DOI: 10.5748/16CONTECSI/SEC-6201

SECURITY ANALYSIS IN INFRASTRUCTURE ADMINISTRATION WITH QUEUE MANAGERS IN PAYMENT SYSTEMS IN THE FINANCIAL ENVIRONMENT

Alexandre Soares Sarto - Instituto de Pesquisas Tecnológicas de São Paulo-assarto@gmail.com
Anderson Aparecido Alves da Silva - Instituto de Pesquisas Tecnológicas de São Paulo - anderson@uol.com.br
Vagner Luiz Gava - Instituto de Pesquisas Tecnológicas de São Paulo - vlgava@ipt.br

The objective of this paper is to present an analysis of the importance of computational infrastructures used by IBM WebSphere MQ software for messaging exchange. The traffic of these messages represents a large volume of business with high financial values. The proper treatment of the computational infrastructure allows a higher protection level against malicious software, resulting in proper handling and management of the queue log manager. Since both the involvement of the information security management team and the application of recommendations from ABNT NBR ISO/IEC 27000 standards group make the queue managers infrastructure safer, the result of this work is the definition of the criteria used in the management of environments with IBM WebSphere MQ.

Keywords: vulnerability, infrastructure, malicious software, log files, ISO 27000.

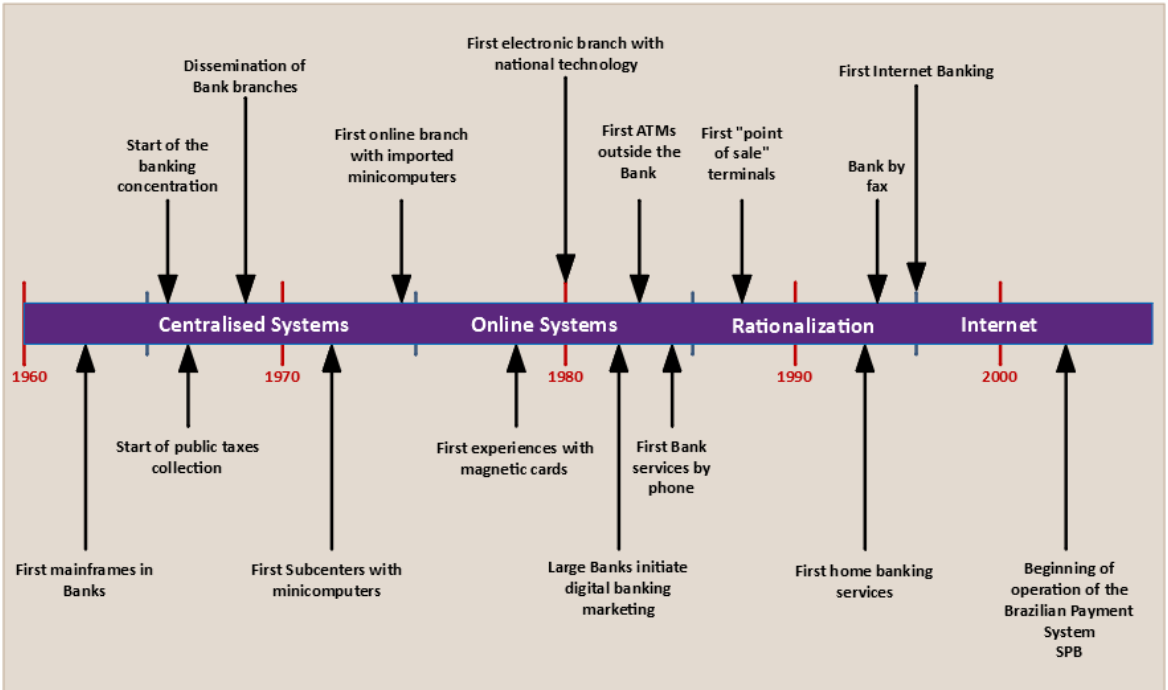
1. INTRODUCTION

Brazilian financial institutions have several technological security resources (*software* and *hardware*) that ensure protection to systems to be used both internally and externally by clients that access *Internet Banking solutions, Home Brokers* and credit card systems, to name a few.

DeFigueiredo (2002) says that since the restructuration of the financial operations made by the Brazilian Central Bank, the security controls over the whole infrastructure used for the traffic of these operations are basic demanded requirements.

Figure 1 shows a brief history of fifty years of banking automation in Brazil.

Figure 1 - Five decades of baking automation in Brazil.



Source: Diniz (2004) (author's redesign).

One of the main activities of the banking system is Brazil's Real-Time Gross Settlement System (STR) that executes the real-time gross settlement in order to make fund transfers in Brazil. This operation is performed by the Brazilian Central Bank (BCB), and the STR is the core of the Brazilian Payment System (SPB) (Brazilian Central Bank, 2012).

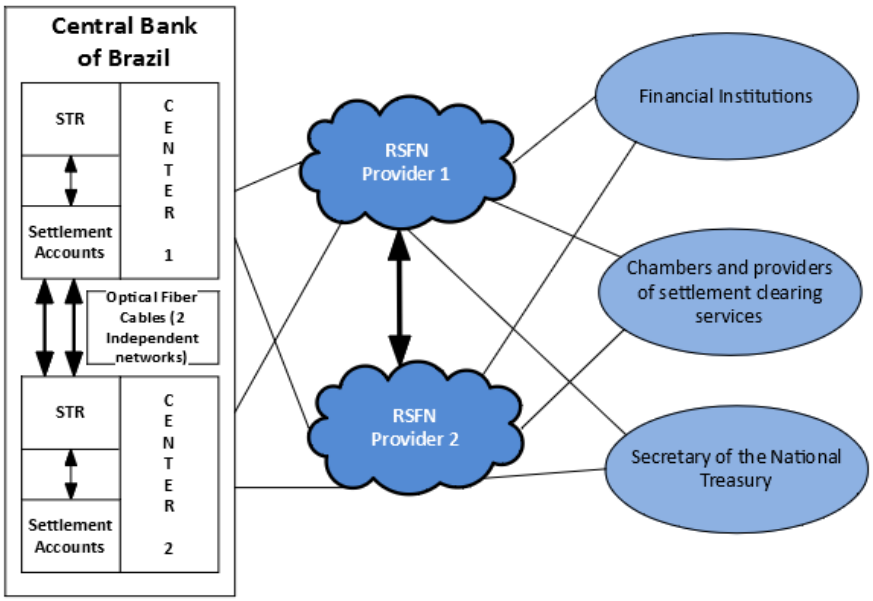
The National Financial System Network (RSFN) is a communication infrastructure that attends data traffic related to critical services, and it is configurated with two independent telecommunication networks which members are Brazil's Central Bank, Chambers, and National Treasure Secretary.

It is important to emphasize that even though it is used a dedicated network with two access providers, there is internal involvement in the Financial Institution (FI) of

employees who have access to this infrastructure and can perform incorrect procedures, compromising the service availability in the Financial Institution.

Figure 2 shows the structure of two communication providers to the National Financial System Network (RSFN) to the STR and from the STR to Financial Institutions, Chambers and National Treasure Secretary (STN).

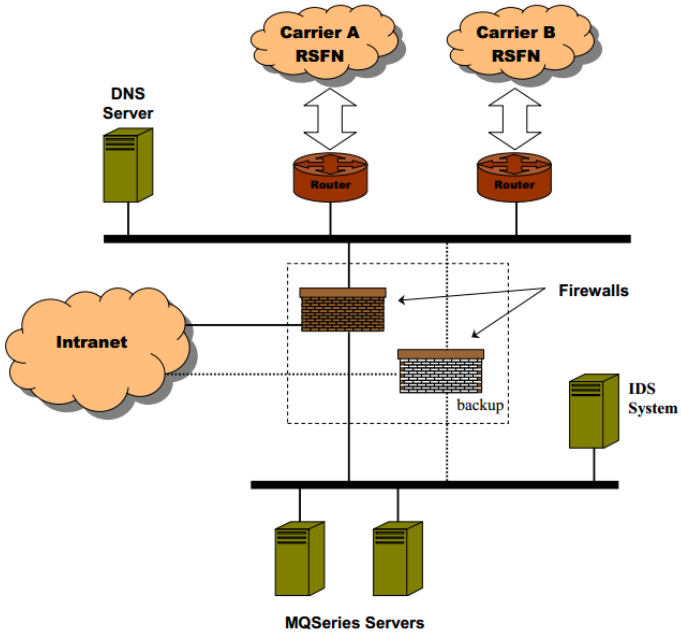
Figure 2 - National Financial System Network (RSFN) Distribution



Source: Queiroz (2008) (author's redesign).

Figure 3 shows the basic communication topology of a Financial Institution to the RSFN.

Figure 3 - Basic Communication Topology of between a Financial Institution and the RSFN.



Source: Defigueiredo (2002).

The software IBM WebSphere MQ creates a communication interface between internal legacy systems and external applications (PAPAZOGLOU et al., 2007). This software is represented by the servers called MQSeries in figure 3.

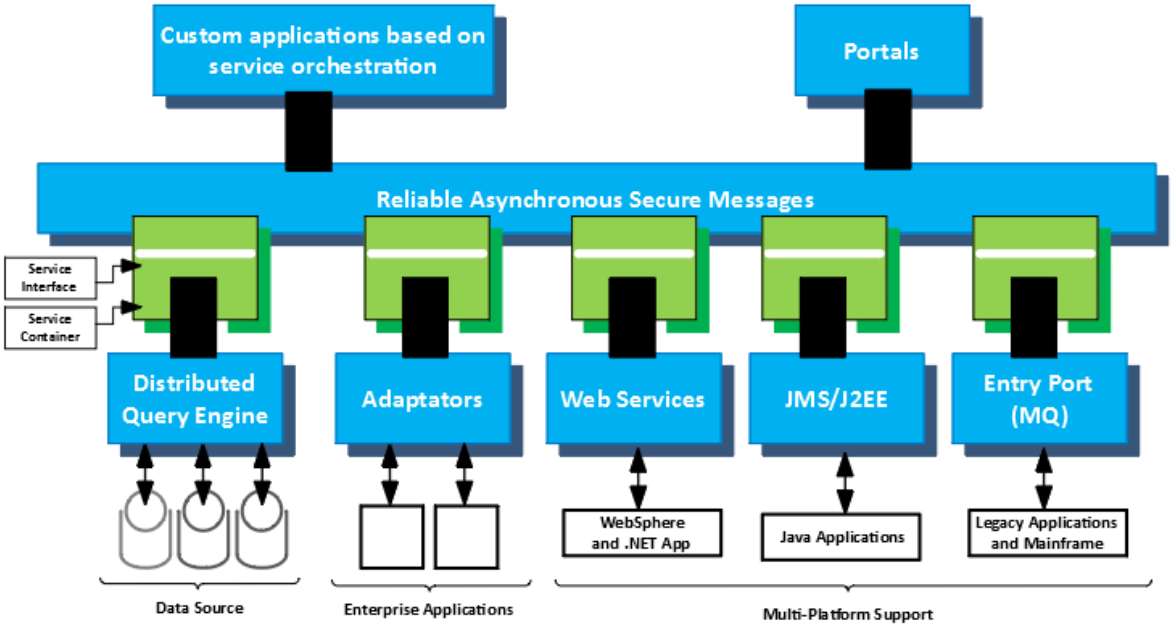
The BCB, the Financial Institutions and the Chambers members of RSFN have independent structures of queue managers configured in their computational infrastructure with IBM WebSphere MQ. Each of these participants has a unique identifier with the Central Bank for SPB. This identifier is used to configure the queue managers being the basis for configuration of remote and local queues, according to the standard established by the BCB (Brazilian Central Bank, 2019).

All the communication between the queue managers of members of SPB is made over the RSFN. Each queue manager is configured to work in a *Transmission Control Protocol/Internet Protocol* (TCP/IP) port.

When the queue manager is configured, the number of *log* files of the manager is defined. The number of *logs* is variable in each operational system: the minimum number in Windows is 2, and the maximum number is 254; in Linux and Unix operating systems the maximum is 510, and the minimum is 2 logs.

Figure 4 brings a simplified vision of an Enterprise Service Bus (ESB), that is the architecture that integrates internal and external applications.

Figure 4 - Simplified Vision of an Enterprise Service Bus (ESB).



Source: Papazoglou et al. (author's redesign) (2007).

All these computational evolutions bring and provide advantages to the application users and the Financial Institutions, but the security cannot be limited to external attacks (LEU et al., 2017).

Internal users need to be securely authenticated in the network, otherwise, they become a liability to security (LEU et al., 2017). Consequently, there is a permanent necessity of evolution in research about security mechanisms directed at controlling people (EVANS et al., 2016). Therefore, to contribute to the security enhancement of the Brazilian banking environment, this paper analyses operational errors caused by human interaction in *log* file administration for IBM WebSphere MQ *software* that is the BCB adopted standard to the Financial Institutions members of RSFN.

Says Zeng et al. (2016), the message registering in the log file is extremely important to the operation of several applications and there are many standards to perform this registering. Besides, Brazilian norm ABNT NBR ISO/IEC 27001 recommends that both the data registered and the system responsible for doing it have the appropriate security to prevent illegal access.

Based on this context, this paper intends to reduce message loss risks and the corruption of the server IBM WebSphere MQ. It is assumed that the specific administration of queue management servers and their log files is a vital part of the message loss risk reduction and corruption of these servers.

According to Accorsi (2009), it is necessary to exist a *log* storage phase so that, if an attacker violates one file, the person responsible for the infrastructure security would be able to identify the violation, these security definitions, however, are insufficient to protect the *logs*.

According to Ray et al. (2013), in the logs are written the events that occur in a computational infrastructure. These *logs* are important because they are the source of

information for problem analysis, the redefinition of parameters in applications and *software* for performance enhancement, identification of security violations in *software* and *hardware*.

2. OBJECTIVES

The objective of this article is to present an analysis of the aspects related to the security of the infrastructure of servers that use the software IBM WebSphere MQ queue manager, to protect these logs manager against human errors.

Based on the problem described in section 1, this article intends to address the following question: How to reduce the risk of losing messages or corrupting the IBM WebSphere MQ server?

The following sections describe concepts related to the research: IBM WebSphere MQ, ISO / IEC 27000, 27001, and 27002 Standards, *malware* and *ransomware*. Then, the problem is analyzed according to the current scientific literature, and a proposal for its resolution is presented.

3. CONCEPTS

In this item, are described the main aspects that influence the security of the IBM WebSphere MQ server.

3.1 IBM WebSphere MQ

According to Deogirikar and Vidhate (2018), IBM WebSphere MQ is a messaging software used by applications to send and receive messages through a network using queue managers. Until 2002, this software was called MQSeries, becoming later WebSphere MQ joining the WebSphere products family. It allows different applications to communicate with each other through message sending (IDATALABS, 2015a)

Table 1 shows that WebSphere MQ is the most used corporate integration application in a list of 46 products (from a total of 60,648 that where researched).

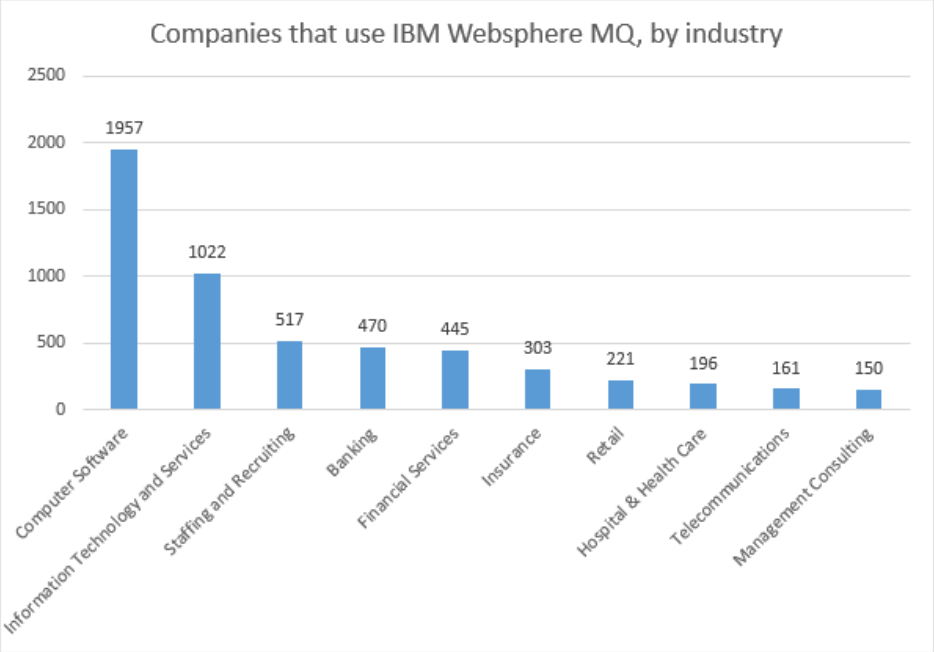
Table 1 - Companies that utilize Corporate Integration Applications.

Product	Number of companies using the applications	Percentage of Market	More information
IBM WebSphere MQ	**8,531**	**14%**	**https://idatalabs.com/tech/products/ibm-websphere-mq.**
BizTalk Server	8,251	13%	https://idatalabs.com/tech/products/biztalk-server.
Apache Kafka	7,298	12%	https://idatalabs.com/tech/products/apache-kafka.
Informatica PowerCenter	6,583	10%	https://idatalabs.com/tech/products/informatica-powercenter
Oracle Fusion Middleware	5,957	9%	https://idatalabs.com/tech/products/oracle-fusion-middleware
Mulesoft	4,227	6%	https://idatalabs.com/tech/products/mulesoft.
IBM WebSphere Message Broker	2,357	< 5%	https://idatalabs.com/tech/products/ibm-websphere-message-broker

Source: Idatalabs (2015b).

Figure 5 shows the sectors that utilize IBM WebSphere MQ, highlighting the banking sector in the fourth position.

Figure 5 - Sectors of Companies that utilize IBM WebSphere MQ



Source: Idatalabs (2015a) (author's redesign).

3.2 ABNT NBR ISO/IEC 27000, 27001 and 27002 standards

The standards series from family norms ABNT NBR ISO/IEC 27000 help the institutions to keep their information safe. The norm 27001 is recognized as the main security standard in companies (EVANS et al., 2016) and provides institutions with the requirements for an Information Security Management System (ISMS), that can be used in legal decisions as a safety assessment point of the company (DISTERER,

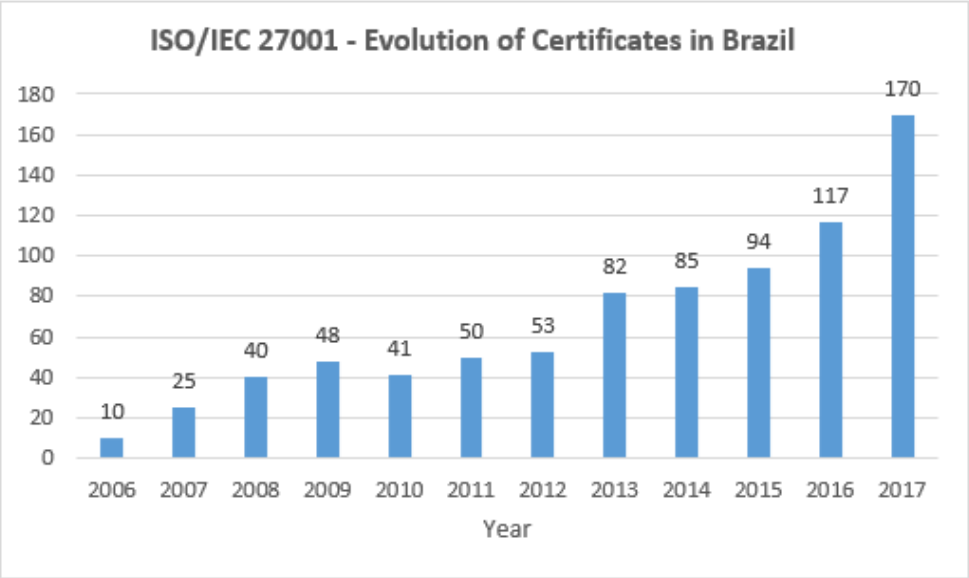
2013). The 27002 makes recommendations for information security management to initiate, implement or maintain ISMS (WATSON et al., 2017).

The ISO / IEC 27001 standard details the scheme for managing information security in a structured way and reducing exposure with the introduction of security controls. (GARY; PRANANTO, 2017).

The investment in the financial sector to modernize the computer systems with international standards is high allowing institutions to acquire certifications, showing that they are dealing with security issues besides implementing security within the computing infrastructures. According to Disterer (2013), there was an increase in the adoption of norms 27001 and 27002.

Figure 6 shows the continuous increase in the attainment of ISO 27001 certificate between 2006 and 2017 in Brazil.

Figure 6 - Adapted from the International Organization for Standardization (2018a)



Source: International Organization for Standardization (2018a).

Table 2 shows the amount of valid ISO standard certificates and the increase of certificates ABNT NBR ISO/IEC 27001 between 2016 and 2017.

Table 2 - World Certificate Amount per Standardization

Certificate	Number of Certificates 2016	Number of Certificates 2017	Alteration	Alteration %
ISO 9001	1,105,937	1,058,504	-47,433	-4
ISO 14001	346,147	362,610	16,463	5
ISO 50001	20,216	21,501	1,285	6
ISO 27001	33,290	39,501	6,211	19
ISO 22000	32,139	32,722	583	2
ISO 13485	29,585	31,520	1,935	7
ISO 22301	3,853	4,281	428	11
ISO 20000-1	4,537	5,005	468	10
ISO 28000	356	494	138	39
ISO 39001	478	620	142	30
TOTAL	1,576,538	1,446,758	-19,780	-1

Source: International Organization for Standardization (2018b). (Author's redesign).

The ISO organization annually collects the information of the certificates valid in the world. Table 2 shows a vision that includes the largest number of certificates for the existing standards and the differences of values in the years is due to the differences of participating certifying bodies and the number of certificates reported by them. There was a reduced number of these organs that did not participate with a low impact in the total because they provide a low volume of data. Table 2 shows only the valid certificates in the world (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018b).

3.3 *Malware* and *Ransomware*

According to Pearce (2018), *malware* is a *software* built to damage or unable a computational infrastructure, and it works as any program. *Malware* is the method used per a hacker to keep a treat alive inside a computational infrastructure and henceforth steal and damage data.

Ransomware is an extremely dangerous *malware* because it encrypts the files in the machines and demands a ransom from the users, mainly in virtual coins, to release passwords allowing access to the encrypted files. Risk of data loss is very high when administrator accounts are infected by *malwares*. Therefore, the recommendation is to

access these machines with accounts without administrator privileges (MORAN, 2015).

The Ransomware known as WannaCry caused meaningful impact all over the world in a short time on May 12th, 2017, infecting several computers running Microsoft Server operational system. According to Kuzuno, Inagaki, and Magata (2018), WannaCry is a malware that infects a computational infrastructure using a vulnerability in the implementation of the Server Message Block 1.0 (SMBv1) in servers using Microsoft operational system.

Figure 7 shows a screen of WannaCry version 2.0, informing the demand to pay a ransom to receive the code to decrypt the computer files. (KUZUNO; INAGAKI; MAGATA, 2018).

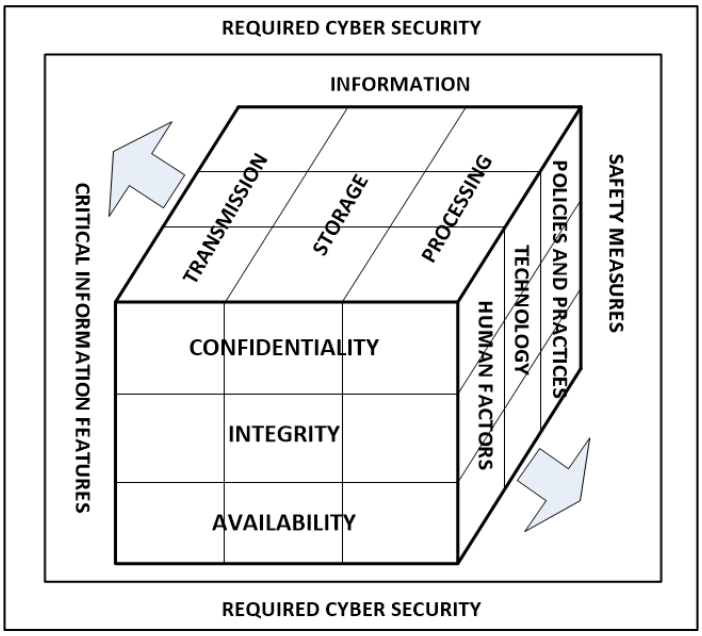
Figure 7 WannaCry ransomware Message.

Source: (TURAEV; ZAVARSKY; SWAR, 2018)

4. ANALYSIS

According to Cherdantseva et al. (2016) the McCumber cube, shown in figure 8, displays an approach to access and mitigate systems vulnerabilities.

Figure 8 - McCumber Cube



Source: Evans et al. (author's redesign) (2016).

According to Cilliers (2017), the McCumber cube was developed in 1991 and is credited as the first model that clarified accordingly the information assurance. This cube presupposes three dimensions to assure information that is:

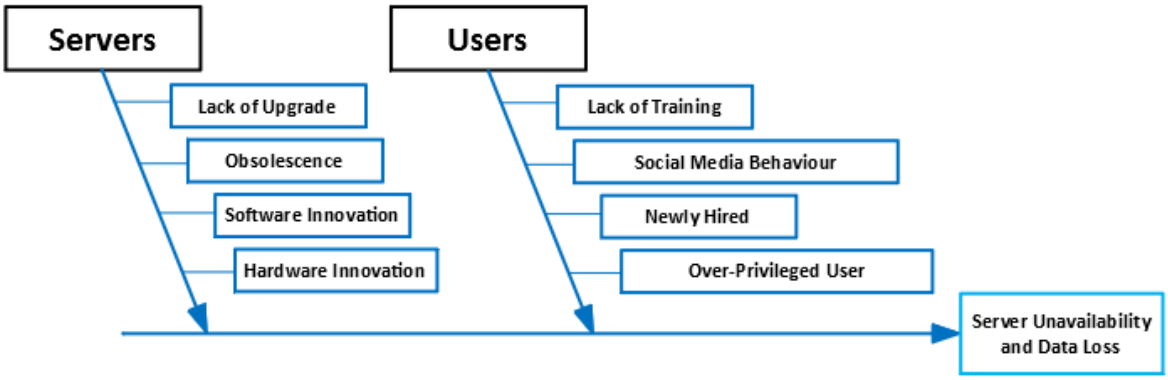
- Information state that corresponds to transmission, storage, and processing;
- Critical information characteristics that concern confidentiality, integrity, and availability;
- Security measures that cover politics and practices, technology, and human factors.

Frese (2015), comments that it is impossible to innovate without making mistakes, once updates change and put new variables into the environment, being software or hardware.

The big companies need to deal with a situation where an internal user becomes a liability to their computational security (Figure 9). As the majority of antivirus and anti-malware software works based on blacklists, the list needs to be kept updated to detect malware. (TURAEV; ZAVARSKY; SWAR, 2018).

Figure 9 shows an association of points related to servers and users and their effects over the computational environment, establishing cause-and-effect.

Figure 9 - Cause-and-effect over computational environment representation



Source: Author's Design.

Several tools can be used to control user activity at the institution's network.

The log files of the queue manager are a vital part of its functioning. To Zeng et al. (2016) the records in these files are extremely important to the operation of several applications, and there are many standards to write these records. Therefore, the ABNT NBR ISO/IEC 27001 international norm recommends that recorded data and the systems that make the writing have protection against damage and illegal access.

The administration of the log files of the queue manager where IBM WebSphere MQ is configured must be done in a way to determine the adequate amount of space to store these files. This volume must be calculated based on the volume of messages that will pass thru the queue manager, considering some unavailability that could occur in the application that reads them, because such problem generates message accumulation, reflecting in the occupied disc space defined by the queue manager.

Before any action in the server to be taken, like a reinitialization of the operational system, it is necessary to check if the queues are empty and in case such messages exist, it is recommended to export the messages to a file and import it after the operational system reinitialization. According to Bell (2002), it is essential to preserve reliable and critical evidence.

Even with high investment and use of advanced technological tools, it is necessary to train and to alert systems administrators and users about the importance in maintaining active the security levels as well as the maintenance of the awareness of security plans to maintain the applications' operability and availability.

According to Turaev, Zavarsky, and Swar (2018), it must not be granted administrator privileges to unqualified network users. To keep infrastructure free from malware, other levels of validation are mandatory, for instance, in the implementation or execution of new applications, it must be considered that only previously homologated applications should be admitted into these machines.

An efficient administration in the application of fixes or security patches can prevent contamination by malware and avoid that a queue manager is contaminated, keeping its data to be cryptographed. According to Furnell and Emm (2017), three measures can significantly reduce *ransomware* contamination risk. They are known as the protection ABC:

- ***A**nti-malware*;
- ***B**ack-up*;
- ***C**ritical patching*.

To deal with vulnerabilities in Microsoft Windows operational system, Microsoft company published a security bulletin called MS17-010 on March 14th, 2017 and among the most serious of them, there is one that allows an invader to execute code remotely (MICROSOFT, 2017).

WannaCry was dealt with by security patch MS17-010 that corrected SMBv1 vulnerability to the following Windows operational systems. (KUZUNO; INAGAKI; MAGATA, 2018):

- Windows Vista, 7, 8.1 e 10;
- Windows Server 2008/2008R2, 2012/2012R2 e 2016;
- Windows Server 2003;
- Windows XP/XP Embedded/8.

4. CONCLUSION

In order to answer the paper question "How to reduce the risk of losing messages or corrupting the IBM WebSphere MQ server?", were made researches in works related to the SMBv1 vulnerability, found in many versions of Windows operational system that were explored by a malware called *WannaCry* that caused loss around the world, inflicting damage in both personal and institutional equipment, with the potential of impacting directly the functioning of an IBM WebSphere MQ queue manager server, cryptographing their log files.

MQ creates their log files and has a standard established by the product and any change in these files, like compacting, excluding, and content alteration will impact the product operation as well as the queue manager, and in a case of contamination by malware that cryptograph these log files, the queue manager will not be able to perform properly.

Another contribution to answering the question of this paper corresponds to the operational errors in log file administration in queue managers, that can make applications unavailable in major financial institutions, generating huge loss as well as image damage to its clients besides penalties by regulatory institutions.

The infrastructure administrators where the queue managers are installed have broad privileges in their environments, and the use of not homologated tools or tools from unknown origins can damage the log files from the log managers or yet, incorrect actions like compacting files to liberate disk space could impact the operation of the queue manager and cause message loss.

Mainly in crises or in environments instabilities where the queue managers are configured with IBM WebSphere MQ middleware is recommended that before any procedure of stabilization, the messages that could still be in the queues and therefore not yet processed by the application server, should have a backup. According to Wang

(2007), the most important action to access a computational scenery in crisis is to preserve highly sensitive evidence that can be changed by a mouse click.

The users are a treat to the information security of the organization. The actions of the institutions before their users must be permanent. Any suspected invasion identified by users should immediately trigger the channels defined by the organization. Training and awareness of all users of the computational infrastructure in the use and application of security policies are vital to ensure stability and protection of information.

ACKNOWLEDGMENTS

This research was translated into the English language by Luci Meire de Lima.

REFERENCES

ACCORSI, Rafael. Log data as digital evidence: what secure logging protocols have to offer?. In: ANNUAL IEEE INTERNATIONAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 33., 2009, Seattle, Washington. Proceedings… Piscataway: IEEE, 2009. p. 398-403, 2009. Available at: https://ieeexplore.ieee.org/abstract/document/5254059. Accessed: 19 mar. 2019.

BANCO CENTRAL DO BRASIL (Brasília). RSFN Rede do Sistema Financeiro Nacional: Manual de Redes do SFN. 2018. Versão 8.2.1. Available at: https://www.bcb.gov.br/sfn/ced/RSFN_Manual_de_Redes_do_SFN_Ver_8.2.1.pdf. Accessed: 25 fev. 2019.

BANCO CENTRAL DO BRASIL. STR (Sistema de Transferência de Reservas) Brazil's Real Time Gross Settlement System: Users Terms and Conditions. Deban - Department Of Banking Operations And Payments System, Brasília: BCB, 2012. 17 p. Available at: https://www.bcb.gov.br/Pom/Spb/Ing/STR-Users_Terms_and_Conditions.pdf. Accessed: 22 fev. 2019.

BANCO CENTRAL DO BRASIL. Departamento de Operações Bancárias e de Sistema de Pagamentos - Deban. Relação de participantes do STR - Ambiente de Produção. 2019. Available at: https://www.bcb.gov.br/pom/spb/estatistica/port/ASTR003.pdf. Accessed: 07 mar. 2019.

BELL, R. E. The Prosecution of Computer Crime. Journal Of Financial Crime, v. 9, n. 4, p. 308-325, Apr. 2002. Emerald. http://dx.doi.org/10.1108/eb026030. Available at: https://www-emeraldinsight-com.ez1.periodicos.capes.gov.br/doi/pdfplus/10.1108/eb026030. Accessed: 10 mar. 2019.

CHERDANTSEVA, Yulia et al. A multifaceted evaluation of the reference model of information assurance & security. Computers & Security, v. 63, p. 45-66, Nov. 2016. Elsevier BV. http://dx.doi.org/10.1016/j.cose.2016.09.007. Available at: https://www.sciencedirect.com/science/article/pii/S0167404816301146. Accessed: 25 fev. 2019.

CILLIERS, Liezel. Exploring information assurance to support electronic health record systems. In: IST-AFRICA WEEK CONFERENCE (IST-AFRICA), 2017,

Windhoek, Namibia. Proceedings… Piscataway: IEEE, 2017. 8 p. http://dx.doi.org/10.23919/istafrica.2017.8102363. Available at: https://ieeexplore.ieee.org/abstract/document/8102363/. Accessed: 19 mar. 2019.

DEFIGUEIREDO, Dimitri do B. Vulnerability Analysis of the Brazilian Payment System. Los Angeles: Department Of Computer Science University of California, 2002. p. 1-7. Available at: http://web.cs.ucdavis.edu/~defigued/index_files/SPBanalysis.pdf. Accessed: 19 fev. 2019.

DEOGIRIKAR, Jyoti; VIDHATE, Amarsinh. A comprehensive development and testing of improved publish-subscribe method for IoT. In: INTERNATIONAL CONFERENCE ON INVENTIVE COMMUNICATION AND COMPUTATIONAL TECHNOLOGIES, 2., 2018, Coimbatore, India. Proceedings… Piscataway: IEEE, 2018. p. 1796-1801. IEEE. http://dx.doi.org/10.1109/icicct.2018.8473351. Available at: https://ieeexplore.ieee.org/document/8473351. Accessed: 05 mar. 2019.

DINIZ, Eduardo H. Cinco décadas de automação. Era Digital, São Paulo, v. 3, n. 3, p. 55-60, out. 2004. Available at: http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/34691. Accessed: 23 fev. 2019.

DISTERER, Georg. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, v. 04, n. 2, p. 92-100, 2013. Scientific Research Publishing, Inc,. http://dx.doi.org/10.4236/jis.2013.42011. Available at: https://file.scirp.org/pdf/JIS_2013042311130103.pdf. Accessed: 23 fev. 2019.

EVANS, Mark et al. Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, v. 9, n. 17, p. 4667-4679, 20 Oct. 2016. Wiley. http://dx.doi.org/10.1002/sec.1657. Available at: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1657. Accessed: 24 fev. 2019.

FRESE, Michael; KEITH, Nina. Action Errors, Error Management, and Learning in Organizations. Annual Review of Psychology, v. 66, n. 1, p. 661-687, 3 Jan. 2015. Annual Reviews. http://dx.doi.org/10.1146/annurev-psych-010814-015205. Available at: https://www.annualreviews.org/doi/abs/10.1146/annurev-psych-010814-015205. Accessed: 23 fev. 2019.

FURNELL, Steven; EMM, David. The ABC of ransomware protection. Computer Fraud & Security, v. 2017, n. 10, p. 5-11, Oct. 2017. Elsevier BV. http://dx.doi.org/10.1016/s1361-3723(17)30089-1. Available at: https://www.sciencedirect.com/science/article/pii/S1361372317300891. Accessed: 05 mar. 2019.

GARY, Ang Chee Kiong; PRANANTO, Utomo Nugroho. Cyber Security in the Energy World. In: ASIAN CONFERENCE ON ENERGY, POWER AND TRANSPORTATION ELECTRIFICATION (ACEPT), 2027, Singapore. Proceedings… Piscataway, IEEE, 2017. p. 1-5. Available at: https://ieeexplore.ieee.org/document/8168583. Accessed: 07 mar. 2019.

IDATALABS. Companies using IBM Websphere MQ. 2015a. Available at: <https://idatalabs.com/tech/products/ibm-websphere-mq>. Accessed: 23 fev. 2019.

IDATALABS. Enterprise Application Integration products. 2015b. Available at: https://idatalabs.com/tech/enterprise-application-integration. Accessed: 23 fev. 2019.

INTERNATIONAL BUSINESS MACHINES. Queue manager logs. 2019. Last updated: Thursday, 28 Feb. 2019. Available at:

https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.5.0/com.ibm.mq.con.doc/q018950_.htm. Accessed: 19 mar. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. The ISO survey of management system standard certifications: ISO/IEC 27001 - Certificates Worldwide. Geneve: ISO, 2018a. Available at: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1. Accessed: 24 fev. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. The ISO survey of management system standard certifications – 2017 – explanatory note. Geneve: ISO, 2018b. Available at: https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Overall_results_and_explanatory_note_on_2017_Survey_results.pdf?nodeid=19208898&vernum=-2. Accessed: 24 fev. 2019.

KUZUNO, Hiroki; INAGAKI, Shun; MAGATA, Kenichi. Constructing a Complete Timeline of a Security Incident by Aggregating Reports. In: ASIA JOINT CONFERENCE ON INFORMATION SECURITY, 13., 2018, Guilin, China, Proceedings… Guilin : Guilin University of Electronic Technology, 2018. p. 109-115, http://dx.doi.org/10.1109/asiajcis.2018.00026. Available at: https://ieeexplore.ieee.org/abstract/document/8453770. Accessed: 05 mar. 2019.

LEU, Fang-yie et al. An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques. IEEE Systems Journal, v. 11, n. 2, p. 427-438, June 2017. Institute of Electrical and Electronics Engineers http://dx.doi.org/10.1109/jsyst.2015.2418434. Available at: https://ieeexplore.ieee.org/abstract/document/7090949. Accessed: 23 fev. 2019.

MICROSOFT. Boletim de Segurança da Microsoft MS17-010 – Crítico. 2017. Atualização de segurança para o Microsoft Windows SMB Server (4013389). Available at: https://docs.microsoft.com/pt-br/security-updates/SecurityBulletins/2017/ms17-010. Accessed: 19 mar. 2019.

MORAN, Joseph. Managing and Protecting Files with User Accounts. In: MORAN, Joseph.(Ed.). File Management Made Simple, Windows Edition. Berkely: Apress, 2015. p. 41-52. http://dx.doi.org/10.1007/978-1-4842-1082-6_4. Available at: https://link.springer.com/chapter/10.1007/978-1-4842-1082-6_4. Accessed: 24 fev. 2019.

PAPAZOGLOU, Michael P. et al. Service-Oriented Computing: State of the Art and Research Challenges. Computer, v. 40, n. 11, p. 38-45, Nov. 2007. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mc.2007.400. Available at: https://ieeexplore-ieee-org.ez1.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=4385255. Accessed: 23 fev. 2019.

PEARCE, Lauren. Incident Response and Malware Analysis. Los Alamos, New Mexico: Los Alamos National Laboratory, 2018. 30 slides, color. LA-UR-18-30641. Available at: https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-18-30641. Accessed: 05 mar. 2019.

QUEIROZ, Mardilson Fernandes. O Sistema de Pagamentos Brasileiro. Brasília: BCB, 2008. 57 slides, color. Available at: https://www.bcb.gov.br/Pre/bcUniversidade/Palestras/BC%20e%20a%20Universidade-sistemadepagamentos-agosto2008.pdf. Accessed: 22 fev. 2019.

RAY, Indrajit et al. Secure Logging as a Service—Delegating Log Management to the Cloud. IEEE Systems Journal, v. 7, n. 2, p.323-334, June 2013. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/jsyst.2012.2221958. Available at: https://ieeexplore.ieee.org/abstract/document/6407695/. Accessed: 19 mar. 2019.

TURAEV, Hasan; ZAVARSKY, Pavol; SWAR, Bobby. Prevention of Ransomware Execution in Enterprise Environment on Windows OS: Assessment of Application Whitelisting Solutions. In: INTERNATIONAL CONFERENCE ON DATA INTELLIGENCE AND SECURITY, 1., 2018, South Padre Island, TX. Proceedings… Piscataway: IEEE, 2018. p. 110-118. http://dx.doi.org/10.1109/icdis.2018.00024. Available at: https://ieeexplore.ieee.org/abstract/document/8367748. Accessed: 23 fev. 2019.

WANG, Shiuh-jeng. Measures of retaining digital evidence to prosecute computer-based cyber-crimes. Computer Standards & Interfaces, v. 29, n. 2, p. 216-223, Feb. 2007. Elsevier BV. http://dx.doi.org/10.1016/j.csi.2006.03.008. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0920548906000456. Accessed: 07 mar. 2019.

WATSON, Venesa et al. Interoperability and Security Challenges of Industrie 4.0. Maximilian Eibl, Martin Gaedke (hrsg.): Informatik, p. 973-985, 2017. Available at: https://dl.gi.de/handle/20.500.12116/3860. Accessed: 07 mar. 2019.

ZENG, Lei et al. Computer operating system logging and security issues: a survey. Security And Communication Networks, v. 9, n. 17, p. 4804-4821, 20 Oct. 2016. Wiley. http://dx.doi.org/10.1002/sec.1677. Available at: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1677. Accessed: 23 fev. 2019.