©LUMEN Proceedings

Available online at: http://lumenpublishing.com/proceedings/.../rec-november-2017/

18th edition of the Conference "Risk in Contemporary Economy", RCE2017, June 9-10, 2017, Galati, Romania

Risk in Contemporary Economy

Information Security – A Growing Challenge for Online Business

Gabriela GHEORGHE*, Ioana LUPASC

https://doi.org/10.18662/lumproc.rce2017.1.14

How to cite: Gheorghe, G., & Lupasc, I. (2017). Information Security – A Growing Challenge for Online Business. In S. Hugues, & N. Cristache (eds.), *Risk in Contemporary Economy* (pp. 164-171). Iasi, Romania: LUMEN Proceedings. https://doi.org/10.18662/lumproc.rce2017.1.14

©LUMEN Proceedings
International Scientific Conference Risk in Contemporary Economy | RCE 2017 | 9-10 June 2017 | Galati – Romania

Information Security – A Growing Challenge for Online Business

Gabriela GHEORGHE*[1], Ioana LUPASC[2]

Abstract

In present, the cyber attack move to a global scale, also the online business cyber threats have the effect of impeding and even huge losses. Security issues currently facing online commerce, online payment systems require finding solutions to improve the security solutions offered by the providers of Business Information solution.

Keywords: *Information technologies, Business Intelligence tools, data mining.*

1. Introduction

A global cyber-attack using hacking tools hit international shipper FedEx and infected computers in 150 countries in May, 2017.

The strongest attack with a specific strain of ransomware hit University College London. UCL first reported problems at email servers. It believes a phishing email, sent around midday, resulted in the ransomware gaining a foothold on its servers, where it began spreading through the university's N (network) and S (shared) drives. In a couple of hours it had restricted access to those drives, and they are currently available in read-only mode for students and staff.

The university is warning that it may be a "zero-day" attack – one not seen in the wild before – due to the fact that it was not picked up by its antivirus software.

[1] Dunărea de Jos University of Galati, Romania, gabriela.gheorghe@ugal.ro.
[2] Dunărea de Jos University of Galati, Romania, ioana.lupasc@ugal.ro.

https://doi.org/10.18662/lumproc.rce2017.1.14
Corresponding Author: Gabriela GHEORGHE
Selection and peer-review under responsibility of the Organizing Committee of the conference

University College London Hospitals, an NHS trust closely associated with the university, decided to suspend their email systems, as a "preventative measure".

Leading international shipper FedEx Corp was another high-profile victim, while in Spain Telecommunications Company Telefonica was among many targets in the country. Portugal Telecom and Telefonica Argentina both said they were also targeted.

In Germany, railway operator Deutsche Bahn was a high-profile target, with screens at stations showing the ransonware message.

Chinese state media say more than 29,000 institutions across the country have been infected, while in Japan, 2,000 computers at 600 locations were reported to have been affected. [1]

In Romania, companies from the energy, transport, telecom and car sectors were affected.

The Dacia Mioveni plant was also affected, production being stopped.

The countries most affected by WannaCry to date were Russia, where the Interior Ministry was hit, Taiwan, Ukraine and India, according to Czech security firm Avast.

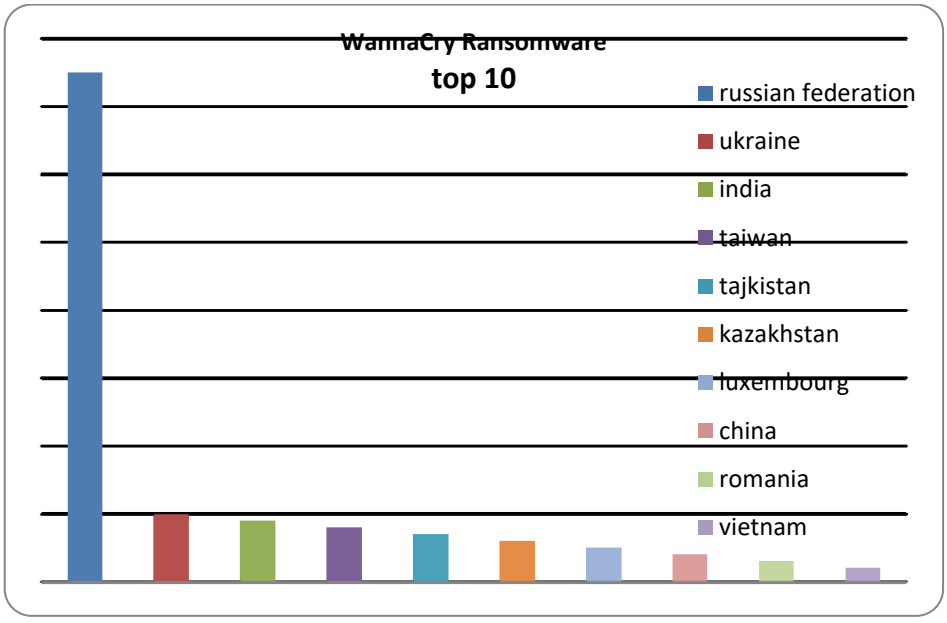

Figure 1. Attack distribution by country – top 10
[source: securelist.com] [2]

2. Problem Statement

Ransomware is malicious code that is used by cybercriminals to launch data kidnapping and lockscreen attacks. The motive for ransomware attacks is monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in virtual currency to protect the criminal's identity. [3]

Ransomware malware can be spread through malicious e-mail attachments, infected software apps, infected external storage devices and compromised websites.

Once your computer has been affected, it locks up the files and encrypts them and demands payment in bitcoin in order to regain access.

A group of 13 countries joined the "No More Ransom" global project initiated by the Netherlands in 2016: Bosnia and Herzegovina, Bulgaria, Colombia, France, Hungary, Ireland, Italy, Latvia, Lithuania, Portugal, Spain, Switzerland and the United Kingdom.

Thus, employees and managers need to realistically assess each new application that comes along. Sometimes people focus only on the good side, and fail to adequately prepare for the inevitable challenges. Other people focus only on the risks, and fail to harness the potential of the new technology. Either approach falls short of effectively managing IS. Only by simultaneously considering both sides of the Double-Edged sword can managers expect their organizations to realize the awesome potential of new technologies. [4]

3. Risks associated with cyber-terrorist attacks

The worst scenario we can imagine is a nuclear war, triggered by a computer virus. But as a result of the recent cyber attack, we can assume that there is a fairly high risk that a nuclear plant will no longer work in parameters and get damaged by a virus that takes control, preventing authorized access.

These risks cannot be ignored, it is clear that security measures should be adapted to these new threats.

On 13 May 2017 nuclear power production in Romania was abruptly disrupted over a period of several hours, the stop was done for safety reasons to apply updates in order to prevent cyber attack. [5]

Figure 2. Roumanian national energetic system
Source: *sistemulenergetic.ro* [6]

"These attacks point out that the criminals will exploit any vulnerability in the system, and also, no sector can be considered immune to attack and need to constantly review its security procedures," said Interpol Digital Crime Center director Sanjay Virmani. [7]

Unlike ATMs that are connected to a dedicated, secure network that does not allow direct interaction with Internet Networking, the online payment system is vulnerable to cyber attacks and we have many examples of successful attacks.

The Carbanak Group used carefully composed emails in an attempt to mislead some selected employees of the bank, to open malicious files, a technique commonly known as "spear phishing".

In this way, hackers could gain access to the bank's internal network as well as to the bank's video surveillance system to imitate the way bank employees work when transferring money.

In some cases, Carbanak took remote control of ATMs and ordered them to release cash at a pre-set time when a group member expects to collect the money.

JP Morgan Chase, the first US asset bank, was the target of a massive cyber attack targeting over 76 million customers and 7 million small and medium businesses, but no fraudulent operations were reported.

Hackers have stolen data such as their clients' names, their phone numbers or e-mail addresses, but they have not been able to peculate passwords, birthdates and social security numbers.

Mirai, a type of malware, disrupted in 2016 internet service for more than 900,000 Deutsche Telekom customers in Germany, and infected almost 2,400 TalkTalk routers in the UK.

Another example of a dedicated virus, collecting information on industrial systems on programmable PLCs, has ravaged especially in the automotive industry, Stuxnet is a malicious computer worm, first identified in 2010, was responsible for causing substantial damage to Iran's nuclear program. Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, and then seeking out Siemens Step7 software vulnerability.

The attack on PLCs with Step 7 installed has demonstrated the need to install antivirus programs not only on servers and workstations in companies' networks but equally on process equipments.

4. Research Methods

We analyze the evolution of cyber-attack phenomenon, in order to highlight the threats and risks associated, at the EU and worldwide level.

5. Discussions

The cyber threat is a continuous one, and this ransomware attack is just one of the manifestations that use vulnerability present in most versions of the Windows operating system. These attacks have become global attacks and affect any device connected to the Internet.

Computers in public institutions, hospitals and other social welfare organizations are not usually upgraded to the latest version of the operating system. If those terminals will not be updated, they will remain vulnerable to other cyber attacks.

This virus encrypts existing data on a computer in order to request the owner a ransom for an unlock key.

The attack began after Microsoft released an extremely rare security update for Windows XP and Windows Vista, warning of WannaCry-style attacks in the future using one of 16 different critical vulnerabilities. [8]

Microsoft announces in March 2017 the EternalBlue bug fix, and after a month the ransomware attack is triggered. If Windows Vista, 7, and 10 computers have Windows update automatically, the pach was installed on time and the stations were protected from attack, as well as the stations with the up-to-date antivirus program.

While Windows XP licenses, for which there is no longer any Microsoft update support, update is no longer active, they remain vulnerable.

There is discussion that Microsoft has deliberately left vulnerability, being used in anti-criminal activity by U.S. National Security Agency (NSA).

In the case of companies producing cars when it is found that a certain lot had technical problems, they recall the whole series of the batch in order to fix the problem, as it concerns the safety of the customer.

In the case of Operating System bugs, the patch can be automatically installed, only if the license agreement allow.

Authorities, banks and some companies that for various reasons use further Windows XP licenses have the option of an update and support agreement for a fee to protect their computer networks, ATMs or process computers.

Some security issues are related to the technologies used such as virtualization and service-oriented architectures and require vertical solutions from the service level to the physical level.

Cloud technology focuses on data security, both in terms of integrity and security, security management is difficult to control, given the number of requirements.

The Cloud model should have a structure to provide access to cloud data only after advancement through security levels.

Cloud technologies redefine concepts such as reducing costs, company flexibility and scalability, global secured access, transforming them into advantages that can't be neglected by any business.

As a member of the EU, Romania has enacted data protection legislation in order to align to the EU Data Protection Directive.

Romania is well positioned in the highly competitive global computer-security market. We can highlight the Internet Security Solution offered by the Romanian Company Bitdefender, one of the antivirus solution market leader's.

We summarize the risks that can be understood by both end-users and IT security specialists in order to prevent cybernetic attacks and reduce losses.

Table 1. Risks that may reduce cyber-terrorist attacks

Risks	Recommendations
The Operation System not up-dated	Up-date must be regularly installed
The System not secured with strong password	Passwords must be changed regularly
The System not protected	System must be protected with firewall and antivirus updated application
Unsolicited or suspicious e-mails	Should be avoided or opened with caution
The Mail Servers, File and Application Servers not secured	All the Servers must be protected with a strong Security Solution
Devices connected to Internet Network not secured	All devices connected to Internet must be secured to prevent unauthorized access

6. Conclusions

Starting from the recent attack that affected the electronic displays of rail traffic in Germany, we must be aware of the risk of logistics being infected at the level of railway stations, airports and last but not least On-board computers for cars.

If we imagine the new electronic devices connected to the IoT (Internet of Things), like Smart TV, refrigerators and air conditioners, alarm and surveillance systems, etc which can be infected and turned into a botnet, an army that can be used by cyber terrorists to control a massive DDOS attack.

It is clear that both hardware systems and operating systems, licensed or free ones must be developed and designed to prevent and stop cyber-terrorist attacks.

Mankind must understand the risks and damages of cyber attacks, make decisions and adapt legislation in order to avoid a cyberwar.

Security systems need to be continually improved, no matter how refined security is, with the advancing technology there will always be a breach that will be exploited.

The risk of cyber attacks has become significant and therefore customers lose confidence in online payment systems and virtual affairs.

References

[1]. Available from: http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/
[2]. Available from: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351
[3]. Available from: http://www.whatis.com.
[4]. Chen, Adela JW, Marie-Claude Boudreau, and Richard T. Watson. "Information systems and ecological sustainability." Journal of Systems and Information Technology 10.3 (2008): 186-201.
[5]. Petre R. Unitatea 1 a centralei de la Cernavodă s-a deconectat de la Sistemul Energetic Național. Journal Romania libera. 2017. Article available from: http://romanialibera.ro/actualitate/eveniment/unitatea-1-a-centralei-de-la-cernavoda-s-a-deconectat-de-la-sistemul-energetic-national-452281
[6]. Sistemul energetic. Available from http:www.sistemulenergetic.ro/statistics/show_graph/2017/5/6/0/0/2017/5/17/23/59
[7]. Kasperski Lab. Available from: http://www.Kasperski.com
[8]. The Guardian. Available from: https://www.theguardian.com/technology/2017/jun/15/university-college-london-hit-by-ransomware-attack-hospitals-email-phishing