kriativ.tech

Edição Nº 8 – Vol I
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
|

Cloud Data Security

Pedro Ramos Brandão
Researcher Évora University (CIFHEUS) - Coordinating Professor – ISTEC
pedro.brandao@istec.pt
Rui Antunes André
Master's Student in Informatics – ISTEC
rui.andre@my.istec.pt
DOI: 10.31112/kriativ-tech-2018-01-21

Abstract: The rapid growth of Cloud Based solutions creates a new paradigm that at same time raises and addresses many of the computer data security problems and challenges. On one side moving to Cloud can address some actual weaknesses and gaps of the enterprise security infrastructure and procedures but on the other side there is a new world of issues that must be addressed when moving infrastructure to a shared third-party provider. This paper will address some of these general drivers and concerns.

Keywords: Cloud, Security, DataCenter, SOC.

Resumo: *O rápido crescimento de soluções baseadas em cloud cria um novo paradigma que ao mesmo tempo gera e endereça muitos dos problemas e desafios relativos à segurança de dados informáticos. De um lado a migração para a cloud pode resolver algumas das fragilidades e falhas de segurança e procedimentos relativos à infra-estrutura da empresa mas por outro lado entramos num novo mundo de questões que devem ser tidas em conta quando se move a infra-estrutura para um fornecedor de serviços partilhados. Este artigo descreve algumas dessas questões e preocupações.*

Palavras-chave: *nuvem, segurança, centro de dados, SOC.*

I. Introduction

Threats, issues and legislation is becoming more and more strong and complex about security and data protection, changing the way about how organizations see computer security in all the dimensions and related management aspects.

In the recent past, not far away from nowadays, most of the solutions were based on setting an user password, an Anti-Virus application and a basic firewall that could filter inbound and outbound traffic. Nowadays, the simple implementation of these measures does not make any sense anymore or is effective

The crescent sophistication of all type of threats against corporate or personal data have an huge impact on the defense management complexity against these possible strikes. This is one of the drivers that could lead some enterprises to take decisions about moving partial or the total infrastructure and IT information systems to the cloud.

It is not cost-effective for a small/medium size company to have the proper conditions to operate a high-tier data center and internal security specialists that can assure 24x7 monitoring and implementation of all mechanisms required to have the organization secured. The largest cloud providers, due their scale and dimension, already address in a native

way these kind of services, physical security and resilience on their data centers.

II. Initial Assumptions and goals

IN this paper we will analyse some data security dimensions in corporate environments, not cloud based, with the objective to expose the difficulties that can be addresses with a possible migration to cloud;

- Physical DataCenter Security
- Detecting and blocking external threats (SOC)
- Business continuity, contingency and resilience

III. Physical DataCenter Security

This dimension, often neglected, has a huge importance on data security, either for organizations or individuals. In case of perimetral security breach, non-authorized personnel access, electricity power supply outages as air condition HVAC systems malfunction can easily lead to non-authorized third party access or even serious failures on IT system availability to the people that need to access it.
Traditionally, in medium / large size organizations, the computer data tends to be stored at their own data centers, normally in the headquarters or operations buildings. Focusing on the Portuguese reality, practically none of these organizations is focused on the specific management of these spaces on their technical components of HVAC, power supply, cabling and physical security and due that, there is an huge number of associated vulnerabilities. In these organizations the physical security based on authorized personnel access control list to the different building perimeters, CCTV monitoring, biometric identification and 24x7 surveillance generally is weak or even nonexistent, which potencies this risk [1].
In respect to the power supply, let's consider N+1, 2N that configures different levels of redundancy [2]. We can consider a good solution when we implement a 2N [3] system. For this, we must have the possibility to contract two power supply providers, each one operating in a different power stations (not possible in Portugal because there is only one provider), secured by different power generator groups and also by redundant UPS systems. These two different and segregated power lines will be supplied to each rack and delivered on segregated PDUs (Power Distribution Units) and to supply non-redundant power supply. Each rack should be supplied by these two power feeds avaliable on the PDUs and using ATSs (Automatic Transfer Switch) for the equipments that don't have dual power. This will assure a zero loss in the case of a failure over each power line / provider.

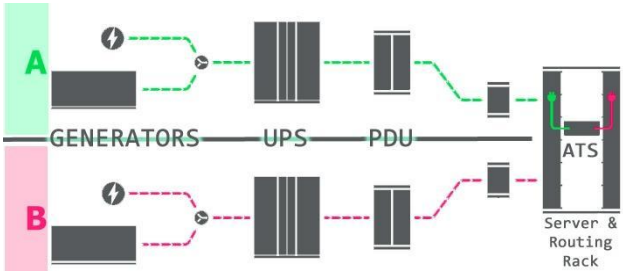

Fig 1- 2N power feed diagram

In relation to Air Condition / AVAC systems, it should be applied at minimum the n+1 redundancy. It means that, in abstract, if it is needing a cooling capacity of 10, there should be 3 units of 5 capacity each. With 3x5 configuration, it is possible the have a malfunction in one unit or even to stop it for maintenance keeping the cooling capacity of 10 [4].

IV. Security Operations Center - Security Incidentes detection, response and mitigation

It should be a requisite of medium to large size organizations, a 24x7 monitoring activity over all external security threats, including security vulnerabilities attack, DDOS and other attacks,

as it should be guaranteed a rapid response to a possible incident. These SOC [5] teams have applications and means that through access pattern analysis and centralized communication with updated databases by other organizations, it is possible to understand in real-time the possible threats and so, have a rapid response in the way that a possible attack can be quickly blocked and mitigated [6].
Obviously it is not easy or simple for the organizations to have the infrastructure and technicians to perform this job. In most of the cases, the entire IT department size is smaller than the expected size of a SOC team should have. One of the obvious moves for most of the large organizations is to contract these services from external specialized providers on IT security.

V. Resilience, Business Continuity and Contigency.

Another requisite which becomes more important day-by-day, and in most cases regulatory, is setup of the Business Continuity Plans [7]. The maturity of these plans is categorized in tiers, from 0 to 7, where 0 is no off-site-data and 7 is an "Highly Automated business integrated solution". For archiving an acceptable tier in order to have an acceptable RTO (Recovery Time Objective) and RPO (Recovery Point Objective) [8] normally it is required to have a secondary site where there is stored all backed-up, copied, replicated or synchronized data from the primary site. This is assured from Tier 4 / 5 upwards. At lower BCM tiers, generally not accepted due their low RTOs and RTSs, in case of a big disaster on main site, the mandatory daily data backups could not have any value, if those copies are not taken off-site daily.

VI. Cloud Environments - Data Security.

For the next analysis, we are considering the NIST Cloud definition [9], normally accepted in the academic and business environment.

The purpose of this point will be to try to demonstrate that cloud solutions, by default, address all the issues in previous points. With every big cloud players, these last challenges are all covered by the service nature; The main data centers of these cloud providers are normally tier IV (in Business Continuity Plan Scale [7]) as all of them have replication capabilities for another set of servers in other datacenter in the same region, on the limit could be for other continent. One classic exemple is the geographic dispersion of Azure sites, available in 56 regions all over the world [11] .

These types of data centers (main cloud suppliers) are tier 4 that means an availability of 99.995% equivalent to maximum downtime of 26 minutes per year. Just a remark that the most advanced datacenter in Portugal (Altice at Covilhã), that also provides some cloud services, is a tier III [13]. Also a small note to mention that one of the biggest and most important datacenter in Portugal works at an old cookie factory building that was rebuilt, near a car dealer in a busy street, where the perimetral security is very poor. It handles some dedicated infrastructures for financial services – banking sector.

Due to all of this, we can assume that the cloud solutions running on major cloud providers data centers are the most secure solutions at physical level and that provide the highest availability levels due to high data centers tiers - normally IV on the Uptime Institute [14] scale.

In relation to the SOC teams, these big players have also the top infrastructures at global level - large multidisciplinar security teams. At Microsoft, as an example, there is a team of 3.500 professionals that monitor 24x7 all of the accesses intrusions attempts in their cloud infrastructures. They address all the problems around the attacks, detection and response to security incidents.

VII. Conclusions.

It is demonstrated in the previous points that all the questions related with corporate and individual's data security hardly can have better answers and performance in self owned infrastructures than in Cloud environments.

The level of investment required to have self and proprietary physical resilient infrastructures and human resource teams capable of monitoring and mitigate in real-time the external threats are very high against the same service cost provided by the principal cloud providers. Due this, it is a common solution the system migration to the Cloud in a way that is possible to improve a security and resilience levels not incrementing a lot the operations running costs. There are many other drivers to migrate to the cloud but these related with security and availability are the most important ones.

The required improvement of maturity level of security systems and resilience of the corporate IT systems and data protection, the financial cost also rises and normally in a way that the organizations can't afford. The move to the Cloud can address it.

Almost all the big organizations, including the financial ones, and after a positive risk assessment, move their commodity applications and services to the Cloud - we're seeing in a recent past a collective movement of the local mail MS Exchange and Lotus Notes to Office 365 and GMail. It is already accepted by the companies that is movement is safe. Starting on this premise, in the high level managers and directors mailbox's content there is already all the sensible organization data, some of them classified as confidential, restricted and secret. This will facilitate and make natural the next steps about moving internal file shares and other commodities also to the cloud - like Googledrive, Onedrive, Dropbox, etc...
In my opinion, this is an absolute non-stoppable movement that establish a new security paradigm that start to be acceptable that cloud management and security is superior than the organizations owned data centers managed by their own teams.

References

[1] vXchnge. (2019). What Are the Most Important Data Center Security Standards. Retrieved 26 February 2020, from https://www.vxchnge.com/blog/data-center-physical-security-standards

[2] Data Center. (2018). Data Center Redundancy: N+1, 2N, 2(N+1) or 3N2 (distributed). Retrieved 26 February 2020, from https://datacenter.com/news_and_insight/data-center-redundancy-2plus1-2n-distributed-redundancy/

[3] Quote Colo. (2013). What is 2N Power and why it is important to Colocation Customers. Retrieved 26 February 2020, from https://www.quotecolo.com/what-is-2n-power-why-it-is-important-to-colocation-customers-2/

[4] Computer Weekly. (2011). Tier 3 Data Center design: the cooling checklist. Retrieved 26 February 2020, from https://www.computerweekly.com/tip/Tier-3-data-center-design-The-cooling-checklist

[5] Wikipedia. (2020). SOC. Retrieved 26 February 2020, from https://pt.wikipedia.org/wiki/SOC

[6] Security Operation Center Concepts & Implementation. Renaud Bidou (2020). Retrieved 26 February 2020, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.8577&rep=rep1&type=pdf

[7] Wikipedia. (2020). Business Continuity Planning. Retrieved 26 February 2020, from https://en.wikipedia.org/wiki/Business_continuity_planning

[8] Wikipedia. (2020). Disaster Recovery. Retrieved 26 February 2020, from https://en.wikipedia.org/wiki/Disaster_recovery

[9] National Institute of Standards and Technology. (2011). The NIST definition of Cloud Computing. Retrieved 26 February 2020, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[10] Statista. (2020). Amazon leads $100 billion Cloud market. Retrieved 26 February 2020, from https://www.statista.com/chart/18819/worldwide-market-share-of-leading-Cloud-infrastructure-service-providers/

[11] Microsoft Azure. (2020). Regiões do Azure. Retrieved 26 February 2020, from https://azure.microsoft.com/pt-pt/global-infrastructure/regions/

[12] Wikipedia. (2020). Data Center. Retrieved 26 February 2020, from https://en.wikipedia.org/wiki/Data_center

[13] Wikipedia. (2020). Data Center da Covilhã. Retrieved 26 February 2020, from https://pt.wikipedia.org/wiki/Data_Center_da_Covilh%C3%A3

[14] Uptime Institute. (2020). Uptime Institute. Retrieved 26 February 2020, from https://uptimeinstitute.com/

[15] Microsoft. (2020). Security Operations. Retrieved 26 February 2020, from https://www.microsoft.com/en-us/security/business/operations