Digitalization concept: Cyber-risks and damages for companies in adhered industries

C Vartolomei[1] **and S Avasilcăi**[1]

[1]"Gheorghe Asachi" Technical University of Iasi, Department of Engineering and Management, Mangeron Blvd. 28, TEX1, 700050, Romania

cristian.vartolomei@tuiasi.ro

Abstract. Starting with the modern binary number system in 1679, followed by the universal computation as a result of the Boolean algebra in 1847, then continued in 1948 with "Mathematical Theory of Communication", capacitors and microchips between 1950s and 1970s, Apple I desktop computer in 1976 and until 2020 when we have devices as smartphones, computers, laptops, smart houses, cities and cars, all these inventions are small but realistic steps that built the current concept adopted by the humankind, called digitalization. Considering this impactful concept during our research, we propose to perform a literature review regarding its implementation in industries as medical, banking, automotive, along with generic examples from undefined ones, followed by the risks and disasters as a result of cyber-attacks, which can be seen as disadvantages of implementing this concept. In the end, we propose to discover the effects on the virtual business environment by exemplifying the cyber-attacks and analyzing them.

1. Introduction

Digitalization has begun to make its presence known with the transition from physical paper documents to digital ones. In this way, the beneficiaries of joining the technologies that made this possible, have observed that these types of digital documents offer them a more accurate way in manipulating the data, finding and reviewing the mistakes, along with a much faster writing speed. From this point on, the mankind began to work on the development of these technologies, to the point where it ensured the interconnection of a variety of systems such as smartphones, laptops, tablets, autonomous cars and smart homes and cities through communication channels as satellites, optical fiber and wireless networks. But even if the benefits of joining this concept continue to evolve, at the same time it joins the disadvantages of accessing data from a system connected to the Internet from anywhere in the world by different cyber-attackers, having an increased level of knowledge regarding the information systems technical side, being able to penetrate the host system and stop its functionality, tamper with its data or steal the information.

The main purpose of this paper is to perform a literature review regarding the impact of the digitalization in different industries, by highlighting in the beginning the way that cardiology medical field, along with the banking and automotive industries have evolved adhering to and implementing different technologies. Along with the aforementioned aspects, this paper also aims to classify the cyber-attacks that can be performed on companies which implemented the digitalization, in order to not being displaced by competition and ensuring benefits as, fast access to information, low handling and storing costs, a better communication between the employees and with the clients, a better organization within

the company, increasing the profit and delivering a qualitative service/product. In this way, by performing this research, we look forward to obtain and enumerate the effects on the virtual business environment for the companies in different industries, as results of cyber-attacks.

2. Digitalization in various industries at a glance

Digitalization has always been important for the humankind, because, for example, considering the medical technologies used for establishing diagnoses, it offered a new and more accurate perspective for the doctors, starting from the arrival of the patient to the hospital until he leaves at home, in some cases without any disease. In this way, considering the cardiology field in medicine, the fact that it has so far occupied the world rank as a mortality rate, cardiovascular diseases are becoming a field of exploration in creation the concept of artificial intelligence, that is an important aspect of the digitalization process. Early detection, accuracy and fast diagnosis are the three most important pillars in active research. Detection of electrical changes at the cardiomyocytes level, before these will become electrocardiographically visible, as well as the detection of episodic atrial fibrillation in a heart with apparently normal rhythm are two useful medicinal tools in a more accurate assessment of myocardial infarction risk, heart failure, as well as the risk of being hospitalized again in the coming years [1].

Along with this example, the banking field has also took advantages by offering the availability of the services 24/7 to the clients, most used one at the moment being the internet banking (available on a computer, a smartphone or a tablet), which ensure national and international money transfers, payment of the invoices, opening of savings accounts and last but not least, payments to the online stores.

Another important field which due to the adoption of the digitalization had a significant impact regarding the product offered to the customer is automotive, by implementing the following concepts:

- Autonomous Driving (AD) – vehicle that is able of sensing its environment and proceeding in a safe way with almost no human interaction [2];
- Connected Car (CC) – vehicles are connected through different communication channels, as Vehicle to Vehicle (V2V) (intercommunication between vehicles in a defined range), Vehicle to Infrastructure (V2I) (communication with a network of vehicles or road infrastructures), Vehicle to Pedestrians (V2P) (a pedestrian can use a computer or mobile application in order to locate nearby taxis along with the estimation of the arrival time – e.g. Uber) and Vehicle to Network (V2N) (different organizations are able to connect with the connected car in order to alert the drivers regarding different changes as weather conditions or traffic jams) [3];
- Internet of Things (IoT) - vehicle that got implemented in its architecture internet connectivity through LAN and WLAN, giving the possibility to access/send/download data and communicate with Internet of Things devices [4];

But even if the adoption of this concept has so many advantages for our actual level of technology progress in various industries, the rise of disadvantages is directly proportional considering the cyber-attacks which can occur.

3. Risks and disasters as a result of cyber-attacks

In order to classify the cyber-attacks which can occur over a company adhered to the digital transformations, during this research we will use the STRIDE model, developed by Microsoft in order to identify computer threats, in six categories as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege [5].

In this way, Figure 1 classifies the attacks from the second row (excepting the “Attack Class”) in subcategories of the STRIDE model (first row), all of them being defined as attack classes, by the followings:

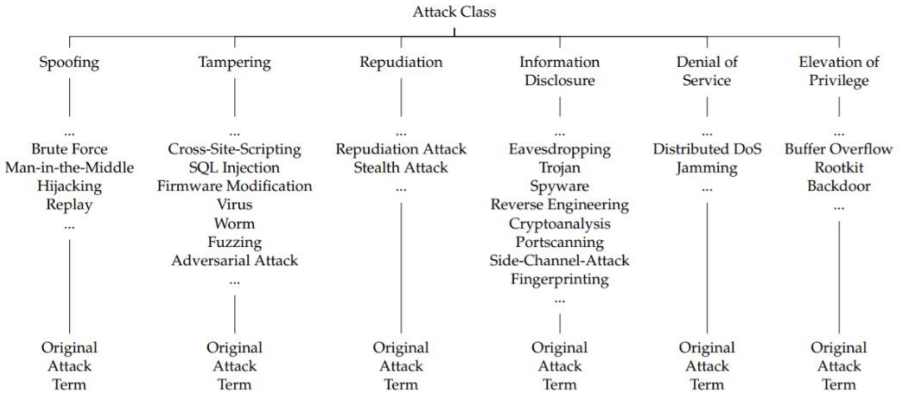

Figure 1. Classification of the attacks based on STRIDE model [6]

3.1 Spoofing

Spoofing element is defined by the brute force attack, in which an attacker can perform authentication attempts on an organization's system in order to obtain access on it, followed by the Man-in-the-Middle (MiM) used to capture and (depending on the attack) to tamper, (e.g. with the data traffic between an employee and the customer), hijacking that results in taking over the control of an established Internet connection between two or more parties [7] and replay attacks where a client-server communication is maliciously or fraudulently repeated or delayed [8], in order to make it unavailable.

3.2 Tampering

In the Tampering element, Cross-Site-Scripting (or XSS) is a type of attack in which the attacker inserts a malicious script in an organization's web-page's field, in order to behave in ways as, e.g. stealing user's credentials. A successful SQL Injection will steal all the info from an organization's database and a firmware modification will change the behavior of a hardware system (e.g. router, switch, smart TV, etc.), while a virus or a worm will replicate itself in order to spread to other systems in the organization's internal network [9]. In the end, a fuzzing attack will send crafted input in order to obtain some traces that will make the attacker to further understand the functionality of a system (being it hardware or software). Also, an adversarial attack is performed in a structured way, considering the level of information gathered, in this concept artificial intelligence being involved.

3.3 Repudiation

Repudiation element, containing also the stealth attack, happens when an organization does not adopt controls to properly track users' actions, thus permitting malicious manipulation of further actions [10], in this way giving the possibility to the attacker to steal data from an organization without being detected.

3.4 Information Disclosure

In Information Disclosure we find some various attacks, as eavesdropping which is performed by capturing data from unencrypted communication channels, followed by the trojan malware which is used to delete, block, modify, copy or corrupting organization's or customer's Intellectual Property (IP) [11]. Forwards, spyware can be defined as being a software used for stealing the internet browsing history (and not limited to) [12], reverse engineering used in decompiling (e.g. an organization's software, in order to obtain its source code for various further attacks), cryptoanalysis that is the study of analyzing an encrypted connection between two parties in order to access the information exchanged [13], port scanning which is a technique used in finding open ports and related running services for an operating system [14], Side-Channel-Attack that breaks encrypted data by monitoring the electromagnetic field radiation emitted by a computer screen to view the data before the encryption

process [15] and traffic fingerprinting, that sniffs an encrypted communication in order to analyze the packets' flow pattern [16].

3.5 Denial of Service

The difference between Denial-of-Service and Distributed Denial-of-Service is that the first one uses only a source to flood until unavailability a victim's system (e.g. an entire organization or only an employee), while the second one uses multiple sources. Also, jamming attack is used in the field of wireless sensor networks, by redirecting electromagnetic signals in order to disturb or interrupt the signal transfer.

3.6 Elevation of Privileges

Elevation of Privileges contains Buffer Overflow, Rootkit and Backdoor. The first one is used in leading a program to put much more data in a buffer that it can hold, while the difference between the followed attacks is that a Rootkit will be applied as a set of software that are used by an attacker when finally gained access to the victim's machine, in order to establish an open-way for anytime he wants to turn back without being detected. In the end, a Backdoor is used to access the victim's machine by installing, e.g. a virus or even by legitimate programs [17].

4. Effects on virtual business environment

Considering all the types of attacks that have been mentioned in the last chapter, during our research we discovered that the effects on the virtual business environment can be defined as:

- Loss or damage of the hardware and software systems that are leading in generating extra expenses for an organization (e.g. in 2014, financial fraud actions in e-commerce in UK lead to costs of £217.4 million, and £60.4 in online banking frauds [18]);
- Loss of income as a result of various attacks that stopped the activity for a period of time or by not having access to the IP anymore (e.g. Kaspersky reports that the average cost for a company as a result of a DDoS attack was $2 million, in 2017 [19]);
- If an attacker steals the IP of a victim's customer, then the victim can be sued for information leakage (e.g. Company Zynga Inc. has been sued in the district of California because a hacker claimed to have accessed the company's database and stolen 218 million user accounts [20]);
- The extorsion losses, as being blackmailed by an attacker to pay a big amount of money in order to not make public some information about own or customers' IP (e.g. In 2019, hackers blackmailed a German IT company with stolen financial and private information whose clients include Oracle, Airbus and Porsche [21]);
- Last but not least, a cyber-attack can damage an organization's reputation in a very serious way, leading in being very hard to find a new customer to deliver a service or a product (e.g. Company TalkTalk received complaints from customers who were waiting to be compensated as a result of a cyber-security breach in October 22, 2015 [22].

5. Conclusions

In the end, along with the literature review regarding the digitalization transformations in the cardiology medical field and industries as banking and automotive, during this research we also described different types of attacks on companies from any industry that implemented the technologies as a part of the aforementioned concept, based on categories provided by the STRIDE model.

Considering all these aspects, we can conclude that the cyber-attacks are a very serious risk for all organizations which adhered to the digitalization, because depending on the attacker's knowledge and capabilities, all the software and hardware used by an employee can be attacked in different ways and with different purposes. In this way, the impact in the virtual business environment can wear a significant risk for the attacked company, as losing the trust on the market regarding the security of the clients'

Intellectual Property, brand's reputation, extra-expenses which can occur, unavailability of the company's both hardware and software systems (which are used by the employees in the development of the product/service or in the communication with the market or with the customers), along with the blackmail situations in which a company can be pushed.

References

[1] Mayo Clinic Artificial Intelligence in Cardiology: Introduction to A.I. https://www.youtube.com/watch?v=mGODKIbiXpE

[2] Taeihagh A and Lim H S M 2019 Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks Transport Reviews 39 (1):103-128. arXiv:1807.05720. doi: 10.1080/01441647.2018.1494640. ISSN 0144-1647

[3] Application of IoT in Automotive Industry. Future of Automobiles https://www.biz4intellia.com/blog/iot-applications-in-automotive-industry/

[4] Kaya I 2018 Connected Car Experiences in 2019: Exploring the Possibilities https://www.cmswire.com/digital-experience/connected-car-experiences-in-2019-exploring-the-possibilities/

[5] Wikipedia https://en.wikipedia.org/wiki/STRIDE_(security)

[6] Sommer F, Dürrwang J and Kriesten R 2019 Survey and Classification of Automotive Security Attacks MDPI 10(4): doi.org/10.3390/info10040148

[7] Rouse M Email spoofing https://searchsecurity.techtarget.com/definition/email-spoofing

[8] Wikipedia https://en.wikipedia.org/wiki/Replay_attack

[9] Wikipedia https://en.wikipedia.org/wiki/Computer_worm

[10] OWASP https://owasp.org/www-community/attacks/Repudiation_Attack

[11] Kaspersky https://www.kaspersky.com/resource-center/threats/trojans

[12] Norton https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

[13] Wikipedia https://en.wikipedia.org/wiki/Cryptanalysis

[14] Whatismyip from https://www.whatismyip.com/port-scanner/

[15] Porup J M 2019 What is a side channel attack?How these end-runs around encryption put everyone at risk https://www.csoonline.com/article/3388647/what-is-a-side-channel-attack-how-these-end-runs-around-encryption-put-everyone-at-risk.html

[16] Gu X, Yang M, Zhan Y, Pan P and Ling Z 2018 Fingerprinting Network Entities Based on Traffic Analysis in High-Speed Network Environment Intrussion Detection and Prevention in Cloud, Fog, and Internet of Things doi.org/10.1155/2018/6124160

[17] Sqasolar https://www.sqasolar.org.uk/solar/material/IS01CGCD/page_19.htm

[18] Understanding the costs of cyber-crime. A report of key findings from the Costs of Cyber Crime Working Group 2018 Home Office Science Advisory Council https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf

[19] Kobialka D 2018 Kaspersky Lab Study: Average Cost of Enterprise DDoS Attack Total $2M https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/

[20] Coble S 2020 Zynga Facing Lawsuit Over Data Breach https://www.infosecurity-magazine.com/news/zynga-facing-lawsuit-over-data/

[21] Hamilton I A 2019 Hackers have stolen a ton of data from IT company whose clients include Oracle, Airbus and Porsche https://www.businessinsider.com/hackers-stole-data-from-citycomp-and-are-blackmailing-the-company-2019-4

[22] TalkTalk case study: reputational risk of cybersecurity attacks 2015 https://www.alva-group.com/blog/the-reputational-risk-of-cyber-attacks-talktalk-case-study/