Cloud Security Group 4

CSIA 6000 Network Security

Team: Milada, Alex, John

**Team Case Project:** Consider how incident detection and response are more complicated in a cloud-based environment. What challenges does the cloud-based solution present to incident response teams, and what role they might have in incident detection?

**In your groups,** establish a collaborative document, to work together to address the question in this Team Case project.

**Instructions:** Use this document as a template for putting together your group’s Collaborative document for the Cloud Security Assignment. Select one of your group members to host the collaborative document, and ensure that it is shared with all group members, as well as the instructor.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Contribution - Milada**

**Software as a Service**

“Software as a Service is built on IaaS and PaaS. It serves business applications utilized by individuals or enterprises, and it can also be referred to as on-demand software. SaaS offers the most popular cloud applications to almost everyone that is online.” (John Vacca, Chapter 4, page 83). SaaS is built on top of IaaS and PaaS.

SaaS is the cloud architecture that provides the customer the most “turn-key” experience. SaaS is the least technical cloud experience that any organization can obtain, so it appeals to small and start-up businesses because it doesn’t require a suite of it professionals to deploy the infrastructure in a cloud. Some of the largest SaaS providers are Office 365, Salesforce, Box, Google Apps, and many more. SaaS is also considered the “customer acquisition” step of the cloud architecture, and once the SaaS provider reaches a certain size they often move into the “customer retention” aspect that involves providing Platform-as-a-Service cloud which allows customers more capabilities in terms of tailoring their computing resources.

Because SaaS is a turn-key experience, the cloud provider is responsible for the vast majority of the security aspects of the cloud. In addition to making sure the cloud architecture is secure as per the IaaS and PaaS requirements, the cloud provider is responsible to set up a comprehensive password protection and permissions system for the customer to use.

The customer’s largest responsibility and capability in terms of ensuring data security is to ensure the SLA signed with the cloud provider is comprehensive and covers the items necessary for the customer. “The SLAs will address data protection, business continuity and recovery, incident response, e-discovery, data retention, and removal.” (John Vacca, Chapter 4, page 95)

The customer should ensure the cloud provider collects and maintains comprehensive logs and that the logs are available for the customer to review on a regular basis.

Dealing with an incident that occurs in a SaaS-type environment is challenging for both the provider and the consumer. It is likely that the customer will be the first to detect that a data breach has occurred. Hopefully the SLA covers the notification procedures and the partial/complete shutdown or isolation procedures that the customer and the provider might want to undertake to minimize damage.

If the provider discovers the incident first – then hopefully the SLA covers the disclosure/non-disclosure points to ensure the customer is actually notified of the incident. It is possible the provider will want to “fix” the breach quietly and not notify the customer – that should be avoided.

In the SaaS situation, there will be two sets of incident response teams – one from the provider and one from the customer, and they will likely be focused on somewhat different aspects of the incident. The provider will be focused on restoring the service and containing the breach (and ensuring other customers are not affected), while the customer will be focused on containing the breach and continuing operations while the recovery can be completed.

References:

<http://www.zdnet.com/article/saas-in-2016-the-key-trends/>

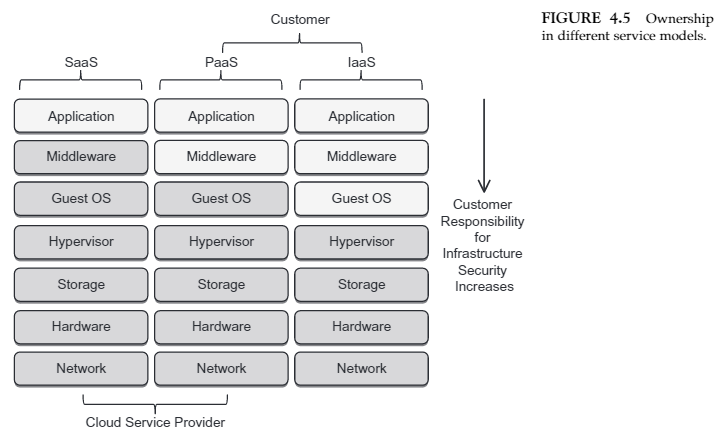
John R Vacca, Network and System Security, Chapter 4

--------------------------------------------------------------------------------------------------------------------------------

**Contribution - Alex**

**Platform as a Service: Google Cloud Platform**

PaaS or Platform as a Service is built on top of Infrastructure as a Service(IaaS). PaaS in the cloud is the deployment environment. PaaS deploys applications, also gives developers the ability to configure new applications. This provides all of the required facilities for supporting the complete life cycle of development of web applications which are available from the internet. Some PaaS providers that the book mentions are Google App Engine(GAE), Microsoft Azure, Engine Yard, and Collabnet. In the PaaS environment the customer administrator has minimal control and accountability. The securing of the PaaS falls under the purview of the provider, the customer must trust that the provider will give the customer the needed amount of privileges and control. On the PaaS is where you will implement your monitoring, such as Intrusion detection services(IDS’s) and new relic. The book states, “PaaS should provide encryption in the application, between client and application, in the database and proxies, as well as any application programming interfaces that deals with the hosted data.” Vulnerability test are also done on PaaS for their system. There is a needed network segregation for the the cloud can increase security, provider can limit traffic between subnets, and providers can also limit infrastructure control subnets. Firewalls can be used for network separation, which when used together with network controls the firewall becomes an extra defence or layer of support. For the access to network, servers, and application for the PaaS it is the responsibility of the service provider, but customers are responsible for the applications they deploy. There is a lot of data that we have to be concerned about securing such as laptops, file servers, servers, network devices, Databases and backups. Which puts a lot of concern out the window for a Info Sec Team, but we still have to be concerned about the security of what the cloud service provider is securing. Making sure that things are secure is needed for the whole scope of your system. We also have to be weary of a third party such as a cloud service taking advantages of our system. Best method for protecting data is applying encryption. The book lists four different recovery techniques, multisite, warm standby, basic backup and restore, and pilot light. A basic backup and restore is good for employees work computers, but for the whole enterprise or a website like ancestry multi site would work the best. Multisite is a backup method where data is synchronously with any major action, but this requires a lot of resource consumption to run.



Google Cloud Platform(GCP) is Google’s public cloud service. Google Cloud is a IaaS solution. The core services that are in GCP are Google Compute Engine, Google App Engine, Google Cloud Storage, and Google Container Engine. With regards to PaaS google app engine gives developers access to scalable hosting, and SDK(Software Developer Kit) to develop software. Google Compute Engine gives users the IaaS environment. Reading the review of google cloud platform from PCMag says that it performs well, great billing, handles large workloads, and great big data analytics in BigQuery. But two things with GCP comparing software options with Amazon Web Services(AWS); GCP doesn't match up, and as a company you need skilled system admins to implement GCP. everything I have read on Google Cloud Platform has been good, but each one of these reviews has directed or compared everything to AWS, which seems to be the industry standard.

Cited Works:

<https://www.youtube.com/watch?v=whkyRvugqlM>

<https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/>

John R Vacca, Network and System Security, Chapter 4

<https://www.youtube.com/watch?v=COhwhZjcjw0>

<http://www.pcmag.com/article2/0,2817,2496296,00.asp>

<http://searchcloudcomputing.techtarget.com/definition/Google-Cloud-Platform>

<http://cloudacademy.com/blog/google-cloud-vs-aws-a-comparison/>

--------------------------------------------------------------------------------------------------------------------------------

**Contribution - John**

**Infrastructure as a service Cloud solutions**

Infrastructure as a service (IaaS) refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. Below describes this in greater detail.

“In an IaaS model, a third-party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its users. IaaS providers also host users' applications and handle tasks including system maintenance, backup and resiliency planning.

IaaS platforms offer highly scalable resources that can be adjusted on-demand. This makes IaaS well-suited for workloads that are temporary, experimental or change unexpectedly.

Other characteristics of IaaS environments include the automation of administrative tasks, dynamic scaling, desktop virtualization and policy-based services.”

“IaaS customers pay on a per-use basis, typically by the hour, week or month. Some providers also charge customers based on the amount of virtual machine space they use. This pay-as-you-go model eliminates the capital expense of deploying in-house hardware and software. However, users should monitor their IaaS environments closely to avoid being charged for unauthorized services.”

Popular IaaS providers are as follows:

* Amazon AWS.
* Windows Azure.
* Google Compute Engine.
* Rackspace Open Cloud.
* IBM SmartCloud Enterprise.
* HP Enterprise Converged Infrastructure

<http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS>

As outlined in Module 4 and the powerpoints presented IaaS still presents a lot of possible vulnerabilities. No different than housing these systems locally in your data centers or offices, you need to take into account the listed aspects to these systems.

•Locking down cloud servers

•Ensuring best practices

•Implementation of safeguards

•Networking

•Operating systems

•Applications

•Vulnerability assessments – patching

•Configuration management

While looking into AWS as a IaaS it's really more of just realizing you are housing all your Infrastructure on their equipment. Their management system is really good to help you manage security features while setting this up, but you also can take measures just as you would with local equipment to get your Intrusion Detection Systems set up to monitor these Cloud based systems.

Currently we are taking logs from our AWS systems and building rules and alerts just as we would with any other system. We also have specific firewall rules and settings applied to ensure we’re secured behind that as well. You can also look into having a VPN to tunnel traffic back to homebase if you need. Or for web hosting from their cloud. Really it’s no different other than you use their scalability and infrastructure and pay by the systems and uptime you configure with them. Really it’s a great model and one we’re very happy to be testing with.