. It should also be changed periodically to avoid as much as possible all dangers of unauthorized access.

After the program ensures that employees have access to the necessary materials, it will be able to analyze which, employee has been introduced to a particular material and determine the next materials to be introduced. This will allow the members of the information security team to provide the necessary material to the employee once he has registered.

It is necessary that awareness training, training materials, and exercises are adapted to the audience in terms of style, format, difficulty, and technical content. Everyone should know why information security is so important, but the motivations may vary.

The organization shall provide personnel with information on the location of security awareness training materials, security policies, standards, and guidance. Also, to introduce all procedures related to information security issues.

The organization's information security department should require that each employee undergo training no later than one month after being hired. Also every year complete information security training. Some employees may be required to complete additional training modules depending on the specific requirements of the job. Staff should be given a reasonable amount of time to complete each module so as not to disrupt the organization's operations.

The security department itself should determine the frequency schedule of the procedures to be carried out throughout the year. They can pre-target a specific department or employee with a special attack based on risk determination.

From time to time, employees may be required to attend remediation training courses or directly participate in remediation activities with information security staff.

Compliance with this procedure is mandatory for all employees of the organization. The information security department of the organization should monitor the implementation of this policy. Also, report the results of training and social engineering exercises to the executive team. In case of non-compliance, a separate annex should be signed, where appropriate punitive actions will be described, be it a fine or a reprimand.

Certain actions or inactions of the organization's employees may cause awareness training to fail. This can happen for the following reasons [3]:

a. Failure to complete the proposed training within the designated time frame;

b. Failing social engineering exercises.

Failing social engineering exercises include:

a. Clicking on a URL as part of a phishing test;

b. Respond to any information during the phishing test;
c. Opening an application that is part of a phishing test.
According to this policy, it is necessary to define responsible and accountable persons. These individuals should include the information security officer/manager responsible for implementing the training program, as well as the information security management representative responsible for developing and maintaining this policy. He is also required to provide appropriate information to the security team and conduct training and educational activities to increase staff awareness and responsibility [4].
All department managers are responsible for ensuring that their subordinates participate in awareness training and educational activities when appropriate.
There is a database where a list of employees with official e-mails is recorded. The database has direct access to training materials, that is, employees are directly connected to the materials to be studied within the training. The program evaluates the passed material according to the percentage of how much material this or that employee has learned. If the employee answers more than 80% of the questions correctly, then his test result is positive and he goes to the next level. If it is negative, then it is returned to the teaching materials so that the materials that were evaluated negatively during the testing are passed again. The program itself determines which module to add to a specific employee to make his level of knowledge satisfactory.
After testing, the program will automatically determine when a phishing email will be sent to an employee and will find out his knowledge level in a real environment. In this case, there are two options. The result is positive if the employee does not go to the fake web page and takes into account the material used in the awareness modules. The result will be negative if the employee goes to a fake web page. After detecting a negative result, the program re-sends the modules that describe the detection of phishing emails and the necessary actions to protect personal information. If the employee successfully passes the phishing test as well, this completes one phase of awareness training and the program moves such an employee to a separate pool of employees who have successfully passed the test. The program sends phishing emails to such employees several times a year. Depending on the results, it either gives access to training modules or leaves it in the base where there are employees with positive results [5, 6].

Thus, the article proposes a mechanism for conducting awareness training, which increases the general level of information security, which directly affects the process of securely transferring data. The necessity and importance of awareness raising training is justified and the ways of its implementation are suggested. Means of identifying types of attacks and ways to deal with them have been developed through awareness raising.

References:

Sakhvadze G., Samkharadze R., Kiknadze M., Gachechiladze L. Planning and automation of information security awareness training. Georgian Technical University. Faculty of Business Technologies. Government and society. Tbilisi. XVI International Scientific Conference. Publishing House "Technical University", 2022. ISBN 978-9941-28-289-7. 276 – 283 p.

Sakhvadze G., Samkharadze R. SECURE TRANSFER OF INFORMATION WITHIN THE INTERNAL NETWORK OF THE ORGANIZATION. International Scientific and Practical Conference "CURRENT ISSUES OF SCIENCE AND INTEGRATED TECHNOLOGIES". Milan, Italy. January 10 – 13, 2023. ISBN – 979-8-88862-816-4 DOI – 10.46299/ISG.2023.1.1. 627-630 p.

Sakhvadze G., Samkharadze R., Kiknadze M. Critical analysis of human factor cyber-attacks. Georgian Technical University. Faculty of Business Technologies. From a series of monographs. Globalization and modern business challenges. Tbilisi. VI International Scientific Conference. Publishing House "Technical University", 2022. ISBN 978-9941-28-127-3. 286-290 p.

Zhamurashvili K., Samkharadze R., Gachechiladze L. Development of security norms for electronic payment systems (monograph). "IT-Consulting Scientific Center" of GTU, 2019. p. 70.

Zhamurashvili K., Samkharadze R. Information systems security infrastructure planning. Tbilisi, "Georgian Technical University". Works. Automated Control Systems. N1(21). 2016. p. 62-65.

Zhamurashvili K., Samkharadze R. Modern cryptographic methods. Tbilisi, "Georgian Technical University". Works. Automated Control Systems. N1(21). 2016. p. 66-70.

ინფორმაციის უსაფრთხოების ტრენინგის დაგეგმვა და ავტომატიზაცია

სამხარაძე რომანი[1], კიკნაძე მზია[1], სახვაძე გიორგი[2], გაჩეჩილაძე ლია[2], აჩარაძე გურამი[2]

[1]ბიზნესისა და ტექნოლოგიების უნივერსიტეტი, თბილისი, საქართველო

პროგრამული ინჟინერიის დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი

აბსტრაქტი

როგორც ცნობილია, ინფორმაციის უსაფრთხოების მიზანია ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა. ინფორმაციის უსაფრთხოება შედგება სამი მიმართულებისგან: კონფიდენციალურობა, მთლიანობა და ხელმისაწვდომობა. ამ სამი მიმართულების გამართული ფუნქციონირება უზრუნველყოფს ორგანიზაციებში მაღალ ინფორმაციულ უსაფრთხოებას.

სტატიაში შემუშავებულია, ინფორმაციული უსაფრთხოების ცნობიერების ამაღლების ტრენინგის სქემა კორპორატიულ ქსელისთვის. წარმოდგენილია მისი დაგეგმვის და ავტომატიზაციის საკითხები. შემუშავებულია ცნობიერების ამაღლების ტრენინგის ჩატარების მექანიზმი, რომელიც ზრდის ინფორმაციული უსაფრთხოების ზოგად დონეს, რაც უშუალოდ აისახება მონაცემების უსაფრთხოდ გადაცემის პროცესზე. დასაბუთებულია ცნობიერების ამაღლების ტრენინგის ჩატარების აუცილებლობა, მნიშვნელობა და შემოთავაზებულია მისი ჩატარების გზები. შემუშავებულია ცნობიერების ამაღლების გზით შეტევის ტიპების ამოცნობის საშუალებები და მათთან გამკლავების გზები.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება, ცნობიერების ტრენინგი, ცნობიერების ამაღლება