The Elimination of Human Factor and its Effects in Corrupting Security

Natalia Lukova-Chuiko, Volodymyr Nakonechnyi, Anastasiia Petrenko and Anna Kyrylenko

Abstract

Security is one of the greatest concerns for organizations in the whole world regardless of its scale. This is so because intruders never sleep and try to compromise organizations security many times in a variety of ways. At first, the increase in hacker campaigns has led to new solutions focused on technology tools, while research related to the human factor has been limited. Eventually, the focus of building cybersecurity shifts to people since 95% of all security incidents occur through human error rather than due to targeted attacks. No matter how many technologies are dedicated to ensuring security, how much money companies spend on security, the weakest point in any system is human – and it is impossible to make people do/don't perform specific actions because of their essence. The purpose of the article is to outline the aspects of the human factor being the main reason for security breaches and to suggest general ways of improving the safeguard level of enterprises by creating new cybersecurity awareness programs to educate each employee and help information security administrators have correct and clear configuration.

Keywords [1]

Security, human factor, threats, misconfigurations, cybersecurity awareness

1. Introduction

Increased threats to information technology have led to new solutions focused on technology tools, while research related to the human factor has been limited. Organizations often ignore the human factor. Security research from Cisco Systems found that users who work remotely will still engage in activities that threaten security. A study of employee behavior showed that upon receiving a suspicious email, 37% will not only open the email but follow the link, while 13% will open the attached file. In addition, after receiving a regular email, 42% clicked on a link and provided confidential information, and 30% opened a file that would supposedly improve computer performance.

A survey was conducted by Cisco among security professionals and IT departments to identify their top priorities over the next several months.

About 44% of respondents said their IT departments and security professionals spent less than 20% of their time on day-to-day operational security. Another 32% said they devoted 20 to 40 percent of their time to safety. Only 20% of participants dedicated a significant portion of their daily and weekly administrative activities to securing their systems and networks (see Figure 1).

Among security software, there are firewalls, antiviruses, intrusion detection systems, data governance systems etc., each of which performs specific functions and is aimed at solving specific tasks. However, we can use the best software, which uses the most advanced technologies, cryptographic algorithms, but at the same time, we cannot be 100% sure that our system is invulnerable. Because people are involved in the implementation of all decisions and their application in practice, and people tend to make mistakes. A person, being a part of the system, was and remains the most vulnerable spot in the security system [1]. For paragraph, use Normal. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text.

Information Technology and Implementation (IT&I-2021), December 01–03, 2021, Kyiv, Ukraine

EMAIL: lukova@ukr.net (N. Lukova-Chuiko); nvc2006@i.ua (V. Nakonechnyi); petrenkoa@fit.knu.ua (A. Petrenko); kyrylenkoa@fit.knu.ua (A. Kyrylenko);

ORCID: 0000-0003-3224-4061 (N. Lukova-Chuiko); 0000-0002-0247-5400 (V. Nakonechnyi); 0000-0002-4713-8125 (A. Petrenko); 0000-0002-5532-0023 (A. Kyrylenko)

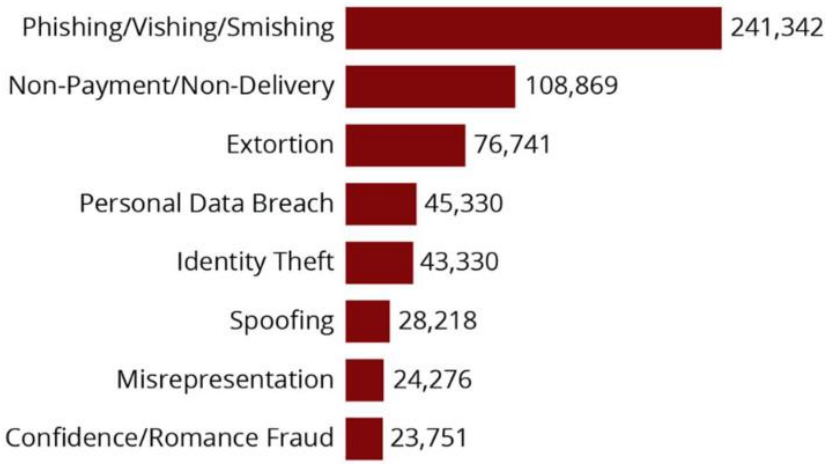

Figure 1: Common types of cyberattacks in 2020

The human factor is the reason for the success of many attacks, and many examples prove this hypothesis.

2. Current situation in the world

Last years the whole world has faced many challenges. The global lockdown hit most technology industries, including information security. Robust data protection remains a daily business challenge. A side effect of the pandemic was a huge increase in the number of hacker attacks on databases. Recent research shows that most companies do not care about proper security and do not pay attention to the issue of information security at all [2].

2.1. Loudest security incidents caused by human factor

The above-mentioned statistics leave no doubt that at the moment the human factor is one of the main risk factors in terms of information security. “As the recent foreign incidents in the oil industry show, the human factor can negate almost all efforts to protect the infrastructure,” says Sergey Khalyapin, chief engineer of the Russian representative office of Citrix. “The more opportunities for ‘outsiders’ to communicate with employees of the company, the higher the risk of losing information or breaching the security system” [3]. On January 12 due to an error in the configuration of the cloud storage, social media management firm Socialarks made public the data of at least 214 million users, including celebrities. During a routine scan of IP addresses, a team of researchers came across a 408-gigabyte Elasticsearch database that was neither password-protected nor encrypted. The database consisted of 318 million records that were illegally collected from user profiles on LinkedIn, Instagram and Facebook [4]. On August 12, the Lithuanian Ministry of Foreign Affairs reported a "spoofing attack". According to representatives of the Ministry of Foreign Affairs, during the attack, the hackers sent letters from the department's e-mail address. Messages with a request to provide personal confidential documents were received not only by private individuals but also by some state institutions of the country [5]. Security has always been the greatest concern for each company regardless of its scale and remains to be. The reason is simple: intruders never sleep and try to compromise organizations security each time with various approaches. Ensuring security is a continuous process and in general consists of several steps.

2.2. Classification of threats

The information infrastructure of an enterprise is constantly exposed to numerous threats, which by their origin is divided into several types and are represented in the Figure 2:

- Natural - threats caused by causes beyond human control. These include hurricanes, fires, lightning strikes, floods, and other natural disasters

- Artificial - a complex of human-created information security threats. Man-made threats, in turn, are divided into intentional and unintentional. Intentional threats include the actions of competitors, hacker attacks, sabotage of offended employees, etc. Unintentional threats arise as a result of actions committed due to lack of competence or through negligence
- Internal - threats that arise within the information infrastructure of the enterprise
- External - threats that originate outside the information infrastructure of the enterprise

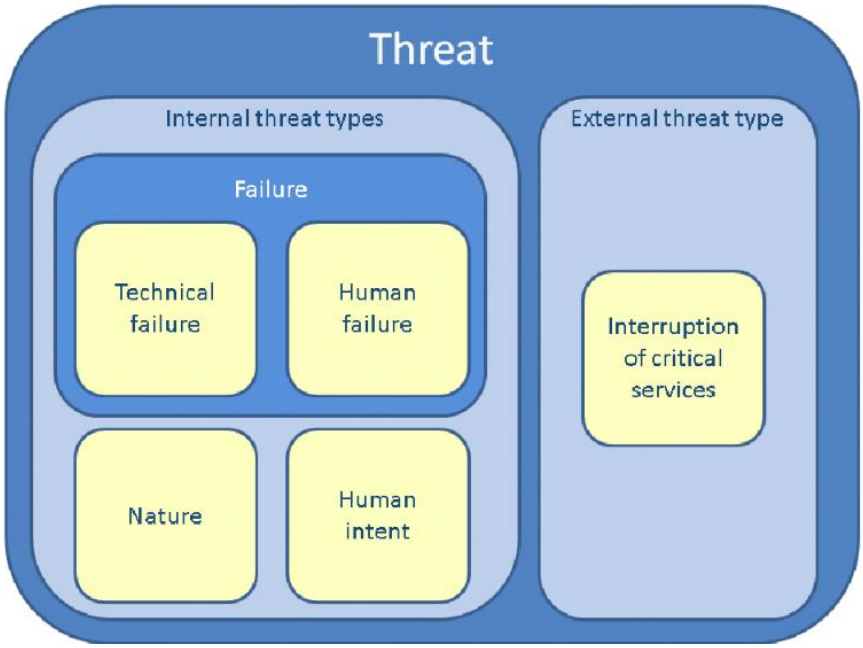

Figure 2: Example figure

At this step, they use SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing), implement SIEM systems, apply IDS/IPS (Intrusion Detection/Prevention System) to their infrastructure and many other tools to secure their data at each level of data flow – from physical to application. On media, we often hear that a company has announced a tender on applying the new tool to increase the level of security. Eventually, the cost is the decisive factor and many other options are considered less important. In that way, companies try to win by quantity, but they have forgotten about the most vulnerable item in the system – human

2.3. Characteristics of human factor and errors

It doesn't matter how many technologies are included in ensuring security, how much funds companies spend on security, the weakest point in any system is human – and it is impossible to make people do/don't perform specific actions because of their essence.

The system cannot check that person who gives the credentials is the owner of them, it only checks that they match the expected input. In that case, the intruder gets access to internal infrastructure without detecting the monitoring system (it perceives him as an authorized user).

That's why we are not able to fully eliminate security threats associated with human factors by technologies. It can only be done by educating the employees and checking their level of awareness. It's a common fact that the effectiveness of studying the courses is not compatible with resources spent on creating, maintaining, and reviewing these training. Human and organizational factors can be related to technical information security. The factors affecting the security of a computer are divided into two categories, namely the human factor and the organizational factor. Human factors are more important than other factors. They are divided into the following groups: factors that relate to management, namely workload and poor performance of staff; end-user factors. Next, we'll focus on four human factors that have significant implications for influencing userbehavior [6]:

1. Lack of motivation. Many organizations believe that employees need to be motivated to behave safely with information assets, and management must be able to determine what motivates their personnel

2. Lack of awareness. The lack of awareness stems from a lack of general knowledge about attacks. Common examples of lack of awareness include the following: Users do not know how to identify spyware and spyware and how important it is to enter a strong password. They cannot protect themselves from identity theft, nor how to control other users' access to their computers

3. Belief. Common examples of risky persuasion are that users believe that installing antivirus software solves their security concerns

4. Illiterate the use of technology. Even the best technology cannot succeed in solving information security problems without continuous human cooperation and effective use of this technology. Common examples of inappropriate use of technology include: creating unauthorized reconfiguration of systems, accessing the passwords of others, obtaining invalid information. Computer security risks can be classified in several ways: abuse of privilege, errors and omissions, denial of service, social engineering, unauthorized access, identity theft, phishing, malware, and unauthorized copies

2.4. Signs of the issue

Estimates from various analytical companies and information security experts indicate that about half of incidents in the field of data protection are associated with the activities of insiders. Analytical center Falcongaze has prepared a list of signs that the company should attend to the issue of protection from information leaks. Let's give it:

1. Lack of corporate security policy
2. High staff turnover and frequent layoffs
3. Uncontrolled use of messengers, email, social networks by employees
4. The presence of employees who spend a lot of time on business trips and business trips
5. Uncontrolled document flow, as a result of which anyone can get access to confidential information

There are other signs that not enough attention has been paid to protection against information leaks, but according to Falcongaze, if at least one of these points is true for your company, it definitely falls into the risk group.

2.5. Minimizing the risks

In 2017, cyber security experts noted the increased interest of cyber fraudsters and insiders in industrial companies. The trend will only intensify, because the informatization of industrial facilities is gaining momentum, and even strong security services will be forced to build up the capacity of protective equipment in order to be ready to repel new types of threats.

How to minimize the influence of the human factor on the information security of an organization? Specialists determine three aspects to the solution to this problem [7]:

1. Formation and regular updating of the list of information and powers that are minimally necessary for the user to perform their duties

As a rule, in the process of working in an organization, a user begins to have more privileges than is necessary to perform his duties. As a result of compromising the account of such a user, the attacker gains significantly more opportunities for illegal actions than the "security" would like. Recipe: The set of rights and privileges for each functional role in the organization should be at the "Need-to-know" level and no more. This kit should be audited annually.

2. Teaching users the basics of information security

This is the most problematic aspect, it is tied to the corporate culture of the organization, the maturity of information security processes, the selection of appropriate communication tools for each user group. At the same time, it is not enough to convey to users the information security policy in a form that is understandable to them, it is necessary to motivate them to implement it. Here I would like to mention the example of Salesforce and the approach of its information security team to changing the

user behaviour model through the introduction of competitive elements (the so-called gamification). This program covered 14 thousand employees of the organization. Based on its results, a survey was conducted, and more than half of the participants said that they were less likely to click on a suspicious link, and more than 80% were more likely to report suspicious activity to the information security service. Recipe: Implementation of a comprehensive training program for personnel, which includes:

- Focus on common attacks that are easiest to stop at the user level
- Submitting material through short, user-friendly online courses, keeping information on attacks up-to-date
- Mandatory fulfilment of the program requirements by all employees of the organization, including top management
- Monitoring the progress of training
- Support of training by top management

3. Minimization of the "zoo" in information security systems, getting rid of disparate legacy solutions and focusing on consolidated information security systems with centralized management

The operation of many separate products responsible for performing various information security tasks increases the likelihood of conflicts between various means, unintentional errors in the configuration of products, and also significantly lengthens the period for their correction. Recipe: The maximum possible consolidation of products from one manufacturer with a centralized management and monitoring system. For example, a single product should be responsible for all endpoint security functions and should be as easy to manage as possible.

3. Security misconfigurations

The pillar of network security is firewall systems but even though it doesn`t guarantee the proper level of access control. This is not because of technical competency lack but rather the heart of the matter is the human factor. Laziness is a well-known problem when dealing with the administration field. Therefore, it leads to security misconfigurations, which in particular can result in data breaches and so on. This is just one particular use case but it should be also discussed in detail.

If we dig in technical details of the network use case of security misconfiguration - not a properly managed process of changing security rules and policies. Moreover, when an access rule on the firewall is being changed there must be an analysis of risks associated with it. And none of this is usually have done ever [8]. Security misconfiguration is on the 6th place in OWASP TOP 10 Vulnerabilities along with broken access control and cross-site scripting. This vulnerability is caused by the human factor as well.The attack vector aims to gain access to default accounts, unused pages, unprotected files and directories, etc. in order to gain unauthorized access to the system. Such flaws often give attackers unauthorized access to some system data or functions. Sometimes such flaws lead to a complete system crash. This vulnerability can greatly affect the reputation of the organization, therefore it is better not to have it and find a way of mitigation

Administrators are people too, and as ordinary workers, they need training and regular audits of the settings for non-compliance with the particular company security standards. A good base for firewall security is the NIST standard, DISA STIGs and CIS benchmarks. Firewall assurance ensures the state of your network is always in line with security policy design and helps reduce risks on firewalls themselves. A firewall is a typical network security solution and its incorrect settings can lead to an information security incident. This can relate to both general configurations and inaccuracies in the logic of the operation of its access policies. For example, weak passwords on the default user interface can make life much easier for an attacker. Or, on the other hand, insufficiently prohibitive rules can allow the passage of potentially malicious traffic, which in turn can lead to unauthorized access and subsequent financial loss and/or data compromise.

If the procedure for making changes in configurations is not established, then any systems will become unusable, because technical solutions also need supervision, especially focusing on the control of human oversight. Therefore, the first remedy will be a well-established change process, and this can help ITSM – in other words, IT Service Management. ITSM is an approach to the provision of IT services in which performers, processes and technologies are used in an optimal combination. ITSM

helps to improve business efficiency and the quality of provided IT services, as well as accounting and control over changes made by administrators in their information systems. The problem here is that an employee can make a mistake in the settings, or apply a potentially unsafe configuration, and if the above method is implemented, there will always be at least one responsible person from the security side who will check and agree on the admissibility of such changes and the risks associated with them for business-critical systems and processes of the company [9].

In addition, not every setting is as safe as it is easy to use. But as an administrator to understand what is permissible and what is not, how it should be so as not to lead to sad consequences. In this situation, it will help to draw up a document on security provisions for various technical solutions under the guidance of the company's security policy. Do not underestimate the strength of the documents, since, in cases of written requirements for the security of systems, the administrator has not only concise instructions and a framework for actions, but can also be brought to disciplinary action in cases of failure to comply with. Also, any rules and regulations are followed only when they can be verified. Therefore, it isnecessary to carry out regular checks of both the security of the settings and their appropriateness. An audit of a company's information security is a complex analytical work to assess the current state of its information systems and search for potential threats. To conduct the analysis, specialists have a list of criteria and standards that your system must comply with. If it has deviations or vulnerabilities, then you urgently need to take action. It is important to conduct an audit well in advance when the problem is at a threat stage [10].

IS audit has a specific list of "step-by-step" tasks:

- Analyze the current level of protection of personal data
- Assess information security in accordance with generally accepted standards
- Determine the likely risks for automated systems
- Identify weaknesses with the possibility of their elimination in the future
- Generate a report for information security specialists

Regardless of the scope of the enterprise, its type, tasks and goals, information security audit often affects the following operational aspects:

- Workers' rights to access servers and databases for collective use
- Ways to confirm the login of each user (authentication)
- Principles of data backup
- Configuration and settings of network devices, storage systems and data transmission
- Operation of antivirus and antispyware software, availability of a license
- Theoretical and practical knowledge of the company's employees about data protection

As a result, a comprehensive audit of the organization's information security will help to reveal how effective a system of protecting personal and corporate data is. If it has no weaknesses, the team will receive confirmation of the security of the entire organization. But if the report reveals hidden risks, then the team need to develop and implement an action plan to eliminate potential risks. In addition, high-quality analytics will help the company choose the most effective data protection methods and reduce its costs in this area. Workshops and other training programs on various technical solutions, with an emphasis on ensuring the security of these systems, can also be a good tool. Since often a person makes a mistake due to ignorance and misunderstanding of what their actions affect.

Although at first glance it seems that secure infrastructure design has nothing to do with the human factor, this is fundamentally not the case. There is no such solution that would draw a logical diagram for a person, taking into account all the nuances of a specific production and safety aspects. And if something is done by a person, it is always error-prone and requires supervision from above

4. Cybersecurity awareness

Over time, the focus of building cybersecurity shifts to people, not technology, as 95% of all security incidents occur through human error, not incidents [11]. Medium-sized companies and organizations spend an average of about $ 300,000 a year on information security training alone (according to Gartner), excluding various education activities [12]. However, even these efforts are not enough to achieve the desired level of security, which would protect as much as possible from the disclosure/theft of information and compliance with the selected level of standards. The reason is simple – people forget

70% of received information within 24 hours without proper attention from the management side and rechecking their understanding of materials [13].

Any mistake costs the company profit, resources (human, time, production - whatever) and, of course, nerves. Quality, security, IT infrastructure, reputation - an incomplete list of vulnerable aspects that can significantly suffer from a turned-off switch, a bug in the software, errors in Excel spreadsheets (except for jokes, for example, during a tender or calculating the profitability of a tariff, product, etc.). One human error - and processes, projects and whole months of work go down the drain. But it is human nature to make mistakes, and sooner or later the person will make mistakes. This means that only one thing remains - to learn how to minimize the influence of the human factor [14].

Such a problem can be applied for everyone – people are the triggers of actions, there are people at the service desk, management is also a common people, people deliver the equipment and check the physical security – everything is about people. So that's why increasing cybersecurity awareness is a crucial part of the organizations, especially international companies, which must comply with several regular standards and requirements are quite high.

It has become very challenging – how to teach everyone to be secure in the environment in an effective manner, track this progress and have a high ROI (Return on Investments). The new solution is to focus on an individual automation approach for each employee, monitor their activity, actions, and that's why covering as much as possible from the perspective of humans as the vulnerable item. It is proposed to use a new service that supports automatic individual evaluation of human compliance, checking their actions when they become a target of any attack.
Data used and/or data schemes:

- Results of the cyber assessment of the company
- Personal data of employees for accounts
- User activity in the network and the state of workstations
- Report on compliance of user actions with the company's requirements.

As for supported services, it can be added assessment of the company's cybersecurity and identification of places that need attention (optional); checking the condition of workstations for compliance with the requirements set by the company; defining activities for a specific employee to eliminate identified problems; providing courses, sending daily recommendations and creating simulated attacks to raise awareness and check regularly; sending employee cyber awareness profiles to managers for reporting. The process can be displayed in the figure below (Figure 3).

Although each of the phrases is already known to practice, in the bunch, they provide the client with an even greater solution. Benefits are the following: the individual approach is the milestone: people are different and it is not a promising idea to educate them in one way, but creating each learning path manually is time-consuming (variables, conditions are mutable and there is no advantage in the long term). It is exactly the place where automation can and should be applied.

Undoubtedly, requirements are the starting point for every process. As someone said, "It doesn't matter how many resources you have, if you do not know how to use them it will never be enough." Organizations should know their gaps and vulnerabilities to patch the right hole. What is the sense if they close a winder while windows are still open? Determination of these requirements can be done in 2 ways: just select the desired level of security or pass the quick test (for personal use) or as a reply to conducted assessment (audit) at the organization level.

Once the initial and desired levels of cybersecurity awareness are determined, it makes sense to identify the person's habits and find a better way for education. Having prepared the skeleton of the learning path, it can be adapted to someone characteristics and be able to suggest things, that matters and will ensure the expected result.

The education part consists of several methods:

- Training/courses. Training is considered to be the most popular solution. The thing there is training can only be valuable when employee clearly understands the content and know what he would know after passing the course
- Checks and tests. It is a well-known fact that people tend to forget about what they have learned. The only way is regularly checking the studied material, which can be retrieved from training and courses due to individual characteristics
- Simulated attacks. The theory is not enough for a clear understanding and assimilation. Such experience can only be received through practice. When people try to do something by themselves, resolve the issue, repel the attack, they were the target, they will remember it better. Using the automation approach, it can be ensured that people are receiving

appropriate attack content regarding their activity as real hackers do. The assessment is performed by simulating attacks and human-factor techniques used by attackers to determine the effectiveness of an organization's security policies, safeguards, and training programs. For example, a phishing attack is carried out by sending mass emails that look like they were sent on behalf of popular brands, service providers, or people known to the addressees. It tracks all email recipients who opened the email, clicked on links, opened attachments, and entered their username and password on a fake website. Detailed statistics will allow you to get both an overall picture of the company and determine corrective actions on an individual basis

- Daily recommendations and digest. Receiving small tips every day about how to increase security, a digest of the latest news and announcements helps people to be on track with current trends and situations in the world because everything is changing and following the outdated guides is not a good approach.

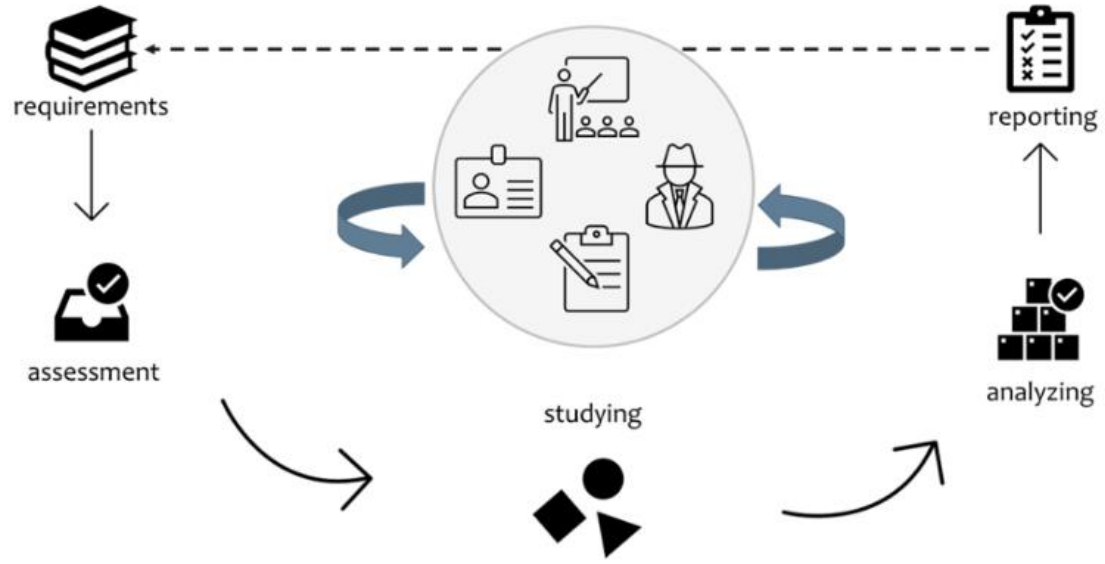

Figure 3: Processes in cybersecurity awareness program

An effective cybersecurity awareness program requires a set of activities that should be interconnected and pursue one goal. The second thing lies in people themselves - the person feels encouraged to study when he knows that he is not just a common employee, but a valuable part of the system, where the individual approach was applied. It helps them to feel unique and not just screw in the system. First of all, properly structured training of personnel can help to reduce the likelihood of unintentional violation of confidentiality and integrity of information, as well as the successful implementation of attacks using social engineering methods.

5. Conclusions

There is an ongoing battle between hackers and security professionals. Unfortunately, the unpredictability of human behavior can destroy the most secure information systems.

This article has attempted to collect and clearly identify the human factors that cause safety problems and provide suggestions on how to overcome them by creating new cybersecurity awareness program to educate each employee and help information security administrators have correct and clear configuration. The consequence of this is that information security is the key to mitigating security threats posed by human vulnerabilities.

Organizations must develop and maintain a culture that values positive safety behavior. They need to instill their culture so that security begins and ends with every person associated with their infrastructure, their business and their services. The best effect is achieved through a combination of software solutions to prevent security incidents, because otherwise it is almost impossible to control a complex distributed structure. To solve a complex of information security tasks, it is necessary:

- Control the storage locations and routes of information movement through all communication channels that are used in the company (mail, Skype, instant messengers, forums, cloud storages, etc.)
- Discover data on the enterprise network at any given time. Analyze data of any format: text, graphic, audio.
- Record the actions of employees, their activity in the enterprise, for working PCs and behavior in the team.
- Track dangerous traits. As a rule, security specialists do this "manually", which is extremely difficult in huge enterprises. But there are IT solutions on the market that make it possible to automate this work. This is done by automated profiling, for example. It shows the values and character of a person, a propensity for adventurism, for example, it demonstrates in dynamics if significant changes occur in a person's personality

It is no coincidence that the authors speak only of a decrease in the likelihood of incidents. Referring to the statistics of the penetration tests carried out, it is obvious that there are no companies where there would be no overly careless and inquisitive employees. Therefore, it is only possible to gradually reduce this vulnerability through a structured process of instructing an employee at all stages of his stay in the company

6. References

[1] "The human factor and its role in ensuring information security ". Securelist | Kaspersky Lab analytics and cyber threat reports. https://securelist.ru/chelovecheskij-faktor-i-ego-rol-v-obesp/725/

[2] ITCLOBAL. "Top 10 the loudest security incidents in the world". SecurityLab.ru. https://www.securitylab.ru/blog/company/ITGLOBAL/350271

[3] C. Cimini, A. Lagorio, F. Pirola, and R. Pinto, "How human factors affect operators' task evolution in Logistics 4.0," Human Factors and Ergonomics in Manufacturing & Service Industries, vol. 31, no. 1, pp. 98–117, Sep. 2020. Accessed: Nov. 9, 2021. [Online]. Available: https://doi.org/10.1002/hfm.20872

[4] A. Hope. "Chinese Startup Leaks 318 Million Private Records Obtained Through Data Scraping Facebook, Instagram, and LinkedIn Social Profiles - CPO Magazine". CPO Magazine. https://www.cpomagazine.com/cyber-security/chinese-startup-leaks-318-million-private-records-obtained-through-data-scraping-facebook-instagram-and-linkedin-social-profiles

[5] LRT.lt. "Hackers steal 'classified' documents, Lithuanian official say riots may be connected". lrt.lt. https://www.lrt.lt/en/news-in-english/19/1467832/hackers-steal-classified-documents-lithuanian-official-say-riots-may-be-connected

[6] V. Rulkov. "The human factor in information security". HABR. https://habr.com/ru/post/344542/

[7] P. Korostelev. "The influence of the human factor on the successful implementation of an information security strategy". itWeek. https://www.itweek.ru/security/article/detail.php?ID=183931

[8] I. Boytsov. "AlgoSec Firewall Analyzer Overview". Anti-Malware.ru. https://www.anti-malware.ru/reviews/AlgoSec_Firewall_Analyzer

[9] "ITSM (IT Service management): implementation of an IT service management system". IT Gildiya. https://it-guild.com/services/implementation/itsm/

[10] Audit of information security at the enterprise." IT Logica. https://itlogica.com.ua/services/informacionnaja-bezopasnost/

[11] "95% of all crashes are human errors not accidents - Northern Ireland - News and Blogs – articles on road safety and youth - Yours." YOURS Home - the youth movement for road safety. - Yours. http://www.youthforroadsafety.org/news-blog/news-blog-item/t/95_of_all_crashes_are_human_errors_not_accidents_northern_ireland

[12] "Large Enterprises Spend Nearly $300K Per Year On Security Awareness Training." Really?" KnowBe4 Security Awareness Training Blog. https://blog.knowbe4.com/large-enterprises-spend-nearly-300k-per-year-on-security-education.-really

[13] 5 Ways to Challenge the Forgetting Curve." LearnUpon. https://www.learnupon.com/blog/ebbinghaus-forgetting-curve/

[14] Axelus. "The human factor in the company: is it dangerous?" Habr. https://habr.com/ru/company/regionsoft/blog/432920/