ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (30-34), Month: October - December 2021, Available at: www.researchpublish.com

SECURE BY DESIGN PRIVATE CLOUD INFRASTRUCTURE

Badi Salah[1], Hasan Ahmadi[2], Mohammed Fadlalla[3], Mohammed Jugaiman[4]

Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **In recent years many enterprises have transformed from traditional data centres into Software Defined Data Centre leveraging private and public Cloud Technologies. This study aims to analyse the resiliency of a typical private cloud infrastructure to security threats and vulnerabilities. A series of assessments and risk analysis were performed that showed the existence of major design weaknesses. Thus, design enhancements are recommended based on the findings to render Private Clouds more secure and to better protect Company data and business.**

Keywords: **private cloud, information technology, cyber security.**

I. INTRODUCTION

Cloud Computing is the delivery of on-demand computing resources ranging from applications to data centres. This brings many benefits to enterprises such as cost efficiency, flexibility, elasticity and business continuity (IBM, 2019).

Large enterprises provide IT applications and services to thousands of active users. Many of such applications are customized to business needs by developers working around the clock onsite, or remote, bringing new features and enhancements as required by the business. Traditionally, enterprises have been running its data centres for years based on physical servers where applications are hosted and pinned to their own physical hardware. With long cycles of commissioning and decommissioning servers and applications, such enterprises could not keep up with the fast-growing business demand. The emergence of virtualization and Cloud computing has helped them to be more dynamic where the transformation to a Software Defined Data Centre has revolutionized the way IT services are provided. The elimination of wait time for procurement, rapid provisioning of servers on demand and the sharing of computing resources are some of the benefits realized with the adoption of cloud technologies. While public cloud providers seem a good fit to help realize these benefits, the introduction of strict data protection regulations most often limits their use. Thus, it becomes imperative to transform traditional on-premise data centres into a private cloud infrastructure.

As such transformation brings numerous benefits and advantages, this big shift in architecture, processes and functionality, introduces major security considerations that must be addressed in early stages. In most cases, not all security considerations are addresses properly due to many factors such as manpower shortage, software compatibility, people resistant to change and having operated a legacy infrastructure for long time.

This study looks at typically transformed Private Cloud architecture, assess and analyse its security and proposes design enhancements. In addition, as future work this study examines tools and solutions that would help in boosting the resiliency of private cloud to emerging security threats and vulnerabilities.

II. MOTIVATION

Although establishing a Private Cloud for new startup companies is challenging, it is even a more complex and challenging task for well-established big scale legacy IT infrastructure typically found in large enterprises. Such implementation touches every aspect of operation, people, processes, and technologies. Thus, a major transformation is required to ensure success of a Private Cloud implementation. Throughout such major transformation, some details may fall in the cracks due to manpower shortages, software compatibility or other factors resulted by running a traditional and a cloud infrastructures side-by-side in a phased approach.

The following is a list of common security considerations that are usually found to be either lacking or even missed:

- Security & operational policies, procedures, processes and standards.
- Access management
- Layers of security around the environment.
- Segregation of duties.
- Protection of multi tenancy applications and services.
- Security monitoring and network protection.
- Log correlation & analysis.
- Software Defined Firewalls may require additional protection.

Enterprises use private cloud to run business critical applications such as Finance, Sales and HR, therefore, security is vital. As the diversity and sophistication of global threats continue to increase, and critical vulnerabilities uncovered, IT organizations need to be ready to face such security challenges. High impact newly-introduced risks is a great motivation to analyse the security resilience of private cloud implementations and to raise its readiness to face emerging threats and vulnerabilities.

III. SECURITY GAPS

Security analysis of a transformed cloud infrastructure requires a closer look at what actually is changed by the transformation process. Traditional datacenters are usually operated and managed with services hosted in silos with different support teams dedicated to each software/infrastructure component as opposed to sharing of resources and central management in a cloud. Noting down these drastic changes help IT organizations identify the focus areas to look for security gaps. The following table summarizes main changes typically occurring with the security challenges they impose:

TABLE 1: INFRASTRUCTURE CHANGES BY TRANSFORMATION

Before transformation		After transformation	Security Challenges
Tenants	Each application has dedicated servers, storage, network cards/cables.	Applications share hardware resources (storage, network cards/cables, storage).	A compromise of one application will affect other applications. A compromise of one hardware component (server or storage) could impact multiple applications. Network flows are more dynamic; source/destination traffic keep shifting between different parts of the network making it harder to detect anomalies with normal tools.
SAN Storage	Storage zoning and LUN masking[1] is done per application.	Storage zoning and LUN masking is done per host cluster[2].	Data segregation is managed by hypervisor which moves application data dynamically as needed. This results in little to no visibility of where application data resides on disk.
Network	Application traffic is directly sent to physical network switches.	Application traffic is abstracted, encapsulated and often encrypted by hypervisors	Normal network monitoring tools provide limited functionality on cloud network traffic.

[1] LUN Masking is a level of security that makes a LUN (logical SAN disk) available to only selected hosts and unavailable to others.

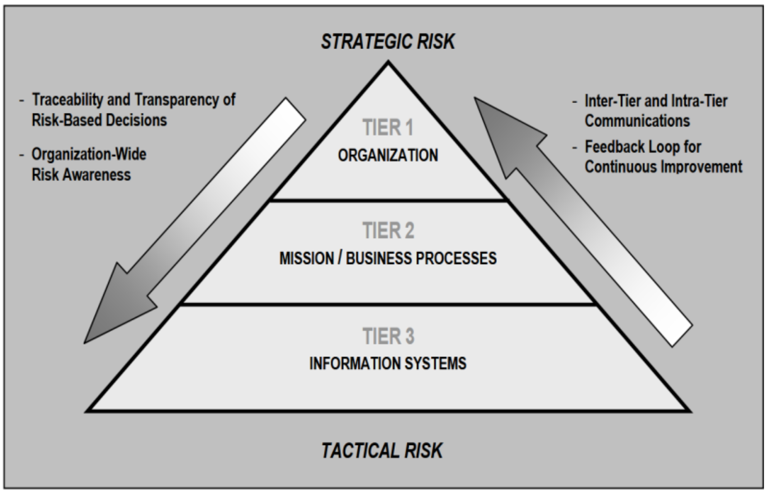
[2] A host cluster is a group of 2 or more bare metal servers which are used to host virtual machines. The server nodes (physical machines) work together to provide redundancy and failover virtual machines.

Infrastructure	Infrastructure components such as compute, network, firewalls and storage run on hardware systems with minimal to no virtualization.	Infrastructure components (compute, network, firewalls and storage) are fully virtualized and managed by hypervisors.	Critical infrastructure components share the same codebase. A vulnerability of the hypervisor affect all critical infrastructure components.
Inf. Mgmt.	Each infrastructure component (compute, network, firewalls, storage) have its own enclosed management mechanism and operated by separate support team.	All infrastructure components are centrally managed cloud tools and operated by cloud admins.	Management tools are single point of failure. Management tools often exposed to all network endpoints. A bug or error on the tools can cause widespread damage. Segregation of duties doesn't hold.
Admin Access	Admin access is divided by infrastructure component. Storage, compute, network, firewalls and DNS each has its own admin accounts.	Admin access to cloud provides admin access to all infrastructure.	Cloud admin accounts have excessive permissions by nature that allows certain operations outside designated duties.
DMZ	DMZ applications hosted on dedicated hardware in terms of compute, storage, network and security. Physical access is also controlled within datacenters.	DMZ share same hardware resources as intranet. Security is provided by virtual firewalls and relies on hypervisor logical segregation.	A DMZ VM could be running on the same hardware as an intranet VM isolated logically. This logical isolation is the only protection.
Policies	Policies and standards in place for long time with many review cycles over the years.	New policies and standards are created to accommodate private cloud operations.	Fairly new policies and standards that haven't been through review cycles.

IV. ASSESS RISK

Calculating risk is very challenging especially in large enterprises. That is due to the ambiguity surrounding value of loss calculation. For instance, loss of reputation or potential business impact are typically estimated to the best of knowledge as the real numbers are usually subject to confidentiality regulations. Therefore, we advise enterprises to adopt a known risk assessment standard such as the National Institute of Standards and Technology (NIST) guide semi-quantitative approach for conducting risk assessments. This approach helps IT conduct risk assessments navigating the ambiguity surrounding these numbers. In semi-quantitative approach representative numbers are used to indicate a risk level ranging from "Very Low" to "Very High". This approach is also vulnerability-oriented; starts with exploitable infrastructure weaknesses and identify threat events that could exercise those weaknesses together with possible consequences of them being exploited.

Assessments should be conducted at Tier 3 (Information System Level) as defined in NIST guidelines. Results can then be fed into risk assessment conducted at higher levels of Tier 2 and Tier 1.


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Below are the top 3 threats and weaknesses IT organizations should consider conducting risk assessment on:

- Admin accounts have excessive privileges: The threat is when privileged accounts are used to introduce additional security gaps, compromise data confidentiality, integrity and/or availability.

- Cloud management components are widely reachable: A threat of malicious actor performing Denial of Service, Brute-force or exploiting an unknown vulnerability to gain access to critical cloud engine component.

- DMZ and intranet VMs reside on the same hardware: Unknown vulnerability could be found by an attacker and threatens to use in an attack.

V. RECOMMENDED DESIGN CHANGES

Based on the risks and security gaps identified on this study, the following design changes are strongly recommended to minimize their impact. In this section of the report we detail these design changes.

A. Hardware and hypervisors

Divide cloud hardware, or hypervisors, to 4 different zones that are separated by physical firewalls:

- Intranet: Dedicated to host intranet VMs.

- Edge: Dedicated for virtual appliances for cloud network control plane such as : (i) Edge switches; (ii) Controllers; (iii) Load Balancers..etc

- Management: Clusters dedicated for cloud engine components such as vCenter, log server, network monitoring, VM monitoring and automation portal.

- DMZ: Clusters that host DMZ VMs.

B. Cloud management

Design an out-of-band management network that is completely separate from intranet network infrastructure. This network should include dedicated switches and should not be routable. Access to this network should be monitored and limited to admin teams only. Traffic flowing in this network is strictly limited to management traffic, network control plane traffic and level-0 administration only.

C. Cloud network

The following are recommended design modifications for cloud network:

- Only allow software-based subnets to be provided to workloads.

- Segregate DMZ and regular subnets by means of routing isolation, no routing should be possible between the two.

- All virtual machines should be protected with distributed cloud firewalls for extra level of security.

- Deploy a perimeter firewall appliance in the cloud edge components and bind it with the data center physical perimeter firewalls.

VI. DESIGN PROS AND CONS

Although the recommended design modifications will address critical security concerns, they may potentially have some drawbacks. In this section, we will shed a light on these areas.

A. Strengths

Reduced attack surface: Critical components such as hypervisors, cloud management interfaces, network controllers are on isolated network that can only be access by system admins. This significantly reduce attack surface.

Unified network access: The perimeter firewall placed at the cloud virtual perimeter, Edge, extending the rules from the actual data centre firewall to the cloud software defined network. This also provides more visibility to security monitoring teams.

DMZ Isolation: Separate hardware, network and storage for DMZ, which gives a level of assurance if an attack should take place in DMZ it won't easily propagate to Intranet. In addition, a misconfiguration of a VM security parameter or networking resources doesn't jeopardize Intranet services. A successful attack to the hypervisor is contained due to the separation of management network.

B. Drawbacks

Cost: The new design is more complex and requires more hardware and software licenses. There are more components to manage and configure for expansion. Such design requires careful planning and diligent work for proper deployment. In addition, there is additional maintenance cost operating such design.

Skilling up: Added security layers of this design require training administrators to adapt to. In addition, troubleshooting becomes trickier as more components are involved.

VII. FUTURE WORK

In future, we will explore tools and techniques that can be developed or deployed to further enhance security of the private cloud. For example, placing an intermediate appliance or firewall that act as a proxy between administrators and cloud management components. Such appliance can intercept and inspect commands then decide an action accordingly.

VIII. CONCLUSION

As Information Technology is dynamic in nature where the trend shows a major shift in operations as many have witnessed moving from Mainframes to Client Server, then to virtualization, and finally private Cloud, it is imperative that Enterprises undergo these transformations with due diligence. This study is a clear example that adopting technology quickly without the careful planning and paying attention to every security detail could jeopardize the existence of the business.

REFERENCES

[1] (J.R.)Winkler, V. (2011). Evaluating Cloud Security: An Information Security Framework. In V. (J.R.)Winkler, Securing the Cloud (pp. 233-252). Elsevier Inc.

[2] Cappuccio, D. (2013, July 1). Software Defined Data Centers – Hype or Reality? Retrieved from Gartner Blog Network: https://blogs.gartner.com/david_cappuccio/2013/07/01/software-defined-data-center

[3] Dimitrios, Z., & Dimitrios, L. (2012, March). Addressing cloud computing security issues. Retrieved from Science Direct: https://www.sciencedirect.com/science/article/pii/S0167739X10002554

[4] Faatz, D. (2018, March 12). Best Practices for Cloud Security . Retrieved from Carnegie Mellon University: https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html

[5] Hange, M. (2011). Security Recommendations for Cloud Computing Providers. Retrieved from German Fedral Office for Information Security.

[6] How to audit the cloud. (2019). Retrieved from ICAEW.

[7] IBM. (2019). Cloud computing: A complete guide. Retrieved from IBM Cloud website: https://www.ibm.com/cloud/learn/cloud-computing

[8] National Institute of Standards and Technology. (2012, Sep). Guide for ConductingRisk Assessments.

[9] Rouse, M. (2018, Fev). cloud SLA (cloud service-level agreement) . Retrieved from Tech Target: https://searchstorage.techtarget.com/definition/cloud-storage-SLA

[10] Suby, M. (2014, July). Best Practice Security in a Cloud-Enabled World.