Brian Sowers

27/11/2022

Data Center, IaaS and SaaS and Mobile

1. IaaS/SaaS/Data Center

a. **Application Service Provider**: (As SaaS) Patching and updating are both the responsibilities of the application provider. The SaaS provider is expected to incur costs and invest time to maintain the application infrastructure, whereas the customer does not. The provider will manage the applications, data, runtime, middleware, operating system, virtualization, servers, storage, and networking.

b. **Network Provider:** Required to promptly respond to and block reported attacks originating from their networks. Will monitor the network to detect any unusual indicators related to user behavior, attack signatures, or packet volume.

c. **Data/Storage Provider**: (As IaaS) An IaaS provider will manage storage among virtualization, servers, and networking while the customer will manage applications, data, runtime, middleware, and the operating system. By providing storage, the provider will conduct backups, routine checks, and allow for the flexibility for the customer to change storage options, all while maintaining the integrity and availability of the data hosted on the provider's cloud infrastructure.

d. **Customer:** When utilizing an IaaS, the customer has control over operating systems, storage, and deployed applications and the IaaS provider will be responsible for the networking components. Further, the provider owns the deployed applications and data and is responsible for

the security of the applications and data (Secure Business Operations Module 3, 23). When utilizing a SaaS provider, customers are provided access to the application but are still responsible for the security of the data. (Secure Business Operations Module 3, 24). It is up to the customer to determine what applications are sanctioned, tolerated, or unsanctioned and to have appropriate policies concerning each category. In both IaaS and SaaS, the customer does not have or need knowledge of the underlying cloud infrastructure on which theses services are provided.

2. Endpoint/Mobile/Enterprise

My security solution would consist of many different sub-solutions aggregating into one large solution. Firstly, for company personnel, I would mandate a cyber security awareness program for end users. I would require all users to authenticate to a VPN server that provides for encryption and uses only secure protocols such as HTTPS. I would require multi-factor authentication to logon to the company application. This could be a combination of a lengthy, secure password, a one time use code, or biometrics if possible. Software updates would be automatically pushed to mobile endpoints once the software updates has proved to be without bugs or vulnerabilities. Second, I would implement a zero-trust model to ensure authenticated users are who they say they really are. I would also categorize applications as sanctioned, tolerated, or unsanctioned and require that only sanctioned and tolerated applications be used. Third, I would use Next Generation Firewalls from Palo Alto to inspect all traffic, including applications, threats, and content. Additionally, I would use Palo Alto's Prisma to help secure SaaS applications.

Works Cited

"Secure Business Operations Module 3". https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_3.pdf. Accessed: 27 November 2022.