SEVEN publicações acadêmicas
EM PARCERIA COM: IEMS UNIASSELVI

A conceptual analysis of the risks and challenges of information security in cloud computing

David Kadab Chaves[1], Gláucya Daú[2], Annibal Scavardayy[3].

ABSTRACT

This article will clarify relevant topics related to technological evolution and how to achieve excellence in cloud computing security. The objective is to demonstrate the real importance of Computer Security in companies that use this resource and that requires every day that data is not only stored, but also preserved. The methodology used in this study was based on an exploratory case study, of a qualitative nature, integrating the literature review. Are we always protected? How do I avoid vulnerabilities? How to mitigate the risks? How do you know how to identify a threat? Questions that are more complex to answer than they appear. It was concluded that companies do not know how to classify information, nor distinguish which are the true assets that should be safeguarded, and the security issue is often ignored.

Keywords: Threats, Cloud Computing, Malware, Information security, Vulnerability.

INTRODUCTION

The current scenario shows a moment in which technological development evolves alarmingly and that it is often not a simple task to reconcile information security with all this technological advancement, but it is extremely important to reflect on how to preserve the three main pillars of information security, they are: confidentiality – ensures that information is accessible only by authorized people; availability – ensures that information is accessible at all times and integrity – ensures that information is complete from its source to its destination. Technological evolution had as a historical milestone, the moment when man was able to store data to use it later. It is observed how computers are already solidified in the form of mobile devices, used even as a support for work; More powerful servers are emerging every day and Cloud Computing has also been gaining ground in society.

When it comes to information security, we can relate cost and benefit. The cost is not always as affordable as desired, but it will prevent future problems that can cause significantly greater impacts than the cost of implementing an effective security policy. Are managers aware of this scenario? Would they be willing to invest in security?

[1] Celso Suckow da Fonseca Federal Center for Technological Education - CEFET/RJ – Rio de Janeiro-RJ
[2] State University of Rio de Janeiro - UERJ – Rio de Janeiro-RJ
Universidade Federal Fluminense - UFF – Niterói-RJ
[3] Federal University of the State of Rio de Janeiro - Unirio - Rio de Janeiro-RJ
Celso Suckow da Fonseca Federal Center for Technological Education - CEFET/RJ – Rio de Janeiro-RJ
Universidade Federal Fluminense - UFF – Niterói-RJ

OBJECTIVE

The objective of this scientific article is to demonstrate the importance of Computer Security in companies that use cloud computing technology, where technological evolution requires that every day data is not only stored, but also preserved. To this end, this work will make a brief introduction to the types of virtual infractions and the people who practice them, so that the understanding is complete. And finally, it will address the main technological trends.

METHODOLOGY

The methodological proposal was based on an exploratory case study, of a qualitative nature, integrating the literature review. The following guiding questions will apply: Are we always protected? How do I avoid vulnerabilities? How to mitigate the risks? How do you know how to identify a threat?

For the literature review, search equations were constructed based on keywords and connected to the theme. The Portal of Journals of the Coordination for the Improvement of Higher Education Personnel (CAPES) was the database for the search for articles. This research methodology was chosen with the intention of facilitating the identification of the technologies used and what can be improved, generating information that can guide the implementation of new technological resources.

DEVELOPMENT

Information is a company's main asset, so it needs to be well protected. This work contains research and studies carried out addressing the cost and benefit subject of investing in security, so that the company can keep up with technological evolution without major losses.

This article was based on several researches that involve the importance of asset security in the business environment. More than 70% of Brazilian companies still do not have an adapted security system. A brief study on cyber infractions and the types of offenders to level the understanding and studies related to a technology that is on the rise, Cloud Computing, will be presented.

CLOUD COMPUTING

Undoubtedly, cloud computing is here to stay, this growing and exponential evolution (MATHER, 2009), which is already ceasing to be a trend and is becoming a reality. Its appeals (ease of accessing data services and applications from any device and from anywhere; and without the need to have a hard drive to perform the storage) are attractive. However, it brings us new challenges in terms of security, privacy, and resilience. A public cloud provider, for strategic reasons, does not open up its technology, organization, and processes.

The issue of safety is of fundamental importance. The acceleration of cloud computing is directly related to the degree of confidence in the model and the technologies involved. Without feeling comfortable with the level of security obtained, company managers will not make favorable decisions. Thus, knowing the multiple aspects that involve security in *Cloud Computing* is an obligation for every manager or technology professional. The report begins with a leveling of the conceptual aspects of cloud computing, its service (Infrastructure as a Service, Platform as a Service, and Software as a Service) and delivery (Public and Private Clouds) models. From there, it describes the critical aspects related to security, basically divided into two domains: the governance domain (including factors such as risks, auditing, evaluation, and reporting); and operational, which includes variables such as cloud data center operation, business continuity, access identity management, virtualization, etc.

Security is indisputably what leads us to reflect on whether we should really invest in *Cloud Computing*. There are several issues that generate distrust, it is not known where the cloud server is located, it is not clear what the providers of this service do to provide excellence in security, it is not known about the physical security of this place and also about the security related to reliability, but there is a slice of security that offers great comfort for those who hire *Cloud Computing* services, because the company that provides this type of service guarantees in a contract that it is responsible for all hosted data, and may even include fines for non-compliance.

Currently, in addition to *Cloud Computing*, the issue of virtualization is also on the rise. Physical servers are becoming obsolete, due to a high demand for virtual servers (TULLOCH, 2014).

As more hands-on experiences are gained with cloud computing, the report will be expanded and added to more detail. According to several surveys conducted, it is still common to see many people thinking that this technology will take time to disseminate, mainly because many industry analysts make conservative estimates of its adoption by the market. It's true that industry analyst reports with estimates regarding *cloud computing* trends and prospects tend to be quite conservative.

Research on this subject, carried out with experts, shows that the results are unanimous, where they explore factors that show that cloud computing is growing more and more exponentially and is a reality that is being incorporated into institutions in a way that provides significant results.

When it is said that it grows exponentially, one must remember the legendary "creator of computing", Von Neumann. He made two important observations: one that human progress is exponential and non-linear. The other is that this exponential growth starts slowly and often goes unnoticed, until it reaches a tipping point, when it turns into something explosive and profoundly transformative.

Generally, forecasts are based on the prospect of linear rather than exponential growth. But the pace of change is accelerating. For example, the last 20 years of progress of the 20th century would be

achieved today in 14 years. Soon in just 7 years and so on. In practical terms, the 21st century will have a pace of technological progress at least 1000 times greater than what we saw in the century that just ended.

New technologies bring many benefits, but it is not advisable to neglect security issues. Cloud computing is a change in the computing model, but the use of public clouds should be looked at carefully. Not that they're inherently unsafe, they're usually not, but our habits often make it easy for them to be hacked. An alternative is to use private clouds (computational clouds internal to the "firewall", when it is easier to have access to the control of security standards and procedures) or even use hybrid clouds, where it is formed by private clouds for critical applications and data, but also using some services provided by external clouds, consisting of certain types of services.

MAIN TYPES OF *MALWARE*

When a device is connected to a network, it automatically ceases to be 100% secure. There are several types of malware that can cause significant impacts for the corporate environment, as well as for personal use. Below are the main types of malware today (ULBRICH, 2004).

Virus: A virus is a malicious computer program that spreads by infecting, i.e., inserting copies of itself and becoming part of other programs and files on a computer. The virus depends on the execution of the host files so that it can become active and continue the infection process.

Worm: *A* worm is a program capable of propagating itself automatically through networks, sending copies of itself from computer to computer. Unlike a virus, the *worm* does not embed copies of itself in other programs or files and does not need to be explicitly run to propagate. Its propagation occurs through the exploitation of existing vulnerabilities or flaws in the configuration of software installed on computers.

Trojan: Trojan is a program that impersonates a "gift" (e.g., virtual cards, photo album, screensaver, games) that in addition to performing functions for which it was apparently designed, also performs other functions that are normally malicious and without the user's knowledge. The *Trojan* is usually responsible for opening ports, thus leaving loopholes for other attacks coming from other types of *malware.*

Keylogger: Keylogger is a program capable of capturing and storing the keystrokes typed by the user on a computer's keyboard. Usually, the activation of the *keylogger* is conditional on a previous action by the user, such as, for example, after accessing an e-commerce or *Internet Banking* site, to capture bank passwords or credit card numbers.

Screenlogger: Screenlogger is the advanced form of *keylogger*, where it is able to store the position of the cursor and the screen presented on the monitor, at the times when the mouse is clicked, or store the region that surrounds the position where the mouse is clicked.

Spyware: Spyware is the word used to refer to a large category of software that has the purpose of monitoring a system's activities and sending the collected information to third parties. They can be used legitimately, but they are often used in a disingenuous, unauthorized, and malicious way; its main tool is a fake URL.

Backdoor: Backdoor is a program that allows an attacker to return to a compromised computer. Usually, this program is placed in such a way that it is not noticed.

Exploits: Exploits are malicious programs designed to exploit an existing vulnerability in computer software.

Sniffers: Sniffers are used to capture and store data traveling on a computer network. It can be used by an attacker to capture sensitive information (such as user passwords) in cases where insecure connections are being used, i.e., without encryption. It leaves the computer's network card in promiscuous mode, that is, the network card starts to process all packets that travel through the connected network and not just packets that were from specific destinations.

DoS (Denial of Service) Attack: DoS attacks, also known as "Denial of Service Attacks", consist of attempts to make computers - *Web* servers, for example - have difficulty or even be prevented from performing their tasks. To do this, instead of "invading" the computer or even infecting it with malware, the attacker makes the machine receive so many requests that it reaches the point of not being able to interpret all of them. In other words, the computer becomes so overloaded that it denies service, leaving all access unavailable. Depending on the service affected, there can be a huge loss for the victim, impacting several pillars of the institution, especially financially.

When the DoS attack originates from several machines, we say that it is a DDoS (*Distributed Denial of Service*) attack, with this, the attack can become much more comprehensive, harmful and with the potential to cause serious damage.

MAIN TYPES OF CYBER OFFENDERS

There is a conception that the virtual offender is called "Hacker", but it is a term given erroneously, the right one for what the individual tried to say, must be "Cracker" (ULBRICH, 2004). Listed below are the main types of cyberbreakers and their nomenclatures, which classify and define them, as well as hackers, crackers, script kiddies, lammers, carders, cyberpunks and newbies, among others (CARMONA, 2002). A hacker is an individual who dedicates himself, with unusual intensity, to knowing and modifying the innermost aspects of computer devices, programs, and networks. Thanks to this knowledge, a *hacker* is often able to obtain extraordinary solutions and effects, which go beyond the limits of the "normal" functioning of systems as envisioned by their creators; including, for example, bypassing the barriers that are supposed to prevent control of certain systems and access to certain data.

Many share information and collaborate on common projects, including conferences, activism, and the creation of free software, constituting a hacker community with specific culture, ideology, and motivations. Others work for companies or government agencies, or are self-employed. *Hackers* were responsible for many important innovations in computing, including the C programming language and the Unix operating system (Kernighan and Ritchie), the emacs text editor (Stallman), the GNU/Linux system (Stallman and Torvalds), and the Google indexer (Page and Brin). *Hackers* have also revealed many weaknesses in encryption and security systems, such as, for example, digital voting machines (Gonggrijp, Haldeman), identity card with chip, blocking of mobile phones, etc.

Hackers: Usually considered as a "*Hacker*", a person or a group that attacks to cause damage or offense to any company, government agency or even a personal computer. Although the way of operating is similar, the goals of these computer geniuses are different, each with their own idealizations. For this reason, they are divided into categories, the main ones being:

- **White Hat Hackers** – These are considered to be the *good hackers*. They are security specialists, acting to expose and resolve possible loopholes and flaws in the systems of the companies that hire them;
- **Black Hat Hackers** – These are the malicious ones, who invade networks and computers, create viruses and *malware* always with illicit intentions, such as stealing bank passwords, confidential data and others;
- **Hacktivists** – They act for ideological reasons. They are mainly responsible for crashes on the websites of governments, agencies, and multinational companies. Their primary method of intrusion is through DDoS attacks.

Crackers: Cracker is a term used to designate the individual who practices the breaking (or cracking) of a security system, illegally or unethically. This term was coined in 1985 by hackers in defense against journalistic use of the term hacker. The use of this term reflects their strong revolt against the theft and vandalism practiced by cracking, as there was some confusion among some people, who referred to people who acted in bad faith, as hackers, and the correct one should be cracker.

Like hackers, crackers also have great knowledge in the field of technology. Crackers with a lot of knowledge will hardly be found, as they can eliminate all their traces, thus becoming "invisible".

The act of breaking the security of a system often requires brilliance to accomplish and the ability to exploit the known vulnerabilities of the target system with creativity. However, some, "erroneously" defined as crackers, use known solutions to recurring problems in vulnerable systems, thus copying or exploiting flaws discovered by others without any effort.

Script Kiddies: Subcategory of crackers. They don't have a clear target, they try to invade everything they come in front of and use tools found on the Internet. They have a digital knowledge well above ordinary users, but they don't even know the basics of programming languages, they just take ready-made programs and use them to infect certain computers.

Lammers: They hardly learn how to use any program, they don't know and they can't learn how things work. Those who come to the chats announcing "I'm going to invade you, I'm the best", but give up, because they can't perform any harmful action, not even the basics of the basics, that is, they are those who only threaten and feel frustrated because they don't understand the subject.

Carders: It's the credit card fraud expert. They know how to get lists of valid cards on sites that use them (shopping sites, paid chat, any site that has features that are paid for in some way, etc.), generate fake numbers that pass verification and even steal and clone real cards. When a card is cloned, the card user does not lose money, however, until he discovers and takes the necessary actions, several purchases would have already been made, always leaving someone with the loss.

Cyberpunks: These are techno-anarchists who fight to maintain privacy in cyberspace through the spread of mass encryption programs. They try to protect ordinary citizens against government and business attempts to scrutinize their lives from the clues left when using any electronic system.

The PGP (Pretty Good Privacy) program created by P. Zimmermann is one of the main tools used by cyberpunks.

Newbies: Newbie is the newbie on the net. He gets into places he shouldn't, asks questions he shouldn't. At this level are the first users who use programs developed by experts, without much knowledge about any hacker ethics, but with basic knowledge about what it is to be one, and just for fun and/or an attempt at social recognition. It is the second step taken to move into the hacker area.

FINAL THOUGHTS

In general, many companies do not know how to classify information, nor distinguish which are the true assets that should be safeguarded. Many organizations, to this day, invest a lot in machines, hardware equipment, which is important, but often the focal point is ignored, which is the logical part of the entire system, especially in terms of security.

This article showed evidence of the main types of malicious *software* (*Malware*), detailing their characteristics and highlighting the importance of prevention.

We also classify the main types of virtual offenders, because there are still many people who do not know how to define them, or define them generalizing as *hackers*, as said, this nomenclature has been used incorrectly in most cases.

This article addressed the technology that is in evidence in the technological market, a trend that is a reality and is present in almost all sectors of many companies. However, the computational security factor is paramount for Cloud Computing to continue growing.

REFERENCES

Ulbrich, H. C. (2004). Universidade H4CK3R. São Paulo: Universo dos Livros.

Carmona, T. (2002). Universo H4CK3R. São Paulo: Digerati Books.

Sosinsky, B. (2011). Cloud Computing Bible (1st ed.). Wiley.

Hugos, M., & Hulitzky, D. (2010). Business in the Cloud (1st ed.). Wiley.

Rhodes-Ousley, M. (2013). Information Security the Complete Reference (2nd ed.). McGraw-Hill.

Bosworth, S., & Kabay, M. E. (Eds.). (2014). Computer Security Handbook (6th ed.). Wiley.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Computing and Privacy (1st ed.). O'Reilly Media.

Tulloch, M., & MSFT. (2014). Network Virtualization and Cloud Computing (1st ed.). Microsoft Press.

Daú, G. L., Scavarda, A., Scavarda, L. F., & Portugal, V. J. T. (2019). The Healthcare Sustainable Supply Chain 4.0: The Circular Economy Transition Conceptual Framework with the Corporate Social Responsibility Mirror. Resources, Conservation & Recycling, 141, 418-430. https://doi.org/10.1016/j.resconrec.2018.10.027

Magrani, E. (2018). A Internet das Coisas (1st ed.). Rio de Janeiro: Editora FGV.

Marquesone, R. (2016). Big Data: Técnicas e tecnologias para extração de valor dos dados (1st ed.). São Paulo: Editora Casa do Código.

Mataric, M. J. (2014). Introdução à Robótica (1st ed.). São Paulo: Editora Blucher.

Netto, A. V., Berton, L., & Takahata, A. K. (2022). Ciência de dados e a inteligência artificial na área da saúde (1st ed.). São Paulo: Editora dos Editores.

Netto, A. V., & Novoa, C. (2019). Fundamentos em gestão e informática em saúde (1st ed.). São Paulo: UNIFESP.

Scavarda, A., Daú, G. L., Scavarda, L. F., & Korzenowski, A. L. (2019a). A proposed healthcare supply chain management framework in the emerging economies with the sustainable lenses: The theory, the practice, and the policy. Resources, Conservation & Recycling, 141, 418-430. https://doi.org/10.1016/j.resconrec.2018.10.027

Scavarda, A., Daú, G. L., Scavarda, L. F., & Caiado, R. G. G. (2019b). An Analysis of Corporate Social Responsibility and Industry 4.0 with Focus on the Youth Generation: A Sustainable Human Resource Management Framework. Retrieved from https://www.mdpi.com/2071-1050/11/18/5130

Schwab, K. (2018). A Quarta Revolução Industrial (1st ed.). São Paulo: Edipro.

Souza, T. A. (2015). Lean Healthcare: Aplicação dos Conceitos de Gestão de Operações em Centros Cirúrgicos. Retrieved from http://www.repositorio.jesuita.org.br/handle/UNISINOS/5157

Stender, G. H. C. (2016). Lean Healthcare: Modelo de Implantação da Ferramenta Kanban a um Almoxarifado de um Hospital Federal no Rio de Janeiro. Retrieved from http://pppro.cefet-rj.br/T/376_Gustavo Henrique Cordeiro Stender.pdf

Vilela Junior, G. de B., & Passos, R. P. (2021). Inteligência Artificial nas Ciências da Saúde (2nd ed.). Campinas: CPAQV.