Cloud Security Presentation

MICHAEL LAMBINICIO

UNIVERSITY MARYLAND GLOBAL CAMPUS

CMIT 436

PROFESSOR JEFF BALDWIN

Shared Responsibility Model (SRM)

-The shared responsibility model identifies the roles and responsibilities between the cloud service providers and consumers. It is a foundational understanding based of the needs of the consumer and services the cloud provider may provide.

-There are multiple models that can be used such as Infrastructure as a service (IaaS), Platform as a service (Paas), and Software as a service (SaaS).

-Some areas that are covered would be:

- *Operating systems*
- *Application management*
- *Data and configurations*
- *Server maintenance*
- *Infrastructure*

SRM for IaaS

Infrastructure as a service is a cloud service model that physical hardware and virtualization are responsibility of the cloud service provider. The consumer will be responsible for everything else. Some examples are given below:

Cloud Service Provider:
-Securing the physical access to data center facilities
-Responsible for physical networking, storage resources and hypervisors that host your virtual machines

Consumer(You):
-Data security
-Application security
-Platform security
-Secure operating systems, firewall configurations and network compliance.

Security Services for IaaS

Cloud service providers who provide IaaS to its consumers should automatically prioritize the physical hardware and equipment as the main asset to monitor. Wherever the servers and data centers are located should have some surveillance and daily monitoring to prevent any intrusions and malfunctions or failures of their systems. This can be accomplished multiple ways:

-Having guards on duty to authorize entrances of actual employees or contractors if needed.

-Installing security cameras through the building and inside the server rooms.

-Having tokens or restricted access to the servers to prevent tampering with services provided to the consumer.

On the internal side, providers should have security monitoring, logging and auditing solutions to protect consumer data.

Disaster Recovery Using IaaS

In simple definition, disaster recovery is having the ability to recover any lost data from a disaster through certain procedures. The main method for this is redundancy. Having the data centers automatically backup the systems according to the provider’s policies will have a huge impact on a robust infrastructure. In turn, this would minimize negative results on incidents that may occur and prevent any interruptions to the consumers.

Pros/Cons of Using IaaS

Pros of IaaS

-Scalable on resources based on the consumers needs. You can change requirements as needed without fronting major expenses.

-Physical security measure invested such as surveillance, access restrictions, etc.

-Data encryption is vital to protect from any breaches and gains of their hardware will be unreadable without decryption keys.

Cons of IaaS

-Consumers have limited control over storage, network equipment and any other hardware resources.

-Possible misconfigurations on security settings due to human error

-Breach of user access and compromising identities can result in breaches and unauthorized changes, impacting consumers.

SRM for PaaS

Platform as a Service is designed to allow the customer the ability to be more involved on the platform's security. Some responsibilities are described below:

PaaS provider:
-Still responsible for the physical hardware and infrastructure
-Manages storage and compute systems
-software development and deployment

Customer(you):
-Operating system configurations
-Security policies
-Must encrypt the data
-All applications used on the platform will be your responsibility

Security Services for PaaS

PaaS providers do have some security solutions for consumers:

-To monitor network traffic compliance through policies, Cloud Access Security Broker, or CASB, is one solution.

-Another solution is Cloud Workload Protection Platform (CWPP) to secure workloads in the cloud environment if there are any malware detections in containers or instances.

-Lastly, you have CSPM (Cloud Security Posture Management) which identifies any misconfigurations and compliance risks.

Disaster Recovery Using PaaS

PaaS models have major advantages of disaster recovery. Big names such as Google or AWS are prime examples of this as they have a massive infrastructure built where they can backup data instantly to recover any failed hardware.

To add, it also has global distribution if the provider has multiple locations set up across the world. For instance, natural disasters can happen at any time and if one city in a country has a natural disaster where all hardware was lost, if properly setup, the backup could have been saved in a completely different country for the customer to recover.

Pros/Cons of Using PaaS

Pros:

-Spend less time on infrastructure and more time on improving your application development and creating good software.

-You are also able to be more involved in the security aspect of your service. You'll have ready-made tools and parts to build.

-PaaS handles all infrastructure regarding management, updates and maintenance of the systems, eliminating the needs for a separate staff for the IT department.

Cons:

-Could potentially have more ongoing costs. If your business thrives and scales higher than before, that will also cause a need for more resources from the provider as well.

-Your business may be relying on the providers products and technologies which could make it difficult to switch to an alternative if needed, called vendor lock-in.

-You will have less control to make any changes if there is some incompatibility issues with hardware to platform.

SRM for SaaS

SaaS, or Software as a service, is the final model in which the consumer only has to focus on utilizing software for their business. All infrastructure maintenance, networking, storage and security are all handled by the provider, examples listed below:

Provider:
-Physical security
-Infrastructure Maintenance
-Platform security

Consumer(you):
-User account management
-Access control
-Data backup
-Data encryption

Security Services for SaaS

Some of the services offered through the SaaS model are end-to-end encryption for both server/user and data storage. Policies for deleting data is a must have. This would prevent accidental deletion from team members who should not have the ability to do so. There is also VPN or VPC that provides an extra layer of security to your servers, allowing users to login anywhere with secure endpoints. Logs are also a big service as it helps monitor and identify incidents that happened and detect cyber attacks.

Disaster Recovery Using SaaS

Like the other disaster recovery methods mentioned for the other models, it's no different with SaaS. Having regular backup solutions to different servers in different locations will prevent any lost data for consumers. Below are also what needs to be identified:

-Having a communication plan with stakeholders

-Identify the roles and responsibilities of the staff in case of a disaster

-Give the maximum amount of data loss in time so you can figure out how often data should be backed up.

-Identify the maximum amount of time that SaaS applications can be down without causing interruption in business.

Pros/Cons of Using SaaS

Pros:

-Automatic updating is done by the provider so it reduces the workload on IT staff from the consumer.

-Very reliable in maintain uptime and investing in strict protocols, including disaster recoveries.

-High security as they have a dedicated security team that comply with industry standards to plan cybersecurity countermeasures against attacks, including encryption, routine updating and strict access controls.

Cons:

-Can be extremely difficult to switch vendors. Because it's all software base, transferring large amounts of data, it would take a long time and sometimes technologies may cause a hurdle if vendor equipment is incompatible.

-Have no control over versions of software if they are updated. The provider may update to new versions of software consumers use daily, regardless if they want it or not. This may lead to extra training and time to re-learn.

Conclusion

I hope this presentation was helpful to understanding the difference of the three models, IaaS, PaaS and SaaS. They all provide their own level of services based on the customers needs. The description of the pros and cons of each one should help clarify which model would best fit your organization. Ultimately, the cloud provider has a foundational piece in providing the hardware at a minimum to help jumpstart your cloud business.

References

-Timonera, K. (2023, December 19). *IaaS security: Top 8 issues & prevention best practices*. eSecurity Planet. https://www.esecurityplanet.com/cloud/iaas-security/#:~:text=Set%20Up%20Strict%20Authentication%20Protocols,detect%20and%20address%20security%20vulnerabilities.

-Tsai, P. (2020, November 19). *Infrastructure-as-a-service security responsibilities*. CloudTweaks. https://cloudtweaks.com/2020/11/infrastructure-as-a-service-security/

-Raza, M. (2023, April 7). *The shared responsibility model for security in the cloud (iaas, Paas & Saas)*. Splunk. https://www.splunk.com/en_us/blog/learn/shared-responsibility-model.html

-Smagulov, A. (2024, January 31). *PAAs security best practices*. anynines Blog. https://blog.anynines.com/posts/paas-security-best-practices/

-Finkel, B., & Schulte, G. (2016, March 7). *How paas can head off disaster*. InfoWorld. https://www.infoworld.com/article/2245326/how-paas-can-head-off-disaster.html

References

-Subramanian, V. (2024, October 24). *SAAS and The Shared Responsibility Model: A Guide to Protecting Your Data*. Backblaze Blog | Cloud Storage & Cloud Backup. https://www.backblaze.com/blog/saas-and-the-shared-responsibility-model-a-guide-to-protecting-your-data/

-Sherrill, A. (2025, January 28). *Paas Cloud Computing: Pros and Cons*. TenHats. https://tenhats.com/platform-as-a-service-cloud-computing/

-Yasar, K., Chai, W., & Casey, K. (2024, November 27). *What is SAAS (software as a service)? everything you need to know: Definition from TechTarget*. Search Cloud Computing. https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service

-*The Shared Responsibility Model: Securing Your Saas Data*. TekConcierge. (2024, May 28). https://tekconcierge.com/the-shared-responsibility-model-securing-your-saas-data/

-Cherian, S. (2024, October 8). *Saas Application Security: Effective Backup and disaster recovery | microminder cybersecurity | holistic cybersecurity services*. SaaS Application Security: Effective Backup and Disaster Recovery. https://www.micromindercs.com/blog/saas-application-security-backup-and-disaster-recovery

-Krishna, A. (2024, June 3). *What is saas security?*. Astra Security. https://www.getastra.com/blog/security-audit/saas-security-guide/