PROJECT, DESIGN AND MANAGEMENT

ISSN: 2683-1597

PDM PROJECT DESIGN & MANAGEMENT

How to cite this article:

Quissanga, F. C. & Fernandes, R. F. (2020). Importance of Information Security in Corporate Information Technology Companies. *Project, Design and Management, 2*(1), 87-102. doi: 10.35992/pdm.v2i1.431

IMPORTANCE OF INFORMATION SECURITY IN CORPORATE INFORMATION TECHNOLOGY COMPANIES

Fernando Cassinda Quissanga
International Iberoamerican University (Mexico), European University of the Atlantic (Spain)
fernandoquissanga@hotmail.com· https://orcid.org/0000-0003-4468-7206
Roberto Fabiano Fernandes
FUNIBER – Iberoamerican University Foundation / Faculdade Cesusc / Universidade do sul de Santa Catarina (Brazil)
roberto.fabiano@funiber.org · https://orcid.org/0000-0002-6738-6572

Abstract: The importance of information security in corporate information technology companies has the primary objective of proposing security measures to protect information in corporate information technology companies. In this sense, the research is a qualitative, exploratory and descriptive, as it is based on the search for bibliographic material that makes it possible to suggest security measures for the protection of information. Secondary data were collected systematically, looking for the keyword - security measures and their synonyms. The search was carried out in computerized databases, such as Google Académico® and the Portal de Periódicos Capes. A set of suggestions for security measures that enable corporate companies in the field of Information Technology to take advantage of has been identified. It is highlighted as a conclusion that the proposed preventive, detective and corrective measures must be involved in a security and contingency plan disseminated throughout the organization.

Keywords: Information security, Security measures, Corporate companies.

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE TECNOLOGÍA DE INFORMACIÓN CORPORATIVA

Resumen: La importancia de la seguridad de la información en las empresas corporativas de tecnología de la información tiene el objetivo principal de proponer medidas de seguridad para proteger la información en las empresas corporativas de tecnología de la información. En este sentido, la investigación es cualitativa, exploratoria y descriptiva, ya que se basa en la búsqueda de material bibliográfico que permita sugerir medidas de seguridad para la protección de la información. Los datos secundarios se recopilaron sistemáticamente, buscando la palabra clave: medidas de seguridad y sus sinónimos. La búsqueda se realizó

en bases de datos computarizadas, como Google Académico® y el Portal de Periódicos Capes. Se ha identificado un conjunto de sugerencias para medidas de seguridad que permiten a las empresas corporativas en el campo de la tecnología de la información aprovechar.
Se destaca como conclusión que las medidas preventivas, de detección y correctivas propuestas deben estar involucradas en un plan de seguridad y contingencia difundido en toda la organización.

Palabras clave: Seguridad de la información, Medidas de seguridad, Empresas corporativas.

IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS CORPORATIVAS DO RAMO DA TECNOLOGIA DE INFORMAÇÃO

Resumo: A importância da segurança da informação nas empresas corporativas no ramo da tecnologia da informação tem como o objetivo primário em propor medidas de segurança para proteger a informação nas empresas corporativas do ramo da tecnologia de informação. Neste sentido, a pesquisa é qualitativa, de cunho exploratório e descritivo, pois tem como base a busca por material bibliográfico que possibilite sugerir medidas de segurança para a proteção das informações. Os dados secundários foram coletados de forma sistemática, buscando-se pela palavra chave – medidas de segurança e seus sinónimos. Realizou-se a busca em bases de dados computadorizadas, como o Google Académico® e o Portal de Periódicos Capes. Identificou-se um conjunto de sugestões de medidas de segurança que possibilitem as empresas corporativas do ramo da Tecnologia da Informação possam usufruir. Destaca-se como conclusão que as medidas preventivas, detetivas e corretivas propostas devem estar envolvidas em um plano de segurança e contingência disseminadas em toda a organização.

Palavras-chave: Segurança da informação, Medidas de Segurança, Empresas corporativas.

Introduction

Information security has been a concern around the world, information has become very important, handling it requires great care, and it is necessary to create conditions to protect it. Therefore, it is impossible to say that we are totally safe, even when it comes to the security of first world countries. This is because the economic losses, the psychological, deontological, and ideological problems are very great, in the present century we face various difficulties to control cybercrime (*brute force*) and espionage (*sniffing*).

Sniffing is understood, according to the definition of the website CERT.br (2012 p.19), *"Traffic interception, or sniffing, is a technique that consists of inspecting data trafficked in computer networks, by using specific programs called trackers."*

However, coups, electoral fraud, leaking political information, state secrets and bank diversions (which are called the phishing technique) have been a cause for concern. Theft with credit cards such as credit card cloning, email spoofing, altering grades in the university database (Pharming).

Nevertheless, it is worth mentioning that information security has become the first concern reported in this article. In 2018, the main concern of the countries was to create a legislation to prevent crime and to be able to bring criminals to justice, because it is very difficult to detect when we are being the subject of a computer crime . The basic security mechanisms must be studied in depth, such as the identification, authentication, authorization, integrity, confidentiality and availability of the information.

Similarly, it is understood that the advent of social media also allowed for an increase in the number of attacks by computer viruses, spies for copying of credentials, user passwords, various codes that will be sent to a remote computer where hackers search

this information to commit crimes. Another technique widely used by *Crackers* is social engineering, the goal of which is to trick people into accessing information that allows them to enter computers or computing devices.

Based on these descriptions, the overall objective of this article is to suggest security measures to protect information in corporate information technology companies.

Method

This research is understood as qualitative, exploratory, and descriptive, since it is based on the search for bibliographic material that suggests security measures for the protection of information. Secondary data was collected systematically, searching for the keyword - security measures and their synonyms. The search was performed in computerized databases, such as Google Scholar® and the Capes Newspaper portal (Portal de Periódicos da Capes). Google Scholar® for Creswell (2010) is a free database that provides a wide variety of bibliographic searches from various sources, such as theses, abstracts, and articles, with the advantage of being able to obtain them in their entirety. Regarding the Capes Newspaper portal, it was chosen as a search source to offer access to the full texts of selected articles in more than 15,000 international, national and foreign journals, and 126 databases with document summaries in all areas of knowledge (Portal de Periódicos da Capes). As for the analysis, the use of descriptive data analysis is considered, since it allows organizing, summarizing, and describing the important aspects of a set of observed characteristics or comparing those characteristics between two or more sets.

Description of the main economic losses caused by the failure of information security.

Based on the literary search, some economic losses were identified when there is no precaution and control, or the use and application of measures based on information security.

Coopamootoo (2018) suggests that companies that protect employee privacy in online interactions:

> In offline interactions, we need to disclose information about ourselves to build trust with others. When we move online, there are differences: businesses must participate to facilitate online interaction and they need to keep information about us to do so. These companies have a duty to protect our privacy, but our information may be at risk of accidental data loss or malicious attacks.

However, the protection and privacy of information has been a concern and fear of users who have services in these companies. The vulnerability of the data that can be used for cyber-attacks, not only for the theft of computers in the case of bank data, but also through the use of social engineering and social networks.

Most users of modern information technology run many risks, as they allow failures due to the lack of caution and control of the cause. Many do not have specific information on security preparation, and the preparation must be based on knowledge, we must all know these information security techniques in order to protect, because experience shows that not only users, but also companies allow most of the time to expose their clients' data as mentioned by Futurelearn, (2018):

> TalkTalk's cyber-attack saw the personal data of 157,000 customers, including credit card details, which were released in October 2015. As a result, the company lost around £60 million and more than 100,000 customers, but the customers were also open to potential identity fraud: in some cases, scammers used the data that allowed them to appear as TalkTalk engineers, contacting customers and persuading them to install malware in their machines.

However, we are faced with a precarious situation, we note that, in addition to the company failing with the security system, customers also facilitate data theft, as they have no knowledge of information security and allow criminals to implement social engineering.

Nevertheless, cyber-attacks in recent years have brought many difficulties, the malware belongs to several groups of computer viruses of approximately 31 present families, for example, the trojan, worms or bugs, dropper and backdoor, are the basis of many economic losses, false identity, espionage, data theft, types of computer fraud and sending data to a remote computer, even if they are geographically distant or on different continents.

Investments in the financial area are at serious risk. Attackers are the basis of these situations, the evolution of cybercrime and cyberterrorism, clients are their targets because they have often neglected and allow their data to be stolen, and through digital thefts of the customers, the company is affected in the same way as its security system. Also, sometimes it allows the theft of information when it does not have an adequate security system to protect its data.

However, the company and customers must be protected to prevent unauthorized people from accessing their credentials and are equipped with all the information security tools, so corporate companies and others must be prepared to avoid economic losses caused by the violation of the security of customers, users, employees and former workers, who already know the entire security system. In this case, it is important to revitalize and restructure the entire security system to avoid such situations, security policies should not be known by third parties, this makes the company vulnerable.

Even speaking of credit card fraud in the United Kingdom, it is appropriate to present the graph of the economic losses of fraud over the years and to know its current status:

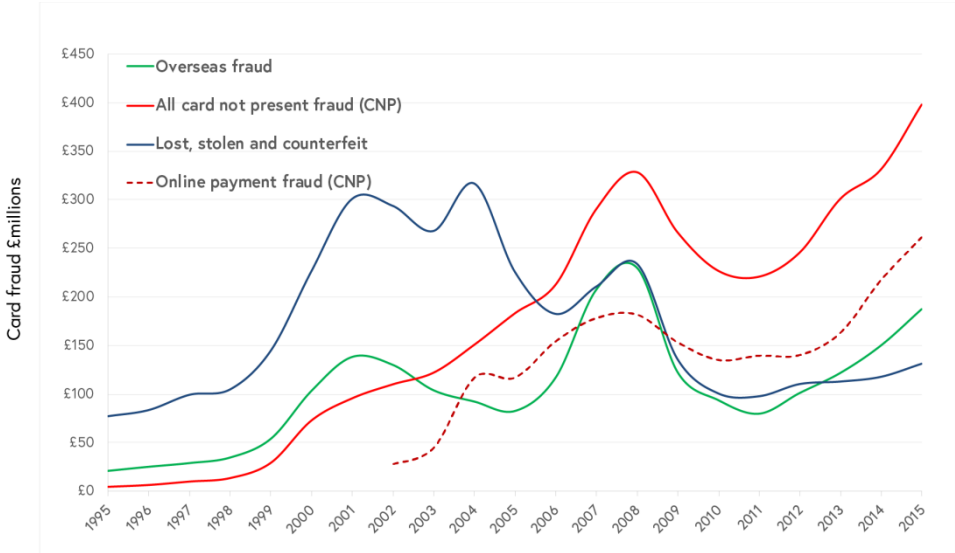

Figure 1. Chart of annual losses with cards issued in the United Kingdom
Note: Source: Futurelearn (2018).

By making a self-observation in figure 1, it is possible to analyze that from 1995 to 2015 there is a substantial increase in computer attacks on credit cards, which resulted from financial losses in the range of 0 to 450 million Euros, values that companies are subject to bankruptcy. Corporate companies with higher financial capital are likely to lose more when there is no prevention against Crackers and virtual pests.

In figure 1, it can be seen that the fraudulent payments made online have a scale of more than 250 million Euros, a large amount of money stolen by financial fraud, so it is necessary to avoid preventing cybercrime.

In the case of thefts, losses and counterfeits mentioned in figure 1, a scale of more than 300 million Euros is mentioned.

However, figure 1 also refers to credit cards made without bank fraud, in the order of 400 million Euros.

According to Financial Fraud Action in the United Kingdom (2017, p. 10): it presents the economic losses caused by thefts through online payments with credit cards: "Losses due to financial fraud in payment cards, remote banks and checks totaled £768.8 million in 2016, an increase of 2% compared to 2015." However, there are countless hardships and financial losses due to lack of information security, and we often notice that some companies expose our data and this has generally caused fraud, and many seek compensation from the company, others do not, and remain silent without knowing where to go, in this case, we must be very careful, how and where we place our credentials, the type of social networks to which we belong, the type of business or online purchase, all these factors must be treated with special attention.

> New technologies eradicate existing ways of committing fraud, but they also introduce other vulnerabilities that scammers adapt to exploit. The chip and PIN made it difficult to use a stolen card and therefore the theft of the card was rejected. However, criminals have identified that online payment has become a weakness since they cannot use Chip and PIN. Online fraud is now the most common form of payment fraud in the UK (Financial Fraud Action in the United Kingdom, 2017, p. 18).

Faced with this fraud, what stands out is that each banking professional must be prepared to know how to administer the management of documents and processes and, in turn, the information and financial assets, must behave like a professional that the bank has. Like its flag, we do not know in concrete terms what the basis for extortion was, but we believe that banks should promote a balanced salary for their technical staff, such as training in the fields of information security, ethics, and professional ethics.

According to the Terra (2018) site:

> The leak of 11.5 million documents, the so-called Panama Papers, from the Panamanian law and consulting firm Mossack Fonseca, the fourth largest offshore law firm in the world, would have revealed details of hundreds of thousands of clients using offshore tax havens allegedly for tax evasion, money laundering, drug trafficking and arms trafficking.

In addition to the analysis of the banks, a close-up is also made on the two corporate mobile phone companies, which we can designate as competitors, Samsung and

Apple. These companies have a very robust security system, they have many experts in information security, to protect prototypes, patents, and the telephone industry. However, these companies are leaders in the international telephony market, but if advanced information security methods are not used in these companies, a failure is fatal, it is not necessary to be very careful, in this case we must be careful to avoid disastrous situations, such as in 2012 in California, where Samsung, accused of violating patents only for the appearance of the devices and touch functions, which was required to pay millions of dollars, we imagine that it is a prototype, the scandal would be greater. In this case, the South Korean company was forced to compensate, according to Oficina Net, (2015):

> On August 24, 2012, a jury in San Jose, California, convicted Samsung of violating a series of patents from its largest competitor, the same jury sentenced the South Korean company to pay the equivalent of $930 million in damages to Apple. For its part, the federal court of appeals of Washington, USA, confirmed, in parts, the decision of the San José jury, trying to reverse part of the sentence, alleging that Samsung was unjustly convicted of violating patents related only to the appearance of the devices and the touch functions of the mobile device of the Apple company.

Some practices in information insecurity.

After the damages caused by the main economic losses caused by the failure of information security, it is appropriate to mention several practices that allow failures in information security. Most of the information users make it possible for these failures to occur, because many of them have an inadequate education for the protection of computer data, which makes it possible, that is, it translates into an open door for cybercriminals, Crackers and computer spies who take the opportunity to commit cybercrime.

According to Laureano (2005, p. 15 apud. Shirey, 2000) we have the definition of some important terms regarding information security:

> Threats
>
> - Intelligent threat: circumstance where an adversary has the technical and operational potential to detect and exploit the vulnerability of a system;
> - Threat: potential security breach. Exists when there is a circumstance, potential, action, or event that could violate security and cause damage;
> - Threat analysis: an analysis of the probability of events and the consequences of detrimental actions for a system;
> - Consequences of a threat: a security breach resulting from the action of a threat. Includes: disclosure, usurpation, disappointment, and interruption.

There are several threats, as we can see that scammers use social engineering, becoming real of a given bank or service, persuading the client to register much to steal their credentials, Internet, especially social networks allow improper access to information, mentioning that one of the fastest ways of spreading computer viruses are pornographic sites. It is one of the criminals' favorites because even some, teenagers and adults, are unaware that criminals use these sites for computer theft. Since contamination occurs when we open the image or video, in this case, the virus has the ability to present itself as an attachment to the document and replicate in the host in no time.

According Martinelli (2008, p. 46):

> Many viruses disguise themselves as supposed games, features, in attachments. Virus creators also use social engineering to reach their victims, claiming registration with government institutions, security, pornography, and free fun. Infected text messages sometimes replace the sender's line by posing as acquaintances, increasing the chances of contamination.

However, computer viruses are so fast and destructive in the transmission process that each one presents its specificity. However, the rule is the same and is based on the behavior of biological viruses that attack human cells, while computer viruses attack operating systems in their respective files. Every company that handles information must have an information security control room to prevent their data from being lost. In this recommendation, the expense of any investment in information security is made, it is important to hire specialists in the area of information security or create a department that supervises the management of files and documents. Companies complain of various computer thefts because some of them do not invest in data protection.

Corporate companies must lead by example in data protection, they must not waste information because they are subject to loss of reputation and other financial losses. As an example, we can mention the Coca-Cola company, which would not like to know the formula for its soft drink.

Nevertheless, large companies have never failed and have always differentiated themselves by protecting their assets. Try to imagine the security system that these companies have, which requires a lot of control and investment. However, it is understood that this culture must be transferred to other corporate companies.

According to Laureano (2005, p. 17):

> To implement security mechanisms, it is necessary to classify the possible forms of attacks on systems:

- Interception: access to information by unauthorized entities (violation of the privacy and confidentiality of the information) is considered interception.
- Interruption: can be defined as the interruption of the normal flow of messages to the destination.
- Modification: consists of the modification of messages by unauthorized entities, violation of the integrity of the message.
- Personification: personification is considered as the entity that accesses the information or transmits a message posing as an authentic entity, a violation of authenticity.

When addressing the information security mechanism, it is necessary to mention the type of physical security (*Hardware*) and logic (*Software*). They must be studied in depth because, for the most part, we are more cautious in one and not the other. It is recommended that there is no point in having a robust logical security (*software*) mechanism and an unprotected physical security system (*hardware*), which can happen is the theft of computing devices.

It is suggested that one be prepared for both forms of information security and invest a lot to have protection in our facilities and within a certain perimeter.

Trace the different ways of computer theft

According to Oliveira (2009, p. 14-15), organizational threats are divided into five:

- Physical threats;
- Logical threats;
- Occupational threat;
- Threat to confidentiality;
- Environmental threat.

Although there are various threats in companies, at this time we will emphasize physical and logical threats, as this is the objective of our investigation.

> However, malware is software designed to infect any program. Worms have the ability to replicate. Spyware programs are designed to spy on users and collect information to monitor the victim. Phishing is generally sent by email and captures extremely confidential information to carry out the fraud later (Quissanga, 2015, p. 6).

However, it is known that there are several types of computer crimes, which are performed by computers, executed through the Internet, in technological, digital form and other crimes of a legal nature. Computer theft is more widespread, so some do not have a law, regulation or criminal code; however, in the current context, countries see studying methods to arrest cybercriminals, a task that has not been easy, some articles or decrees used out of context that harm or benefit criminals are considered too far from reality. Despite this, the control of computer thefts must be made a deeper and more complete study, implementing detection measures, because there are various forms of cyber attacks.

Nevertheless, companies must be prepared to prevent attacks, this implies using all security devices, both logical and physical, and training their technical personnel or hiring companies specialized in the area of information security, in case they do not have all security tools when we are exposed on the Internet, we become more vulnerable, for this reason we need to implement the firewall to avoid unnecessary traffic that can be a transmission route for computer viruses, in this case all foreign packets, that is, not authorizing the firewall removes, denies all suspicious packets, allowing only authorized ones.

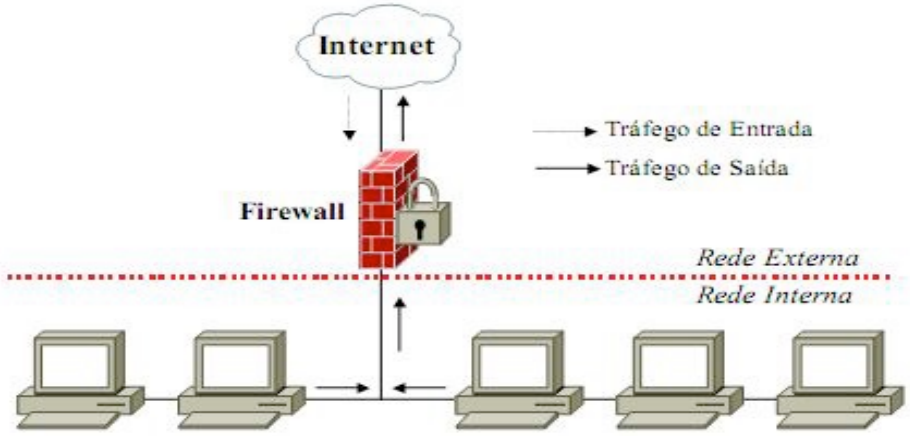

Figure 2. Defense is more complex than the attack.
Note: Source: Oliveira (2009, p.28).

However, in figure 2, it can be analyzed that defense is more complex than attack. Therefore, we must be prepared to avoid any violation of information security, because if we are attacked, we will hardly be able to defend ourselves from the attack. The term hacker is still widely debated, but we prefer to use Cracker because

it has a clear definition of cybercriminal. The Hacker, on the other hand, does not necessarily practice a virtual crime, but both have the same capabilities as the Hacker, but he presents himself defensively and is generally hired to protect a company's security system.

Computer theft forms are very quiet and unpredictable. Therefore, choosing a security method has been a great challenge, due to the problems we live in. While some study ways to protect themselves, others spend a lot of time to detect any information that allows virtual fraud; however, the forms of attack are diverse, each with its specificity, each case is a case, so it has been difficult to detect real security flaws.

Oliveira (2009, p. 40) basically mentions that the attackers carry out the following steps:

Step 1: The attacker, when it penetrates its network, breaks a certain machine.

Step 2: Installs a sniffer program.

Step 3: This program monitors the network to access network services, traps are made and recorded in a log file.

Step 4: Then the attacker recovers the log file.

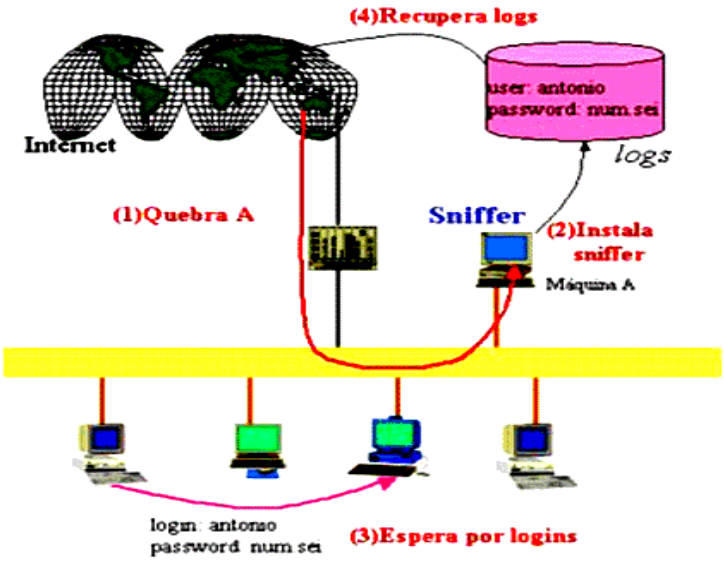

Figure 3. Information theft
Note: Source: Oliveira (2009, p. 40)

Today's corporate companies present computer programs or applications for bank transfers, balance inquiries, extract statements and various types of online payments, these tasks make some users vulnerable because they have no security education, these operations are generally performed by cell phone devices used by people who can access credentials, not to mention other forms of cybercrime. Bank fraud, in addition to social engineering, also sends strange messages, or emails, that generally contain malware or spyware. For example, we can analyze phishing.

Implementation of information security measures.

It is important to have basic training in security techniques, companies must train their employees to improve information security.

According to Oliveira (2009, p. 10) "It is useless for an organization to act virtually if the information fed into the system is vulnerable. Just as this is a differential factor for globalization, vulnerability can lead to the failure of a company".

The following are some unsafe practices:

1. Open suspicious email;
2. Online purchases with credit cards from unreliable companies;
3. Leave the Bluetooth on on your cell phone;
4. Install software on your phone from sites outside the Play Store, App store, itunes store, and Google store;
5. Allow your mobile device to be unprotected;
6. Allow unauthorized people to access your credentials;
7. Use of suspicious websites;
8. Use your computer without a strong password;
9. Use of misleading advertising;
10. Using storage devices on infected computers;
11. Use dubious source multimedia sharing;
12. Using an unprotected wireless network;
13. Using a computer without updated or unprotected antivirus;
14. Use a server without antimalware, antispyware and firewall.

Some companies also allow security breaches, either by hardware or software, but now we will address the failures related to the logical part:

Logical security flaws in companies:

1. Allow Crackers to monitor customer credentials;
2. Allow vulnerability in security systems;
3. Allow the cloning of customers' credit cards;
4. Allow the leakage of news and multimedia from customers;
5. Allow loss of confidential customer data and files;
6. Allow the diversion of bank details;
7. Allow deviations from formulas, patents, and prototypes;
8. Allow the change of academic data in the universities.

Physical or hardware security flaws that facilitate cybercrime:

1. Allow unauthorized access to the control or security room (social engineering);
2. Allow access to security cameras;
3. Allow access or theft of computing devices (HDs, external drives, USB sticks and CDs) that contain confidential information;
4. Due to lack of attention, allow the use of ATMs with cloned cards.

However, for information security measures, we recommend the SET protocol, according to Gonsalez (2011):

> The SET protocol (Secure Electronic Transaction) is a protocol created with the aim of providing security in time to carry out a transaction on the Internet. This protocol was created solely and exclusively to carry out secure electronic transactions that offer services such as:

- Authentication;
- Confidentiality;
- Integrity;
- Privacy;
- Immediate verification;
- No repudiation.

Many security measures are known to exist: preventive, detective, and corrective.

Preventive measures

These are precautionary measures against computer attacks. For example, servers are advised to install firewalls, use cryptographic techniques, set a strong password, create backups or redundant backups. For computing devices like computers, we recommend installing a complete, full-featured antivirus, especially antimalware, antispyware, and antispam, and undergo a constant update process. For physical control, you must install surveillance cameras, alarms, hire a physical protection company to control the space, and you need to hire a Hacker to monitor and test security systems. Without forgetting the training of technicians in the security system.

Detection measures

These measures are necessary when you want to monitor or audit your company's security or if there is an attacker tracker. These are measures that can carry out is to the presence of the Hacker hired to monitor all resources and report the security status of the company.

Corrective measures

Measures of this type are worrisome, but their impact is greater when the previous measures were not carried out in their entirety, although we have previously stated that the security problem is very delicate and requires large investments that companies are not always financially prepared to support this situation. They are those that happen in an emergency, without being planned, and damage the environment of information technologies, therefore, they must be resolved quickly for the health of the company. It is necessary to measure the risks as data loss are often irreparable, for this reason, the Hacker must assess the risks that have the company using this or that kind of security, knowing that so far we don't have completely safe security systems.

Security and contingency policy.

Physical threats;

> They are those to whom the used material resources in the information environment are exposed, putting the operational integrity of the organization at risk. Unfortunately, in many companies, they spend a lot on information security and end up forgetting to protect their assets (Oliveira, 2009, p. 15).

Physical security

Physical security is also very common, including fires, electric shocks, storms, electrical problems, misuse of equipment, inadequate access to the security room and the data processing center.

The physical security measures are:

1. Post guards in the control center;

2. Place doors with locks;
3. Installation of surveillance cameras;
4. Install alarms that transmit directly to the police control center;
5. Install fire extinguishers;
6. Install physical firewall;
7. Install eavesdropping systems;
8. Use No-Breaks.

According to Oliveira (2009, p. 15):

Logic threat

"These occur when there is a change in functional capacity due to fraud, accident, or resource error".

Logic security

Logical security is more extensive:

1. Cryptography: it is the art of writing and hiding codes so that the information is unrecognizable;
2. Firewall: it has the function of allowing or preventing packets. Being one of the foundations of security;
3. Circuit-level Gateway: it has the function of allowing or denying specific commands of specific applications through a proxy server, and they operate at layer 4 of the OSI model;
4. Bastion Hosts: are those that the hosts, before reaching the internal network, need to go to bastion hosts first, with or without permission;
5. Behavior-Based Intrusion Detection: used to deviate normal user behavior;
6. Radius protocol: it is a client/server security system;
7. NAT - Network Address Translation: used to store IP addresses;
8. Network-Based Intrusion Detection System (NIDS): also monitor network traffic from headers and packet content;
9. Single Sign-On (SSO): is a method that uses transparent and unique authentication for various corporate systems;
10. Honeypot: it is widely used to test security systems, allowing greater visibility of the real state of the company, it is also used to preserve the network from attacks;
11. Virtual Private Network (VPN): they are responsible for guaranteeing the authenticity, privacy, integrity of data, especially encryption technology;
12. Kerberos: has a secret key for each user;
13. Knowledge - Based Intrusion Detection: attacks are detected as an antivirus;
14. Intrusion detection systems (IDS): aims to monitor and accompany the internal and external action of the network;
15. Write the URL in the browser: it allows to use the accredited sites in a secure way;

16. DMZ - Demilitarized zones: it is an intermediate network made up of a firewall, servers and a switch, which remains between the internal and external networks.

Results

The research was conducted to propose security measures for corporate companies in the information technology industry. In this understanding, two forms of protection of information security have been proposed: logical (Software) and physical (Hardware).

The basic security mechanisms must be studied in depth, such as the identification, authentication, authorization, integrity, confidentiality and availability of information.

Nowadays, there should be a special look at social media as they also allow numerous computer virus attacks, spying for credential copies, user passwords, various codes, allowing to send them to a remote computer and thus, let the Crackers commit the crime.

It is noteworthy that, although it is something that has already been widely studied and disseminated in the literature, the constant study and research on the subject of information security helps prevention, thus reducing unnecessary economic expenses based on preventive measures of security, which are precautionary measures. For computer attacks, for example on servers, it is advisable to install firewall, antimalware, antispyware and use cryptographic techniques, set a strong password, create redundant backups or backups.

As for detection measures, these are needed when you want to monitor or audit security in companies or if there is an attacker tracker. These are measures that can be carried out with the presence of the hired Hacker to monitor all resources and report the security status of the company.

Regarding corrective measures, it is worrying, but its impact is greater when the previous measures are not carried out in their entirety. Finally, it is recommended that, in general, a contingency plan be adopted to avoid attacks on corporate companies so that all the proposed measures can be implemented.

Conclusion

Cyber attacks have brought many difficulties, malware belongs to several groups of computer viruses, such as trojan, worms or bugs, dropper and backdoor, they are the basis of many economic losses, false identity, espionage and data theft, types of computer fraud and sending data to a remote computer, even if they are geographically distant or on different continents.

The economic losses caused by failures in information security have turned into a scandal involving great figures in the world. However, coups, electoral fraud, leaking political information, state secrets and bank diversions have worried everyone. However,

policies to create legislation to punish cybercriminals are the best way out. These cases woke up the international community as corporate governments turned their intentions on information security, which was a national concern that has now become a global problem.

As for these attacks on companies, they are known to be more expressive by Crackers or Hackers , and a less representative number of former employees. To this end, it is recommended that preventive, detective and corrective security measures be used within a security and contingency plan.

The identified and proposed security measures are based on physics and logic. For the control of physical security, special attention is paid to the physical environment of the organization.

Regarding logical security, which is more comprehensive, especially for information security for corporate companies, the suggestion is the use of cryptography, the use of a firewall that allows or prevents the entry or exit of important data packets.

References:

CERT.br. (2012). Cartilha de Segurançapara Internet: Interceptação de tráfego (Sniffing). 4.0-Versão. São Paulo. Disponible en: http://cartilha.cert.br/.

Coopamootoo, K. (2018). Cyber Security: Privacidade online e offline. [vídeo]. Newcastle University. Retrieved from https://www.futurelearn.com/courses/cyber-security/0/steps/19596.

Creswell, J. W. (2010) Projeto de pesquisa métodos qualitativo, quantitativo e misto. In: Projeto de pesquisa métodos qualitativo, quantitativo e misto.

Financial Fraud Action UK. (2017). Fraud The Facts: This category covers fraud on cards that have been. Retrieved from https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf.

Futurelearn. (2018a). Cyber Security: Riscos pessoais decorrentes de violação de privacidade nos negócios. [vídeo]. Newcastle University. Retrieved from https://www.futurelearn.com/courses/cyber-security/0/steps/19598.

Futurelearn (2018b) Cyber Security for Small and Medium Enterprises: What can we learn from this attack? Universidade Deakin. Retrieved from https://www.futurelearn.com/courses/cyber-security-business#what-is-upgrade.

Gonsalez. Y. J. (2011) Que es Protocolo SET. Universidad de le Salle. Retrieved from https://www.researchgate.net/publication/261551164_QUE_ES_PROTOCOLO_SET

Martinelli, H. (2008). *Vírus de Celular: Estudo e classificação para um protótipo de defesa: O início das ameaças: Quanto às formas de propagação mais comuns temos*. Uniritter. Brasil - RS, Porto Alegre.

Laureano, M. A. P. (2005) Gestão de segurança da informação. Retrieved from http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf.

Oficina da Net. (2015) Samsung é condenada a pagar indenização milionária a Apple. Retrieved from https://www.oficinadanet.com.br/post/14544-samsung-e-condenada-a-pagar-indenizacao-milionaria-a-apple.

Oliveira, G. (2009). *Segurança de redes:As ameaças organizacionais.* Escola Superior Aberta do Brasil - Vitoria - Espírito Santo.

Quissanga, F. C. (2015).*Caracterização de vírus informáticos em telefonia móvel celular:Propagação e infecção.*(Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria - Espírito Santo.

Portal de periódicos capes. Missão e Objetivos. Retrieved from https://www.periodicos.capes.gov.br/index.php?option=com_pcontent&view=pcontent&alias=missao-objetivo&Itemid=144.

Terra (2016). Panama Papers. Retrieved from https://www.terra.com.br/noticias/mundo/panama-papers-geram-denuncias-e-investigacoes-em-todo omundo,814039f797239995dea030884e41f8faakajlviv.html.

Date delivered: 14/03/2020
Date reviewed: 14/04/2020
Date accepted: 02/06/2020