Analysis of the human factor as an internal threat to the security of an organization

Grigorina BOCE
Department of Informatics and Scientific Education, Mediterranean University of Albania, Tirana, Albania
E-mail address: grigorina.boce@umsh.edu.al

Abstract

Over the last few years, the phenomenon we are facing more and more every day is the exposure to technology and the Internet. Threats and their types keep growing and incidents and attacks are observed more and more. The threats themselves are internal and external and each of them has its own effects on the functioning of the organization. But, according to recent studies, companies have already begun to feel threatened by internal ones more than external ones, due to the very fact that these threats can never be totally eliminated as long as a person is one of them.

Keywords: Access, Information, Threat.

1. Introduction

In the last decade, insider threats have become a major problem for companies. This is due to the very fact that the actors who take part are insiders of the company. Some problems arise from this. For starters, being insiders, they have access to the company's most critical systems. This means that if a wrong attack were to happen, the consequences would be fatal. Also, being insiders with good skills, reflected in the fact that they have been given positions that require accounts with unlimited access, they can hide their tracks and actions very well. This paper will focus on the privileged employee as an internal threat.

2. Information systems

Systems are one of the structures that surround us the most these days. It is enough to take a look around the environment that surrounds us and everywhere we encounter real examples of systems. What essentially characterizes a system is the feature of organization and interaction. The system, as a group of elements which are organized for a certain purpose, is dependent in terms of its operation on the performance of each of the components. It is enough for one of the component elements to malfunction, not be at the required level or leave, and the system will limp as a whole. [1] Information systems bring people and technology together, an interaction that basically has the same theory of operation and functioning as other system structures.

2.1 Security objectives of a system

The application of information security measures in a company mainly aims to achieve the three objectives of security, confidentiality, integrity and availability. Seen from the point of view of protecting a system, these objectives can be defined as follows (1):

- **Confidentiality:** When it comes to confidentiality, all attention goes to the concept of protection from unauthorized access. Since the system itself has data as a component, the protection of their confidentiality is the main measure in the application of information security

- **Integrity:** Integrity protection is closely related to the concept of preserving content unaltered, in its original version. Achieving integrity in a system means ensuring that system components can be modified (added, deleted, changed) only by authorized persons.
- **Availability:** Considering the role of the system in an organization, it is important that when necessary, the system and its components are accessible by authorized persons.

2.2 Threats to the security of a system

No matter how carefully a system is created and designed, as long as humans interact with it there will always be a possibility of failure, malfunction or misuse of the system and its components. This is about the very nature of man as a component of the system. In addition, many systems in the company carry weaknesses in their creation and design, thus making them vulnerable to threats and attacks. Regarding the categories of damage that can be caused against a system, we can weight the classes as follows (1):

- **Interference:** Tampering means that an unauthorized party has gained access to an asset. The problem in these cases lies in the fact that it is not always detected at the moment the intervention takes place.
- **Interruption:** The loss, unavailability or return of a component to an unusable state means the disruption of a system.
- **Modification:** Modifying system components starts with an intrusion but goes beyond it, where in addition to gaining unauthorized access, the accessed components are also modified.
- **Manufacture:** Fabrication or falsification consists in adding objects/modules to the system by unauthorized parties and using them for their own benefit.

2.3 The human factor

It is enough for one of the constituent components of the company's system to be compromised and one or several of the security objectives fail. During this work, man will be treated and examined as the cause of failures in achieving the security of systems. To understand the human position in an attack, the following figure is presented. [2]

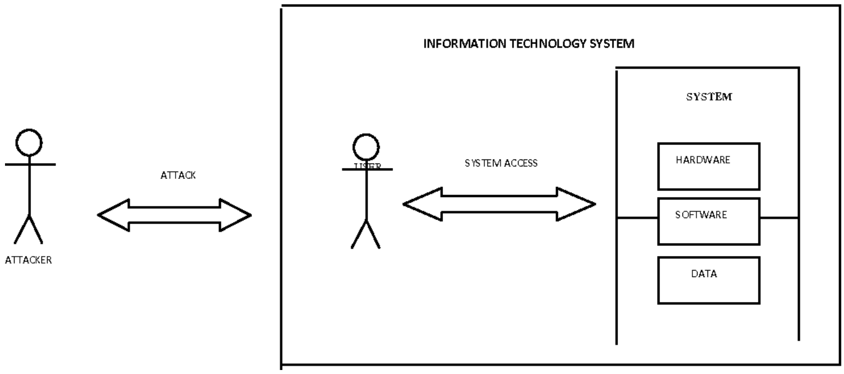

Fig. 2. Human positioning in an attack, Nikolakopoulos, 2009

Since the user has access to the technological components of the system, it can itself become the cause of failures as a result of mistakes or intentional actions, but it can also be used by an attacker outside the system to compromise the system. Thus, man poses a threat to the information system in a company.

3. *Security threats*

The most important task of the security team in a company is to protect assets. Since the asset constitutes value for the company, their damage, destruction, loss or modification causes harm and loss. Thus, their protection becomes a necessity. However, the development of various events, whether intentional or not, poses a risk to assets and their protection. Often, these targeted assets are under constant pressure from threat agents who attempt to discover and exploit any vulnerabilities the asset may exhibit. As a result, a threat to an asset is considered any object/person/entity that poses a risk to the security of the asset. According to a paper published by Microsoft, one way of classifying security threats to a company would be as follows:

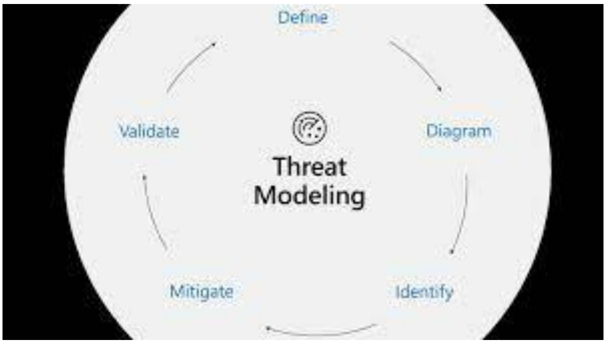

Fig. 3. Security Threat Classification, Microsoft

As can be seen, the emphasis is on man. Thus, attacks are classified based on the human being into whether or not the attacks are human-caused, and if so, with or without malicious intent. Depending on the positioning of the person, whether he is an internal or external actor of the company, we classify threats to the company's security into external threats and internal threats. [3]

3.1 External Threats

"Only when things start and go wrong do machines remember how powerful they are" - Clive James

Threats from outsiders constitute one of the two largest groups of threats, and the percentages of such attacks are extremely high. These outsiders, such as hackers, organized criminal groups, government entities or company competitors, work to discover the weaknesses that the company's system may have in order to exploit them for their own purposes and to gain access from the outside - inside the company. [4] These threats, among others, pose a high risk to the organization as they are usually highly qualified and experienced persons, which makes it difficult to identify them. Attacks of this type, generated as a result of successful external threats, can be active or passive.

During an active attack, in addition to gaining the desired access, external persons also intervene in the system and undertake actions of various natures. The opposite happens in a passive attack. After gaining access to the company's assets, these attackers intercept and study the network, system and users. External threats can be classified into several large groups such as threats to physical security, legal threats, economic, social, network and software threats, etc. [4]

According to a 2015 report by Akamai on the State of the Internet, this year marked the highest number of packet attacks with approximately 214 million packets per second. This volume would be enough to knock out Tier 1 routers, such as those used by ISPs. This form of attack is one of the types of DoS attacks against networks and network devices. The same report lists the 10 countries in the world from which most DDoS attacks originate. [5]

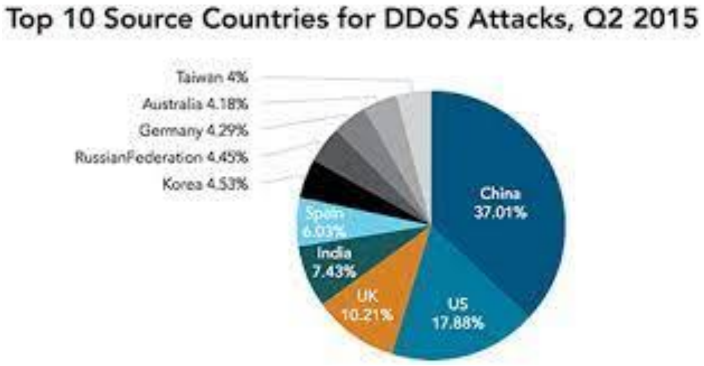

Fig. 4. Top 10 DDoS generating countries, Akamai, 2015

3.2 Insider Threats

"We have found in our research that internal threats are not viewed as seriously as external threats. But when companies had an internal threat, it generally cost more than external incidents. This is mainly because the insider can cleverly hide the crime for months, years, sometimes forever." - Dr. Larry Ponemon, Chairman, Ponemon Institute, SecureWorld Boston (14).

A threat is classified as insider when an insider misuses his rights or makes mistakes that result in the misuse of these rights.

3.3 What is an insider?

If in recent years the template definition was "employee of the company with access to IT systems" [6] now, with the evolution of technology and network schemes, access methods and partnerships, we encounter a new conception of the term Insider. An Insider can be any employee, contractor, partner, vendor who enjoys access to company data and systems. [7]

For this study, only employees will be considered as one of the internal threats of a company.

According to a 2018 study by Crowd Research Partners, 90% of companies surveyed felt vulnerable to insider threats. Also according to this study, the losses from these attacks if they were successful for 55% of the companies vary in the values of $100,000-$1,000,000. Whereas, for 9% of them, this loss exceeds the value of $1,000,000 (7).

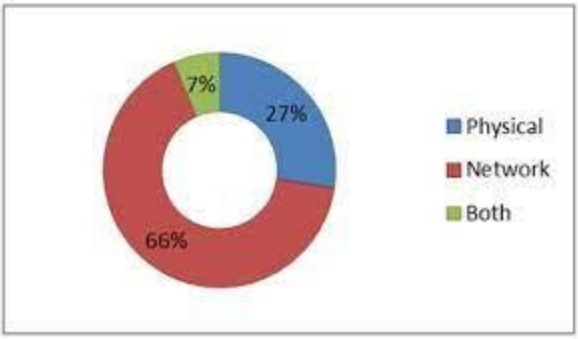

Fig. 5. Assessing companies on risk from insider threats, Crowd Research Partners, 2018

Looking at these numbers, the question arises, Why are these insider threats considered so dangerous and the damage they can cause so high?

The first reason consists of the right of privileged access. An insider is considered such for the very fact that he possesses privileged and often unlimited access as a "superuser" to servers, network, data and applications. Being with privileged rights and so close to these valuable assets increases the dangerousness of this type of threat, as even the smallest mistake/action is enough to have a large-scale incident. [8]

The second reason is closely related to the skills of these people. Usually, the people who enjoy and are equipped with rights of this level, are very familiar with the IT environment, assets and have high knowledge which they can also use to hide their tracks. For these reasons, their identification is difficult and takes time, which increases the costs of improving the situation and returning to the previous state. [8]

3.4 The privileged employee as an insider threat

The figures presented above in this study and beyond, show that indeed companies have reason to worry about the influence of privileged employees on security threats. According to a 2017 security attack study by Balabit and Landhouse, 4 out of 5 companies had experienced a data breach incident this year, and about 50% of these attacks were caused by employees. [9]

Fig. 6 Report on % of attacks by each insider actor, Balabit&Landhouse, 2017

However, it is worth noting the difference in intent behind these incentives. Such threats can be intentional but not always; they are often the result of mistakes and unintentional actions. As shown by the results of the report, 30% out of 50% in total are the result of unintentional actions of employees and only the rest initiated with a purpose.

Unintended threats: "A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems, encryption and other security technologies, but if an attacker can contact a trusted person within the company, and that person obeys, and if the attacker gets that that you want, then all the money spent on the technology is essentially wasted."- Kevin Mitnick, "A convicted hacker debunks some myths", www.cnn.com, October 13, 2005.

A random insider can turn out to be one in a variety of situations. One of the reasons is human error. This comes from a lack of information, training or safety awareness. For example, clicking on a malicious link or opening a document attached to an email without first checking it is enough to compromise an entire system. Also, insiders are often manipulated by outsiders and used to attack a system. As an example, we can mention the theft of credentials and accessing the system through them. According to a 2015 article by Nicole van Deursen, some other common forms of insider threats are [10]:

- Sending documents with sensitive information to the wrong recipients.
- System misconfigurations.
- Poor patch management practices.
- Using easily guessable names and passwords or leaving those given by default.
- Visits to compromised websites.
- Loss of equipment that may have accessed company assets.
- Sharing passwords with others.
- Leaving computers unattended when outside the workplace or allowing other people to use them.

Intentional threats: Human error among employees is not the only attack vector to which businesses fall victim. A large part of the internal attacks and intentional threats by the employee where it is observed working against the company and the employer. Like any threat that results in an incident, the impact insider attacks have is multifaceted. These consequences are reflected both on the financial side of the company as well as on the reputation, organizational culture and even the risk of bankruptcy. But the question arises, what motivates these insiders to act with malicious intent against the company they belong to?

According to a 2017 article by digital security solutions specialist Marcell Gogan, some of the motivations behind these acts may be: [11]

- Seeing these attacks on data or systems as an opportunity for personal gain from the most diverse.
- Making statements.

Often employees may want to make political or social statements and in support of them distribute data or damage it. As an example, Edward Snowden leaked his employer's data to protest ongoing government surveillance.

- Industrial espionage.

And the most honest employees can be tempted in the face of offers they receive from competing companies to sell and take out of the company the data or information that constitutes its competitive advantage.

- Seeing yourself as a future competitor.

These employees may want to start their own business in the future similar to where they are now, so they aim to get information and use, view and acquire customer lists, etc.

3.5 *Intentional threats*

Human error among employees is not the only attack vector to which businesses fall victim. A large part of the internal attacks and intentional threats by the employee where it is observed working against the company and the employer. Like any threat that results in an incident, the impact insider attacks have is multifaceted. These consequences are reflected both on the financial side of the company as well as on the reputation, organizational culture and even the risk of bankruptcy. But the question arises, what motivates these insiders to act with malicious intent against the company they belong to?

4. Conclusions

Security is not the purchase of a device, the drafting of a policy or an awareness training of employees. Safety is a continuous and permanent process that requires the full commitment and involvement of everyone in the company, a process that should not be stopped or neglected. This is due to the very fact that we can never be totally sure that we have reached maximum security and that nothing can threaten us anymore. Safety is not achieved once, but must be worked on constantly to minimize it every time.

Regardless of how much a company invests in protection technology against threats and attacks, the most important link to invest in is the human. This is due to the very fact that a lot can be invested in the latest technologies, but if there are not the right people to manage and use them, then the security objectives will not be achieved and these technologies will not be used properly. Also, regardless of how much we have invested in technology, one moment of human weakness is enough and it can reach the threat of business continuity. Internal threats are the most harmful and frightening for a company. It may never be understood that an insider attack has occurred. This and because employers tend to wait for the threat from the outside and not from the inside, such threats are difficult to understand since they leave no traces and touch the heart of the company's assets. This is because the individuals who cause it have full access to the most critical assets. If an outsider has to penetrate multiple layers to get to critical assets, an insider is just a command away.

From the general point of view of companies, there are no real structures for security management. Also, they do not design policies that will minimize internal threats, they have not yet understood the importance and influence of man as a threatening factor, this is also based on the lack of training or awareness among employees. There are even cases where basic protection technologies such as antiviruses and firewalls are missing.

References

[1] Crawford, K. C. (2016), *Artificial intelligence's white guy problem*, The New York Times, https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html.

[2] Kurzweil, R. K. (2001), *The Law of Accelerating Returns*, Https://Www.Kurzweilai.Net/. https://www.kurzweilai.net/the-law-of-accelerating-returns.

[3] Gaines-Ross, L. G. R. (2016), *What Do People — Not Techies, Not Companies — Think About Artificial Intelligence?*, Harvard Business Review, https://hbr.org/2016/10/what-do-people-not-techies-not-companies-think-about-artificial-intelligence.

[4] Angwin, Larson, Mattu, Kirchner, J. A, J. L, S. M, L. K. (2016), Machine Bias. Https://Www.Propublica.Org/, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[5] Cambridge Dictionary (2021), Https://Dictionary.Cambridge.Org/, https://dictionary.cambridge.org/dictionary/english/bias.

[6] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021), *A survey on bias and fairness in machine learning*, ACM Computing Surveys (CSUR), 54(6), 1-35.

[7] Danziger, S., Levav, J., & Avnaim-Pesso, L. (2011), *Extraneous factors in judicial decisions*, Proceedings of the National Academy of Sciences, 108(17), 6889-6892.

[8] Buolamwini, J. B. (2019), *Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It*, TIME, https://time.com/5520558/artificial-intelligence-racial-gender-bias/.

[9] Maryfield, B. M. (2018), *Implicit Racial Bias*, Justice Research and Statistics Association, https://www.jrsa.org/pubs/factsheets/jrsa-factsheet-implicit-racial-bias.pdf.

[10] Feast, J. (2019), *4 Ways to Address Gender Bias in AI*, Harvard Business Review 20, https://hbr.org/2019/11/4-ways-to-address-gender-bias-in-ai

[11] Gogan, M. (2017), *Insider threats as the main security threat in 2017,* Retrieved March, 12, 2018.