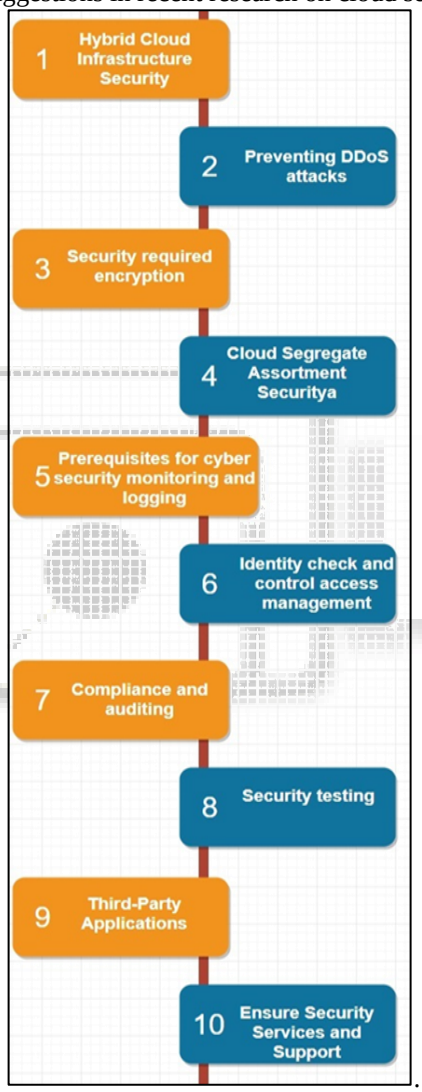
Checklist for (Must Have) Cloud Security Roles & Responsibilities

Ashish Yadav
Computer Science & Information Technology
CERT, India

Abstract— This document contains a Checklist for cloud security roles and responsibilities that can be used to develop or calculate security, privacy, risk and requirements for any kind of cloud computing jobs and services. The paper has been conjunct from established industry rules, guidelines, policies, standards and best practices, additional with importance of GDPR guidelines, and discussing minimum security suggestions in recent research on cloud security



Checklist for Cloud Roles & Responsibilities

Key words: Cloud Security

I. HYBRID CLOUD INFRASTRUCTURE SECURITY

A worldwide view of substantial threat activity for continuous coverage across the infrastructure. A dedicated universal security research team developing threat pattern, signatures, connection rules, log analysis, and website application security policies and procedures to protect you from any adverse situation in any cloud environment 24x7x365 monitoring by any other cloud related applications and solution.

II. PREVENTING DDOS ATTACKS

Protect outer layer (internet facing layer) of cloud infrastructures against all known types of DDoS attacks on the websites, data centres, infrastructure or DNS of cloud infrastructures. Develop a Denial of Service Response Plan to Secure Network Infrastructure, Practice Basic Network Security, Maintain Strong Network Architecture, Outsourcing expert DDoS prevention, understand the Warning Signs.

III. SECURITY REQUIRED ENCRYPTION

Encryption is used on any data is indisputable. Select cloud environments that adopt encryption procedure. Know how is encryption handled? Who has the keys? The encryption keys, metadata and access control is onsite available. Secure important information in transit with end-to-end encryption. Now-a-days encryption technology provides privacy and security for commerce that use the Internet to communicate and run business online.

IV. CLOUD SEGREGATE ASSORTMENT SECURITY

The cloud provider work force, data centre work force may not be the same person who operates the system. Does your organization have a configuration and change management plan? Evaluate the ability of cloud services to comply with information security best practices and ensure future deployments within the cloud. Deployments with its configuration and change management plan implementing logical controls to application level security configurations such as mandatory access controls for authorization to access the data.

V. PREREQUISITES FOR CYBER SECURITY MONITORING & LOGGING

Develop a cyber-security monitoring and logging strategy, consider all effecting factors of cyber security monitoring and logging together in one framework, understand the key concepts of cyber security monitoring and logging. Find how to carry out cyber security logging and monitoring in a more fruitful way which leveraging industry best practice.

VI. IDENTITY CHECK & CONTROL ACCESS MANAGEMENT

Identity check and control access management are important aspects of security for a cloud. What rules are implemented for Remote access, Is multi factor authentication used? , Does system can detect multiple unsuccessful logins with similarly suspicious authentication or intrusion detection and credential compromise activities? , What steps of policies are applied if a user private details or account is compromised?

VII. COMPLIANCE & AUDITING

The trusted cloud infrastructure is a framework that can work as a baseline for compliance and auditing. Compliance and auditing refer to entire internal and external processes that an organization implements for control requirement such as procedures, implement policies, processes with other requirements.

VIII. SECURITY TESTING

Security testing, especially Vulnerability Assessment & Penetration Testing, can easily produce a myth of security. Cloud Computing Vulnerability Assessment and Penetration Testing are method of actively testing and examining the Cloud system security by simulating the attack from the malicious code.

IX. THIRD-PARTY APPLICATIONS

Integration with third-party tools plays a significant role. Because there is technology preference with cloud integration. Have a strategy to develop and tests in comply with third-party components. Native to cloud service, domestic, third party cloud. It directly effects on the performance, availability, IDS/IPS with firewall policy as well as authority of the service. Preferable Cloud service also allows you to build policies to handle third party applications which organisation or user installed. These policies secure domain by automatically invalidate access to the domain or account attached with the application.

X. ENSURE SECURITY SERVICES & SUPPORT

Cloud continues enhancing security but it remains a big factor of concern in the cloud. A dedicated security team, including a senior members of the company on board, is manifest of ensuring the security, confidentiality, and integrity of cloud service.

XI. CONCLUSION

Adoption of cloud services will continue to rise. Better Cloud is built and hosted certainly reduce the attack surface by limiting the security challenges. These initiatives should also produce results that successfully reduction security, privacy, risks over time.

REFERENCES

[1] https://www.coalfire.com/The-Coalfire-Blog/May-2018/Cloud-Security-Governance
[2] https://fraudwatchinternational.com/mobile-applications/third-party-apps-threatening-companys-security/
[3] https://www.bettercloud.com/security-and-compliance/
[4] https://www.intel.com/content/www/us/en/cloud-computing/overview.html
[5] https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/vendor-and-thirdparty-management

