Data Center, IaaS and SaaS and Mobile

Angela Milova

Palo Alto - Secure the Future

1. IaaS/SaaS/Data Center- 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. Application Service Provider, b. Network Provider c. Data/Storage Provider, d. Customer

It is crucial that all parties involved communicate and establish a comprehensive and effective security framework for the entire cloud services solution. In cloud service solutions, security responsibilities and expectations vary among different providers and customers. a) Application Service Provider (ASP): Responsibilities include developing secure applications, patching them regularly, and implementing robust user authentication and authorization with the least privilege to avoid any data breach. Monitoring and responding to incidents faster and documenting them on the playbook for further reference is also essential. Expectations involve not only ensuring functionality but also securing applications. Vulnerability scans are conducted often, and vulnerabilities are patched based on criticality. In case of issues with the application, clear communication needs to happen between the security team, the web development team, and the customers (Gomes, Iivari, Ahokangas, et. al, 2023). b) Network Provider: Having a secure network infrastructure is fundamental for a company. Implementing firewalls and intrusion/prevention systems is also crucial. Data in transit needs to be encrypted to ensure the confidentiality of it. Expectations when it comes to a network provider are that the network needs to be reliable and secure at all times. Monitoring and mitigating network-based threats as fast as possible is also another expectation. In case there are network security incidents, it is important that they are addressed as soon as possible (Erlangga, Ramathan, 2022). c) Data/Storage Provider: Data storage is a crucial part of the organization. As data is the most important asset and the most valuable thing that malicious actors are after, it is important to

ensure its protection. Responsibilities include securing the data centers and databases and implementing encryption for data at rest. This ensures that the data is protected from unauthorized users. Regular backups are important to ensure the availability and integrity of data. Documentation on how data is saved and backed up is very important to have consistency. Expectations when it comes to data storage are that data should not be altered or modified to comply with the confidentiality and integrity of the CIA triad. Managing access controls to data storage must be done only by authorized users. Least privilege policy needs to be followed to access the data, especially on personally Identifiable Information (PII) (Galiveeti, Tawalbeh, El-Latif, et. al, 2021). d) Customer: It is important that the company and the customers have transparent communication as this ensures trust. Responsibilities include implementing security measurements in the cloud environment using identity access management to ensure that customers are protected. Also, it is important to monitor user activity and ensure compliance with security policies. This becomes very important, especially in the health sector, where insider threats are rising. Expectations that come with this section are that customers access a secure and well-maintained cloud infrastructure (Mohammed, Zeebaree, et. al, 2021). Constant communication when it comes to the latest security breaches and awareness to ensure security in the cloud environment. One service that customers could use is Palo Alto Prisma, which provides many good tools to ensure security in cloud environments.

2. Endpoint/Mobile/Enterprise- 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 provide secure sessions for the cloud-based application without directly securing mobile endpoints requires a combination of different security measures. Some of them include: a) Implementing and Enforcing Multi-Factor Authentication (MFA): Many companies implement MFA; however, not many enforce it. While MFA may not be very convenient for users, it adds an important extra layer of security, preventing unauthorized users from gaining access to a system even if they have obtained some credentials (Muxtoriddinov, Khudoykulov, Allanov, 2023). b) Cloud-Based Access Control: Based on strong authentication and MFA, implementing context-aware access policies becomes crucial. These policies consider factors such as user location, device type, and time of access. They help prevent unauthorized access from untrusted locations or devices (Granger, 2023). For example, if a user consistently logs in and uses MFA from the United States, an attempt from another country can be blocked, protecting both the user and the company from malicious attempts. c) Token-Based Authentication: Using token-based authentication reduces reliance on traditional username-password combinations. Many users tend to use easily memoizable passwords that are susceptible to brute-force attacks. Implementing OAuth, for example, reduces the risk associated with using a username and password; instead, it employs a token, enabling secure third-party access to resources without exposing credentials (Loginradius, n.d). d) Encrypted Sessions: Enforcing the use of HTTPS instead of HTTP ensures that data is encrypted in transit (Cloudflare, n.d). Implementing encryption provides better protection against attacks such as man-in-the-middle attacks. e) Real-Time Alerts: Building rules

and dashboards with real-time alerts is crucial for the security team. These alerts offer immediate feedback on suspicious activities, unauthorized access attempts, or any unusual user behavior. Monitoring user behavior is especially vital in a cloud-based application as it enables a fast response to threats (Yang, Okutan, Werner, 2021). By combining cloud-based access controls, multi-factor authentication, session management, and continuous monitoring, this security solution helps secure sessions to the cloud-based application without directly securing the mobile endpoints.

References

Erlangga, W. K. A., & Ramadhan, M. R. (2022). Potential Security Issues in Implementing IaaS and PaaS Cloud Service Models. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, *3*(2)

Galiveeti, S., Tawalbeh, L. A., El-Latif, & Tawalbeh, M., A. A. A. (2021). Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. In *Artificial intelligence and blockchain for future cybersecurity applications*. Cham: Springer International Publishing.

Gomes, J. F., Iivari, M., Ahokangas, P., Isotalo, L., & Niemelä, R. (2023). Cybersecurity business models of IoT-mobile management services in futures digital hospitals.

Granger, J. (2023, November 20). *10 benefits of cloud-based access control systems*. ButterflyMX® - Official Site | Video Intercoms & Access Control.

Loginradius. *Pros and cons of using token-based authentication*. (n.d.).

Mohammed, C. M., & Zeebaree, S. R. (2021). Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. *International Journal of Science and Business*

Muxtoriddinov, M., Khudoykulov, Z., & Allanov, O. (2023, October). Multifactor Authentication (MFA) in Network Security: Strengthening Access Controls. In *Conference on Digital Innovation:" Modern Problems and Solutions"*.

Why is HTTP not secure? | HTTP vs. HTTPS | cloudflare. (n.d.).

Yang, S. J., Okutan, A., Werner, G., Su, S. H., Goel, A., & Cahill, N. D. (2021). Near Real-time Learning and Extraction of Attack Models from Intrusion Alerts.