Brian Sowers

11/24/2023

Data Center, IaaS and SaaS and Mobile

1. Consider the scenario where you are managing your company's cloud services solution. In general terms, briefly explain the security responsibilities and expectations for:

A) The responsibility for patching and updating the application lies with the Application Service Provider. The provider takes care of maintaining the application infrastructure, which includes things like data management, runtime, middleware, operating systems, virtualization, servers, storage, and networking. In this scenario, customers don't have to worry about these technical aspects; it's all handled by the provider (Secure Business Operations Module 3, 23).

B) Network Providers are tasked with responding promptly to and blocking any reported attacks that originate from their networks. They also keep a close eye on network activities to detect any unusual behavior, signs of attacks, or abnormal data packet volumes.

C) Data and Storage Providers manage the storage aspects of virtualization, servers, and networking. Meanwhile, customers are responsible for handling applications, data, runtime, middleware, and the operating system. The data and storage provider handles tasks like data backups, routine checks, and allows customers to customize their storage options while ensuring the data's integrity and availability on their cloud infrastructure.

D) Customers have different roles depending on whether they are using IaaS or SaaS. With IaaS, customers have control over operating systems, storage, and deployed applications, while the provider manages networking components and owns the applications and data. In the case of

SaaS, customers are given access to the application but are responsible for the security of their data. Customers also decide which applications are sanctioned, tolerated, or unsanctioned and establish appropriate policies for each category. Importantly, customers don't need to have in-depth knowledge of the underlying cloud infrastructure in either IaaS or SaaS scenarios (Secure Business Operations Module 3, 22).

2. Consider the scenario where you are managing your company's cloud services solution. Your company application is accessed through many different mobile BYOD endpoints. Describe a security solution that will secure sessions to your cloud-based application without having to secure the mobile endpoint.

To secure sessions to a company's cloud-based application accessed through various mobile Bring Your Own Device (BYOD) endpoints without directly securing the mobile devices, a multi-layered security strategy is essential. "A layered approach for data center security starts with the network," and it should include measures like firewalls, intrusion detection, and encryption protocols to protect data in transit (Goel & Dhamija, 2015). Additionally, deploying a Web Application Firewall (WAF) can provide an extra layer of protection by "filtering incoming traffic for potential threats at the application layer" (Goel & Dhamija, 2015).

Real-time user session monitoring tools can be instrumental in securing sessions, as they focus on monitoring "user behavior and timing" directly within the application (Kephart, 1). These tools help detect any suspicious behavior during user interactions with the application, enhancing overall security. "Strong authentication methods, such as multi-factor authentication

(MFA), and stringent access controls" are also vital (Goel & Dhamija, 2015). This ensures that only authorized users can access the application.

Furthermore, regular security audits and vulnerability assessments are crucial to identify and address potential security weaknesses proactively (Goel & Dhamija, 2015). Data encryption for both data at rest and in transit within the cloud-based application adds an extra layer of security, protecting sensitive information regardless of the security status of the mobile endpoints. This aligns with recommendations to follow the ISO 27000 framework and deploy best-of-breed technologies for designing a robust security architecture (Goel & Dhamija, 2015). By implementing this comprehensive security approach, companies can enhance the protection of their cloud-based application while maintaining flexibility for users with different mobile BYOD devices.

Works Cited

Goel, Prikshit, and Kamal Dhamija. “Securing the Future with Next-Generation Data Center Security.” *Tata Consultancy Services.* https://panacademy.net/CourseFiles/sbo/Next_Generation_Data_Center_Security.pdf. Accessed: 24 November 2023.

Kephart, Nick. “Monitoring SaaS Performance from the End User.” *ThousandEyes.* https://www.thousandeyes.com/blog/monitoring-end-user-saas-performance. Accessed: 24 November 2023.

“Secure Business Operations Module 3”. https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_3.pdf. Accessed: 24 November 2023.