Research Focus

Volume 1, Issue 2, 2019, p. 12-26

ISSN: 2668-4675

www.researchfocus.org

Photo by Armando Castillejos on Unsplash

The Importance of Cybersecurity in a Digitalized Society

Cosmina Emanuela Ioana CALIN

Computer Science for Business, Romanian-American University, Romania

Abstract

In the era of digitalization, it is vital to take into great consideration the safety of the virtual data. Being connected in a network (Internet or simply an intra-net connection) can bring a lot of risks to the owner such as the loss of privacy caused by malware software, breaches in the current system or other forms of attacks. The leak of information could become the source of other illegal acts as blackmail, frames or the exploitation of information by the other competitors by sabotaging the company. The software used for protecting the equipment may seem expensive, but the damage that a virus could cause implies much greater costs. The cyber-attacks registered in the EU territory produce annual damage of 400 billion euros. The ransomware attacks were three times more in 2017 than in 2015, and numbers seem to be continuously growing. A study made by EU showed that 87% of the European citizens consider cyber-crimes as a direct threat to the internal security of the EU. For these reasons, the EU Council requested on the 18th of October 2018, a plan to consolidate the cyber-security policy and to combat cyber-crimes.

Keywords: digital, digitalization, security, cybersecurity, virtual attacks, breaches in security

Introduction

Cyber-security has many definitions, one of them being “preservation of confidentiality, integrity, and availability of information in the Cyberspace” (ENISA 2019). In order to begin looking into the cyber-crimes, it is crucial to understand what digitalization means. This term represents the set of actions taken in order to convert physical level data into digitalized documents, organized into systems.

When computers were first invented, the only security that was needed was only on a physical level. Even with the appearance of the first networks, there were not a lot of changes regarding the protection of the computers involved. As the internet has evolved, it has increasingly felt the idea of building a far-gone security system, based on well-documented policies that would function on different levels. The algorithms came to be more complex and difficult to be comprehended by the non-specialized people.

The concept of security is very old but with the appearance of computers, the word developed a new meaning. “Cyber threats are not solely a technical phenomenon, but also a social one” (Bernardo).

Cybersecurity may also have the meaning of a “toolbox” for the client - the means for the user to protect himself from the illegal acts of criminals and implicitly, to protect his own rights such as his privacy or intellectual property. The costs that these actions may imply are medium to high, making it harder for the common user. Also, the importance of this field was hardly discussed by the media, when referring to ordinary citizens. Even now, informative advertisements are not concentrated on this particular field. In turn, people seem to pay little attention to security in general, even in the field of business: “Despite the proliferation of cyberattack capabilities and their potential implications, many organizations still perform poorly with respect to cybersecurity management” (Jalali, Siegel, & Madnick, 2018).

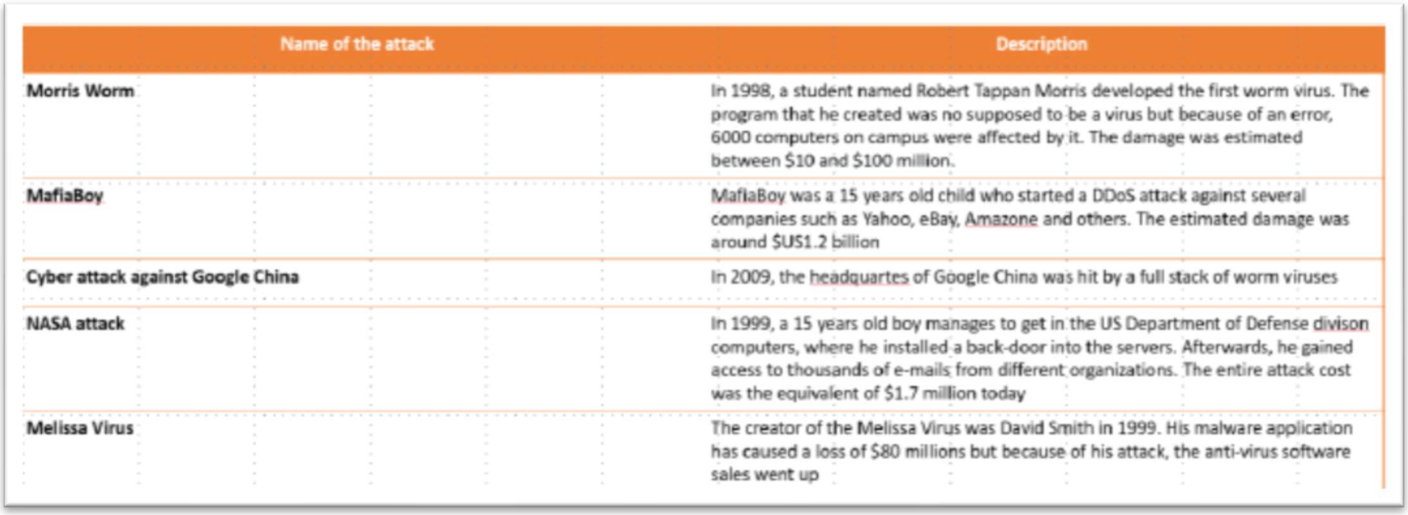
A study produced by GCHQ has shown that 80 % of the anonymous hackers would not stand a chance if prior to the attack, the owners of the businesses had implemented the standard procedures of a basic policy.

In this article, we are going to focus on the importance of security in computer systems by analyzing some of the possible threats to the systems, the way that an attack works and the ways to prevent or solve these virtual security problems. We also intend to take a look into the various fields that may be affected by the infection with virtual viruses and the risks that a company or entity has to face in that specific area. Another important aspect caught in this paper is based on understanding the attacker, by identifying elements of his profile such as his motives or his provenance (education, job, details of his social life).

Consequences of a virtual attack on the client

In order to understand the importance of a well-prepared system in case of an attack, we are going to look through a number of well-known attacks, that happened in the past but which left a trace of uncertainty about the level of security for the clients. Indeed, those illegal intrusions caused great costs for the companies involved.

First, we may summarize some of the older versions of attacks. These attacks were focused on big companies and national organizations.



Name of the attack	Description
Morris Worm	In 1998, a student named Robert Tappan Morris developed the first worm virus. The program that he created was no supposed to be a virus but because of an error, 6000 computers on campus were affected by it. The damage was estimated between $10 and $100 million.
MafiaBoy	MafiaBoy was a 15 years old child who started a DDoS attack against several companies such as Yahoo, eBay, Amazone and others. The estimated damage was around $US1.2 billion
Cyber attack against Google China	In 2009, the headquartes of Google China was hit by a full stack of worm viruses
NASA attack	In 1999, a 15 years old boy manages to get in the US Department of Defense divison computers, where he installed a back-door into the servers. Afterwards, he gained access to thousands of e-mails from different organizations. The entire attack cost was the equivalent of $1.7 million today
Melissa Virus	The creator of the Melissa Virus was David Smith in 1999. His malware application has caused a loss of $80 millions but because of his attack, the anti-virus software sales went up

Table 1 – Attacks on companies between 1998 and 2009

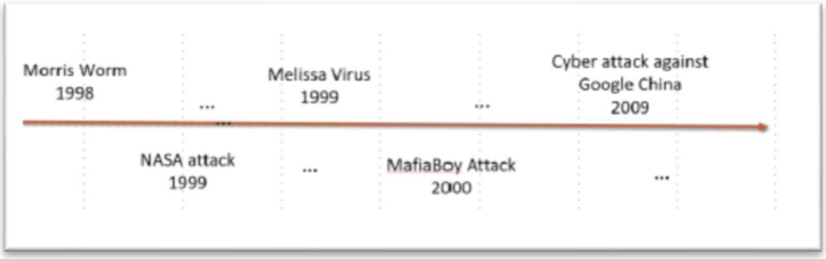
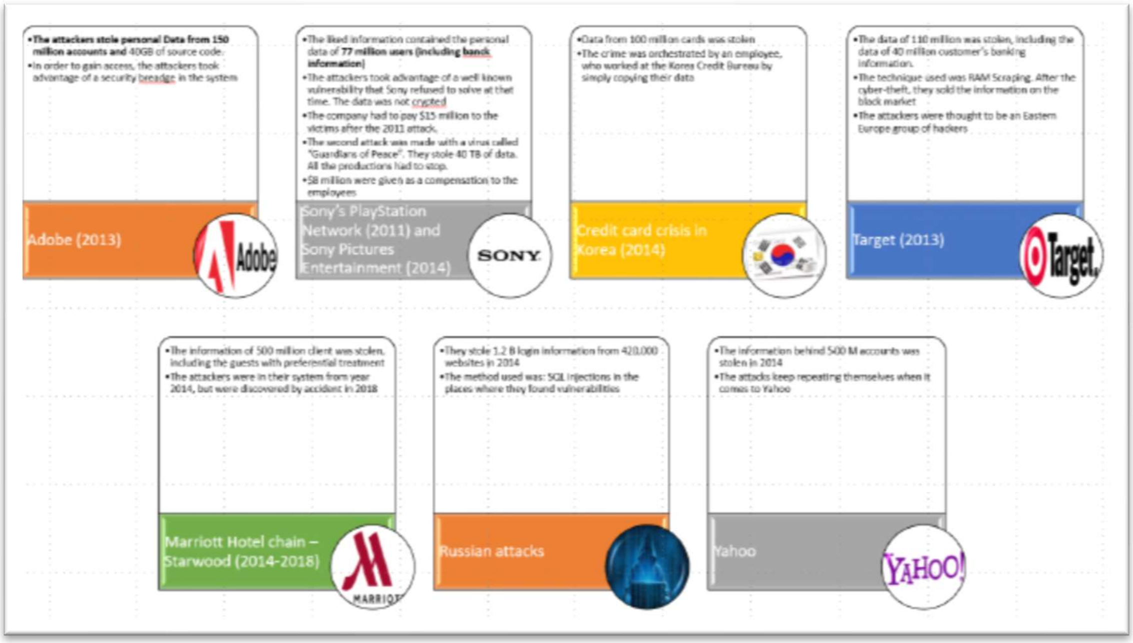


Figure 1. The chronological axis of virus attacks

If we look through the data, we may observe that some of the attackers were barely teenagers, who had a passion for computers. Even so, the damage that they caused was huge. The damage produced by more recent attacks was even greater. It was remarkable how some of the companies made it through. Many firms closed down after major attacks like the ones presented in Figure 2.



- **The attackers stole personal Data from 150 million accounts and** 40GB of source code.
- In order to gain access, the attackers took advantage of a security breadge in the system

Adobe (2013)

- The liked information contained the personal data of **77 million users (including banck information)**
- The attackers took advantage of a well known vulnerability that Sony refused to solve at that time. The data was not crypted
- The company had to pay $15 million to the victims after the 2011 attack.
- The second attack was made with a virus called "Guardians of Peace". They stole 40 TB of data. All the productions had to stop.
- $8 million were given as a compensation to the employees

Sony's PlayStation Network (2011) and Sony Pictures Entertainment (2014)

- Data from 100 million cards was stolen
- The crime was orchestrated by an employee, who worked at the Korea Credit Bureau by simply copying their data

Credit card crisis in Korea (2014)

- The data of 110 million was stolen, including the data of 40 million customer's banking information.
- The technique used was RAM Scraping. After the cyber-theft, they sold the information on the black market
- The attackers were thought to be an Eastern Europe group of hackers

Target (2013)

- The information of 500 million client was stolen, including the guests with preferential treatment
- The attackers were in their system from year 2014, but were discovered by accident in 2018

Marriott Hotel chain – Starwood (2014-2018)

- They stole 1.2 B login information from 420,000 websites in 2014
- The method used was: SQL injections in the places where they found vulnerabilities

Russian attacks

- The information behind 500 M accounts was stolen in 2014
- The attacks keep repeating themselves when it comes to Yahoo

Yahoo

Figure 2. Major virtual attacks on companies between 2013-2018

The graphic presented in Figure 3 shows the probability of being virtually attacked as a company, depending on the geo-region. It can be seen that apparently, Russian businesses have the lowest chances of being attacked.

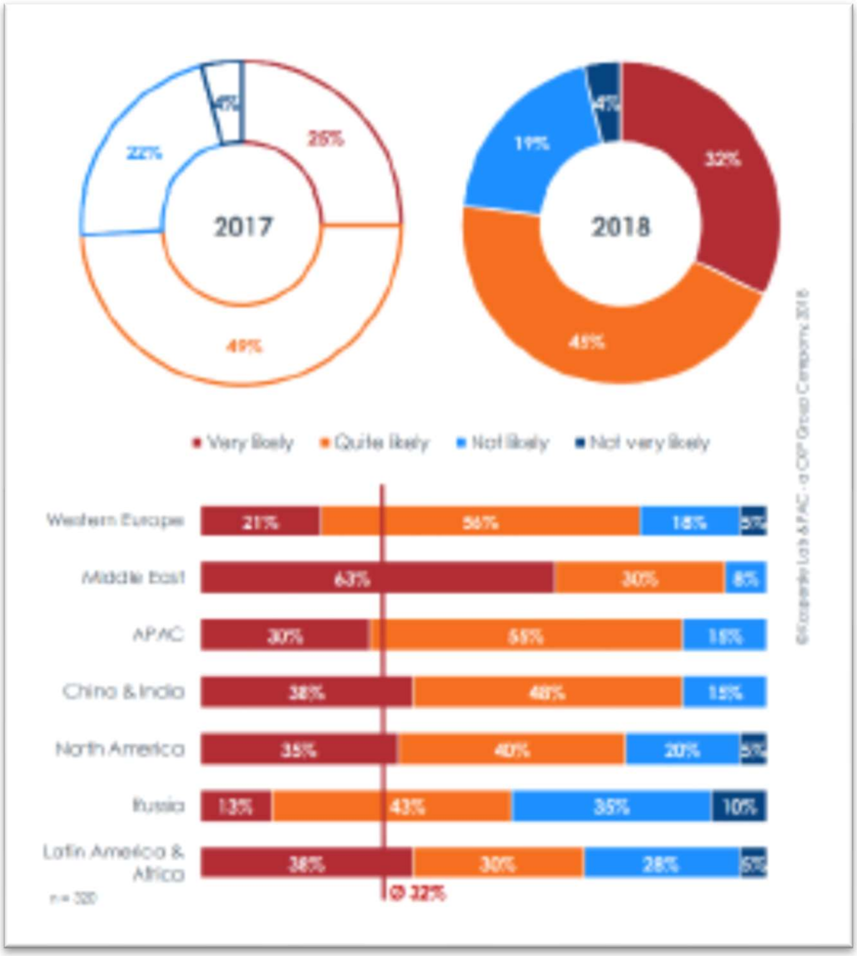


Figure 3. Probability of being attacked, geographical distribution

The profile of an attacker

Attackers may come from different backgrounds, on different levels of education. The motives behind their behavior may vary from the need of power to wishing to gain more money or simply, just for the fun of the game. From this point of view, we can categorize attackers in criminals (people who wish to gain money, steal personal data or other illegal activities), business opponents, hackers or even employees.

According to a study done by Lee Hadlington which was attended by 538 subjects from which 515 responded to all the questions, it was found that the Internet addiction has a relevant connection to the wrong use of it. Statements that had a positive point of view regarding cyber security, were associated with a negative meaning. The study used a set of instruments defined in its content. The subjects were employees from different sectors, that worked different amounts of time.

Nowadays, a problem that is of much concern, is the addiction of children to the Internet and Smartphones. They spend hours behind the display and even in schools, they refuse to turn off their mobile devices. This matter was analyzed in Finnish research work, that concluded in admitting that the alarming number of children who were genuinely interested in gadgets is growing. They proposed a possible solution in which the educational system would embrace a northern approach that consists of letting the children write and study on tablets and promoting the e-learning method. After the study, the model was applied. After a year, the students and their parents were asked on how they viewed the system and if they would enjoy continuing it. The answer of the majority was that they preferred the classical system.

The basic ways to attack a system

We are going to discuss some of the most used methods for breaking in a system. We will also take a look into what the main vulnerabilities are and how a hacker could exploit them.

Even though there are hackers that have the knowledge to break into some of the most secure systems in the world, the majority of them do not reach a professional level in the true sense of things. Some of them use small applications taken from the internet or that were given from one person to another. In both cases, the application has a GUI that is very easy to use (just by pressing a button you could provoke damage). Not all the malware applications have a specific target – the computer chooses the target randomly until it can find one or more victims.

These are the main types of attacks that could damage a system (the list does not include all the possibilities):

1. **Attacks that are focused on finding the password**: the application is based on a series of permutations (unless the found name corresponds to the password, the algorithm will go to the next attempt)

2. **DDoS:** this kind of attacks work on a very simple principle – the application sends a great number of requests in order to block the server. This is made by using a botnet (a series of bots=infected computer that responds to the hacker)

3. **DDoS extraction:** the attacker asks for money in exchange for not closing down the whole platform

4. **Malware:** these programs are formed using code sequences that have a destructive/malicious purpose:

5. **Spyware:** software that spies on the victims, without them knowing

6. **Worms/Viruses**

7. **Ransomware:** the attacker blokes a file and asks for money in exchange for the needed files

8. **Phishing:** a large number of emails sent to the potential victims. Their role is to convince the user to give up data or money to them (may take place in the business environment or in the private sector). In order for the messages to be persuasive, they come with a captivating story that involves earning money if the victim agrees on helping them or other similar stories;

9. **Spearphishing:** follows the same logic as the one above, but the difference is that the mail seems to be written by a known person, who needs help;

10. **Monetary-Fraude:** the attacker disguises himself as the CEO or CFO to ask for certain amounts of money to be transferred into an account given by him, on the premises of closing a new contract.

11. **Man in the Middle:** it represents an attack in which the attacker intrudes in the line of communication of two working stations, via a network. There are several types that include:

a) an infected Hot-Spot (the attacker uses his hot-spot as a free wi-fi network; when the victim connects to it, the attacker can start stealing data from the infected piece of equipment)

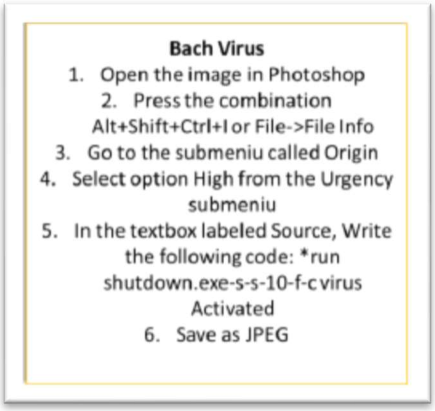
b) ARP Spoofing (when a server tries to connect to another, it uses the IP address. When the MAC is unknown, the server askes in the network for the piece of equipment who has that particular IP address. At that moment, the attacker sniffs in and declares his computer as being original one.

c) mDNS S. – the application works the same, except that it is used for internal networks

d) DNS S. – the attacker inserts a DNS fake cache to a server, using the name of the domain

Techniques used for these types of attacks are sniffing methods, inserting corrupted codes, stealing data when running a session or the removal of SSL.

12. **Steganography** – may be defined as the art of concealing data in other forms of data (a small hidden text in a message). This method is used sometimes by hackers to communicate with one another. This method may also be used to infiltrate viruses into picture (when the victim downloads the picture, the virus would be saved automatically in the computer with the picture (Figure 4).



Bach Virus

1. Open the image in Photoshop
2. Press the combination Alt+Shift+Ctrl+I or File->File Info
3. Go to the submeniu called Origin
4. Select option High from the Urgency submeniu
5. In the textbox labeled Source, Write the following code: *run shutdown.exe-s-s-10-f-c virus Activated
6. Save as JPEG

Figure 4. Example of a Batch Virus

13. **Miner malware** – The miners infect victim’s computers by inserting malware codes on websites (when a user clicks inside the page, a new webpage would appear and the virus enters the system. These are mainly used by miners to create a cryptocurrency with the resources of the victim’s computer). The number of attacks has gradually declined because of the decrease in the cryptocurrency value.

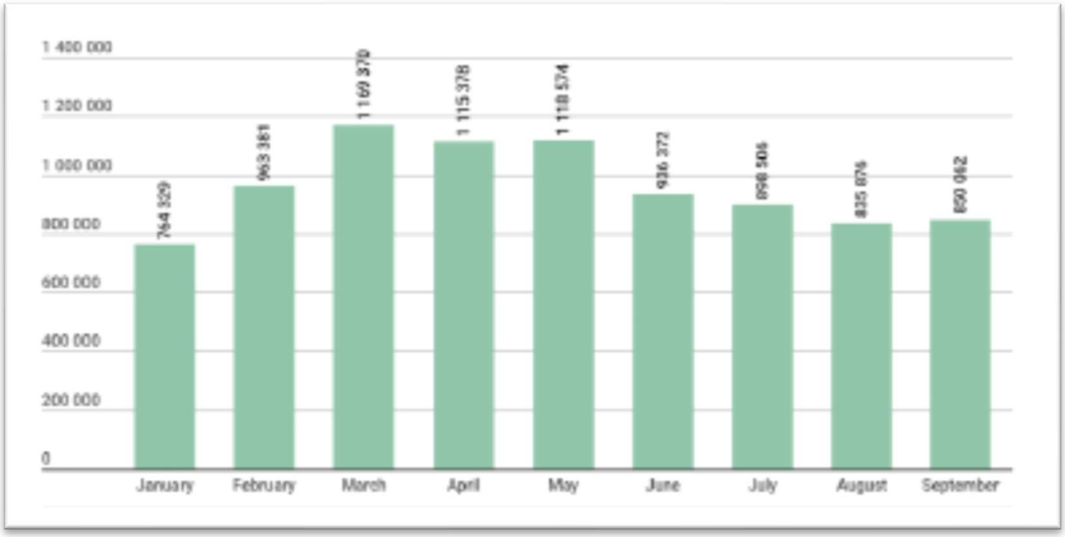


Figure 5. Number of miner attacks on individual computers in 2018

Given the fact that we have seen a number of possible threats, we now shall pursuit some of the most common vulnerabilities that we may encounter in a system:

- The absence of a number of functions in Access Control
- The password may be short and very easy to be broken
- Mediocre or nonexistent security policy
- Ignorance and/or unwillingness to invest in security software
- Unlimited access to the equipment
- Zero-day attack (when the intruder figures the vulnerability of a well-preserved system)
- Opening random e-mails or sites
- Security breaches
- Not having implemented a proper policy
- Not having software designed for security or programs that are not very well configured (antivirus, Spybot, firewall, etc.)

Different activities that could be subjected to virtual attacks

With only a few exceptions, users from all fields could be attacked by a cyber-criminal. There are software programs that run until they find an easy to attack system, infect it and then start again. The only people who are not susceptible to these forms of injustice are the people who don’t have a computer or at least, not having it connected to the internet (this category includes not only computers but also other gadgets and pieces of equipment).

As it was shown at the beginning of the article through statistics given by well-renowned institutions and organizations, classical attacks on computers and smart devices (phones, tablets, smartwatches, smart TVs) have become very common. However, we have to assess the possible damages in order to decide on the most suited strategy and the most important area to protect.

Another problem that affects greatly is caused by uncommon attacks, that do exist and could cause unthinkable damage to the victims. These possible scenarios seem to be taken out of an SF movie.

In the medical field, a hacker would generally attack a network of a hospital or of a clinic in order to manipulate certain parts of data. In a study written by Adrian Baranchuck and his fellow colleagues, it was proven that a cyber offender could also hack into an insulin pump. The experiment was conducted for Medtronic devices and also for the Johnson & Johnson equipment. The same goes for the pumps that have the role of infusing drugs. For these kinds of actions, the repercussions could be deadly.

In the same kind of situation could be an aviation company. From gaining access to the data of the clients and the employees to being able to affect the safety of the flights represent the major concerns for the airline companies. A mistake could cost not only money or involve several lawsuits, but also the life of individuals. In order to protect the customer’s safety, companies invest large amounts of money.

Another phenomenon that emerged in recent years is the cyberbullying, especially among teenagers. This is a form of virtual violence in which, unlike the normal methods, the perpetrators use specific instruments (blackmail, slender, pictures or videos taken in secret or stolen from the victim’s computer or phone, verbal violence and so on) to virtually harass their victims through social medial. This type of violence does not necessarily involve hacking, but the use of digital means to provoke damage. The effects caused by these personal attacks are worse than we could imagine: depression, low self-esteem and even suicide. In Romania, in 2018, only 11% of the parents have declared that their children were virtually abused. In general, only 34 % of the kids around the globe tell their parents about being bullied.

Kids may also be manipulated into giving personal data of their parents. Social media and online games are only some of the tools for the attacker to get in contact with the child.

Methods used to prevent security attacks

In some cases, attacks are easier to develop (the whole process has the same planning as of a virtual application) despite the system designers preoccupation to predict possible attacks and do solve them before it is too late. IT specialists try to find ways to implement more secured systems and ways to determine when security violations are most predictable to occur.

Unfortunately, most people don’t consider themselves as potential victims, thinking that they do not have to hide any information. It was confirmed that approx. 80 % of the people don’t follow a regular security policy.

An experimented was conducted under the form of an online game. The experiment was conducted in two rounds. It was shown that the professional IT subject solved the tasks better than the non-professional subjects in the first round when the attacks were known to happen. On the second round, when the attacks were completely unknown, the two groups performed at nearly the same level.

One of the proposed solutions for detecting attacks was a way to evaluate virtual risks in a holistic way. The authors use a confidence network for the purpose of integrating trust as a parameter in a human-based category of users, for the purpose of quantifying most of the information into several trust segments. Each of the segments was then discussed and also, the relationships between them.

There are a few steps to follow when designing any kind of security policy as it may follow:

1. Analyze the current system and identify the sensitive information

2. Always update the policy that you follow

3. Define security levels for each member/employee

4. Teach the members/employees about security issues and ways to protect the information on the internet

As can be seen, being able to prevent attackers from gaining access to unauthorized documents is a very hard and long-time process, with great financial costs, including solutions such as:

1. A good antivirus program (from an established provider)

2. A Spybot for detecting the viruses that pry on the system

3. A well-set firewall

4. IP white lists (permit access to the intranet or platform only to people with security clearance)

5. Use only sites that have certain certificates like SSL

6. Use applications that have a security module included

7. Data encryption

    a. Private/symmetric key – both computers (the receiver and the transmitter) have the key

    b. Public/asymmetric key – The key is published but only the receiver has the key to access it

    c. Models that use to first encrypt the data with an asymmetric key and then the result encrypted with a symmetric key

8. Steganography and digital holography – to mark the authenticity of data

9. Respect the standards of PCI-DDS

    a. Designing, implementing and maintaining a safe connection (firewall, good password)

    b. Protecting the data of the clients (secured DataStores, encrypted-data)

c. Implementing and updating management of risks application

d. Keep track of the number of visits (limit the number of times a user can enter)

e. Testing and monitoring the hole network

f. Upgrade the security policies

10. Use certificates for your website (SSL)

11. Add a 2FA authentication module – log-in in two steps

12. Create alternative account for a better control

Importance of catching the culprit

Hackers that perform illegal acts are punishable by law. Those who commit acts of terrorism, harass their victims or steal their personal data or money should specifically be found in order to stop them from further criminal acts. The investigation is generally conducted by the police or other competent institutions.

Articles on digital forensics could be found on the Internet but with difficulty, because of the lack of sharing data on this particular field. This problem was addressed by Cinthya Grajeda and her esteemed colleagues in their article on digital forensics, using multiple datasets.

Conclusions

Children are able to evolve faster because they got the chance to gain access to information, information that in the past took a long time to gather. By playing games, they get to exercise the movements of their fingers and reflexes. By watching online videos and only by simply typing some letters, they get to learn foreign words and become resourceful. Their safety on the Internet is a matter of concern but with good supervision and a parental app, everything would go smoothly.

Having the floors cleaned by a robot, making food and sweets with mixers and other kitchen equipment, having the possibility to control the central heating from afar by simply touching the phone are activities that were considered implausible in the past but common now. These examples were presented only to show the incredible development in a mere number of years.

Cybersecurity represents only a mean into achieving the full potential of technology. Its importance is undoubtedly critical, given the possible risks that a user has to face such as the loss of money and prestige and loss of intellectual rights.

“There is no 100% security. You’re just trying to defend yourself, but threats always exist... we’re always vulnerable to the threat” (Oil and Gas industry, UAE). This citation may be true, but with enough interest, we can level-up the safety and integrity of our system

References

Jalali, M., Siegel, M., & Madnick, S. (2018, 03 09),Decision-making and biases in cybersecurity capability.

Hadlington.Lee (2017.06.23),Human factors in cybersecurity;Examining the link between Internet addiction,impulsivity,attitudestowards,cyber security,and risky cyber security behaviours.

Metropolitan Police(2017), The Little Book of Cyber Scams

Paakkaria,Antti, Rautiob, Pauliina,,Verneri, Digital labour in school: Smartphones and their consequences in classrooms

Grajeda,Cinthya, Breitinger, Frank, Baggili, Ibrahim (2017), Availability of datasets for digital forensics - And what is missing

Dufva, Tomi, Dufva, Mikko (2018), Grasping the future of the digital society

Noam,Ben-Asher, Gonzalez, Cleotilde (2015), Training for the unknown: The role of feedback and similarity in detecting zero-day attacks

Baranchuk,Adrian,… (2018), Cybersecurity for Cardiac Implantable Electronic Devices

Bernardo, Danilo V. (2015), Clear and present danger: Interventive and retaliatory approaches to cyber threats

Henshel, D., Cains, M. G. ,Hoffman,B.,Kelley, T. (2015), Trust as a human factor in holistic cyber security risk assessment

https://www.sita.aero/air-transport-it-review/articles/lets-tackle-the-cyber-threat-in-aviation

https://www.mro-network.com/big-data/cyberattacks-and-aviation-sector-how-can-airlines-best-prepare

https://www.comparitech.com/internet-providers/cyberbullying-statistics/

http://www.bullyingstatistics.org/content/cyber-bullying-statistics.html

https://techjury.net/stats-about/cyberbullying/

https://www.phocuswire.com/SITA-Air-transport-IT-cybersecurity

https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/ - The data was used for Table 1

https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks - The data was used for Fig. 2

https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/

ENISA,Industry 4.0 Cybersecurity: Challenges & Recommendations

Please cite this article as:

Calin, C. E. I. (2019). The Importance of Cybersecurity in a Digitalized Society. Research Focus, 1(2), 12-26. DOI: https://doi.org/10.36068/1.11

Research Focus. International Open-Access Scientific Journal for Students and Graduates Research

ISSN: 2668-4675