OPTION #1: Security of Data

Liam Bergerson

CSU - Global

ITS441-1

J. Leaston

10/9/22

OPTION #1: Security of Data

As more organizations transition from traditional, on-premise data storage to cloud data storage, the security requirements become more crucial. In order to protect data in the cloud from being stolen, modified, or deleted, cloud security methods are needed to ensure sensitive data retains confidentiality and integrity. Multiple security solutions are available to organizations and a few will be discussed, including identity and access management (IAM), data loss prevention (DLP), security information and event management (SIEM), and encryption techniques for data-at-rest and in-transit.

Identity and Access Management (IAM)

Identity and access management provides organizations with a centralized way of managing user identities, automating access controls, and meeting compliance requirements across cloud environments (Redhat, 2022). IAM essentially ensures the right people have the right access to cloud data to mitigate security or compliance risks. IAM presents an authentication mechanism that both captures login information and allows IT administrators to monitor and manage activity across the infrastructure (Redhat, 2022). One such method to achieve IAM's goal of authentication is by using multi-factor authentication. IAM also accomplishes authorization by implementing access controls in the infrastructure. More specifically, it assigns a user identity with a predefined set of access rights associated with the user identity (Redhat, 2022). The principle of least privilege is followed when assigning access rights to each user. The user only needs access to resources that they need to accomplish their work and nothing more.

Data Loss Prevention (DLP)

Perhaps one of the biggest disasters that can happen within an organization is the loss of sensitive data. As more and more organizations migrate from on-premise data storage over to cloud storage, the need for data loss prevention strategies grows. Data loss prevention is essentially a set of tools and processes that are used to ensure all sensitive data of an organization is not lost, misused, or accessed by unauthorized users (Widler, 2019). When an organization chooses a DLP solution, it requires identical protection for all users on or off of the network. Basically it means that all users should be provided with the same level of security to all users with policies that follow users wherever they go (Widler, 2019). If this concept is not implemented, remote users can easily bypass inspection protocols which poses a risk towards the confidentiality of data. Inspection of SSL-encrypted traffic should also be considered when choosing a DLP solution. However, it should only be considered if the organization is harboring critically sensitive data that absolutely cannot be leaked. Due to the enormous amount of processing power SSL-encrypted traffic inspection requires, finding a DLP solution that supports this ability will be costly. Most, if not all, of the traffic going across networks is encrypted. Uninspected, encrypted, traffic can risk the confidentiality of data (Widler, 2019). Unauthorized users can use encryption for their benefit and try to leak sensitive data over the network because it cannot be inspected. Inspection of SSL-encrypted traffic can prevent data obfuscation by threat actors by natively scanning encrypted traffic for sensitive data.

Data-at-Rest and Data-in-Transit Encryption

Encryption for data-at-rest is encrypting data that is not traveling within the system or network, or being interacted with by an application (Ryan, 2021). It's essentially encrypted data sitting in a repository. Encryption for data-at-rest is needed to protect sensitive data from unauthorized users that have breached the network and are looking for data within databases or unstructured data locations. Symmetric key encryptions can be used to encrypt data-at-rest. Symmetric key encryption uses one single key for encrypting and decrypting information. For example, BitLocker for Windows uses AES-128 bit encryption to encrypt all data within a repository. In terms of the cloud environment, BitLocker can be used in the Microsoft Azure cloud service to encrypt all sensitive data within the cloud so it cannot be accessed by unauthorized users.

Encryption for data-in-transit is used to send data over the network or over web pages (Ryan, 2021). Encryption for data-in-transit is needed to prevent sensitive data that is being sent over the network or the web from being intercepted by unauthorized users. Asymmetric encryption can be used to achieve protection of data-in-transit across networks. Asymmetric encryption uses two keys, the public key which encrypts, and the private key which decrypts. For example, Cloud Key Management Services from Google supports the Rivest, Shamir, Adleman (RSA) algorithm for asymmetric encryption to encrypt data in the cloud. For web pages, Secure Socket Layer (SSL) and Transport Layer Security (TLS) can be used to encrypt traffic going to and from web pages (Ryan, 2021).

Conclusion

As technology evolves throughout the years, the size of data increases as well. Traditional on-premise data centers are slowly becoming more expensive to set up and maintain for organizations. This results in more organizations transitioning to the cloud which offers far more options for data storage and is cost-effective. However, the need for security also becomes more critical to secure sensitive data being stored on the cloud. Methods like identity and access management, data loss prevention, and encryption techniques for data-at-rest and data-in-transit become more prominent in order to ensure sensitive data retains its confidentiality and integrity.

References

Redhat. (2022). *What is identity and access management (IAM)?* https://www.redhat.com/en/topics/security/what-identity-and-access-management-iam

Ryan. (2021, June 9). *Encryption in-transit and Encryption at-rest - Definitions and Best Practices*. Ryadel. Retrieved October 6, 2022, from https://www.ryadel.com/en/data-encryption-in-transit-at-rest-definitions-best-practices-tutorial-guide/

Widler, M. (2019, December 6). *Data loss prevention's future is in the cloud*. ITProPortal. Retrieved October 6, 2022, from https://www.itproportal.com/features/data-loss-preventions-future-is-in-the-cloud/