Data Security in Cloud Platforms

Liam Bergerson

CSU - Global

ITS446-1

J. Mills

1/29/23

Data Security in Cloud Platforms

The idea of cloud computing was invented in the 1950s. As the years go by, cloud computing is becoming more advanced. Presently, the cloud is the most advanced it has been since its invention. However, the security threats towards the cloud are becoming more advanced as well. Measures must be taken by organizations to prevent these threats from being exploited for private cloud models. For the public cloud, the cloud provider must ensure that security measures are in place to also prevent threats from being exploited. In this paper, some best practices will also be discussed in order to secure hypervisors.

Security Measures

To ensure that data is protected on the cloud, multiple security measures must be in place. Encryption should be one of the first measures implemented in a cloud environment. Advanced encryption must be in place for data at rest and data in transit. For data at rest, symmetric encryption will be used, more specifically, AES-256. Symmetric encryption uses the same key to encrypt and decrypt data. Advanced Encryption Standard 256 (AES-256) is a symmetric encryption standard that uses a 256-bit block cipher to encrypt data. For data in transit, TLS/SSL will be used. Transport Layer Security/Secure Sockets Layer (TLS/SSL) is an asymmetric encryption standard that is used to secure web sites. Asymmetric encryption uses a public key to encrypt data and a private key to decrypt data.

Account security must also be considered when securing a cloud environment. In order to achieve this, every user must have only the minimum amount of permissions in order to achieve operations and nothing more. This is known as the principle of least

privilege. A password policy that includes complexity requirements must be mandatory. A complex password should be around eight or more characters long with the inclusion of upper and lowercase letters, numbers, and special characters. To further secure the login process, Two-Factor Authentication (2FA) will prompt the user to input a multi-digit code from a third-party app in order to fully log in.

Finally, since the cloud environment is mainly accessed via the network, that also must be secured (Heydari et al., 2014). Security measures such as firewalls, intrusion detection systems, and anti-virus software will be used to ensure maximum network security (Coppelino et al., 2016). Firewalls will ensure malicious traffic is blocked from entering the network. Intrusion Detection Systems will ensure that malicious traffic that passes through the firewall and enters the network will be detected. Finally, anti-virus software will be used to quarantine and remove any malicious software on systems and network devices.

Cloud Platform Simplicity

The three cloud platforms that organizations can use are private, public, and hybrid. All three of these platforms range in complexity in regards to configuration, patching, and securing. In a private cloud model, the organization takes full responsibility for configuration, patching, and security. In a public cloud model, the cloud provider is responsible for configuring, patching, and securing the service. In a hybrid model, the organization will have to take some responsibility for configuring, patching, and securing the cloud, however, the public cloud is leveraged for other means. The public cloud is the easiest route for an organization to take due to almost all responsibility being taken by the cloud provider for its implementation. In a private cloud

model, the organization is completely responsible for buying the equipment needed. The setup and configuration equipment is a complicated ordeal that may require a specialized skill set. Security is also an ordeal that may require additional assistance. In a hybrid cloud model, the same issue as with a private model may arise, but isn't as prominent. The only difference is that the public cloud is leveraged for cases such as elasticity where resources are scaled up or scaled down based on traffic. For the public cloud, the only thing the organization must do is research cloud providers and pick the best one for their needs. The cloud provider is responsible for configuring, patching, and securing the service.

Hypervisor Security Best Practices

Shackleford (2012) discusses many best practices in order to optimally secure a hypervisor. Hypervisors must be patched when a new patch releases. Patch management is a core security principle in IT. It fixes vulnerabilities that were present in previous patches. Hypervisors must also follow this principle in order for security to be improved. Establishing secure communications will ensure that communication with remote clients and management platforms are secure. Secure Sockets Layer and Transport Layer Security along with digital certificates are used to achieve secure communications. Changing default settings is one of the easiest things to do to drastically improve security, however, it is commonly disregarded. For example, In VMware ESXi, information accessed by the web browser will point to the IP address of the management interface by default. This must be changed so threat actors do not have information on the management interface of the hypervisor. Securing the permissions of users and groups will prevent users from having too many permissions.

Having too many permissions will allow for more entry points for a threat actor. As mentioned previously, the principle of least privilege will be used to restrict access for all users and groups.

Conclusion

In order for data to be properly secured on the cloud, various security measures have been identified such as encryption, account security, and network security. Some cloud platforms are easier to secure than others. The public cloud model has been identified as the easiest to configure, patch, and secure as the organization need only research and pick a cloud provider that suits their needs. The cloud provider itself is responsible for configuring, patching, and securing the service. Finally, some best practices to secure a hypervisor have been identified such as changing default settings, securing communications, patch management, and user and group access control.

References

Coppelino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2016). *Cloud security: Emerging threats and current solutions*. Sciencedirect. https://linkinghub.elsevier.com/retrieve/pii/S0045790616300544

Heydari, A., Tavakoli, M., & Riazi, M. (2014). *An Overview of Public Cloud Security Issues*. Researchgate. https://www.researchgate.net/publication/263389263_An_Overview_of_Public_Cloud_Security_Issues

Shackleford, D. (2012). *Virtualization Security: Protecting Virtualized Environments* (1st ed.). Sybex.