Desarrollo de software en sistemas distribuidos

Curso 2020

Desarrollo de software en sistemas distribuidos

Seguridad en Cloud Computing

Aspectos de seguridad

- Amenazas, desafíos y guias asociadas a la infraestructura de IT en la nube a nivel de:
  - La red
  - Los host
  - Las aplicaciones
- Generalmente se asocia la seguridad a IaaS, pero también debe considerarse a nivel de SaaS y PaaS ya que algunas son propias del modelo de servicio

Aspectos de seguridad

- Otra dimensión a considerar es respecto del modelo de despliegue: público, privado o híbrido.

- En clouds públicos el alcance de la infraestructura de seguridad se encuentra en manos del proveedor. En este sentido es importante tener en cuenta que nivel de seguridad otorga el proveedor y cuales aspectos son responsabilidad del cliente.

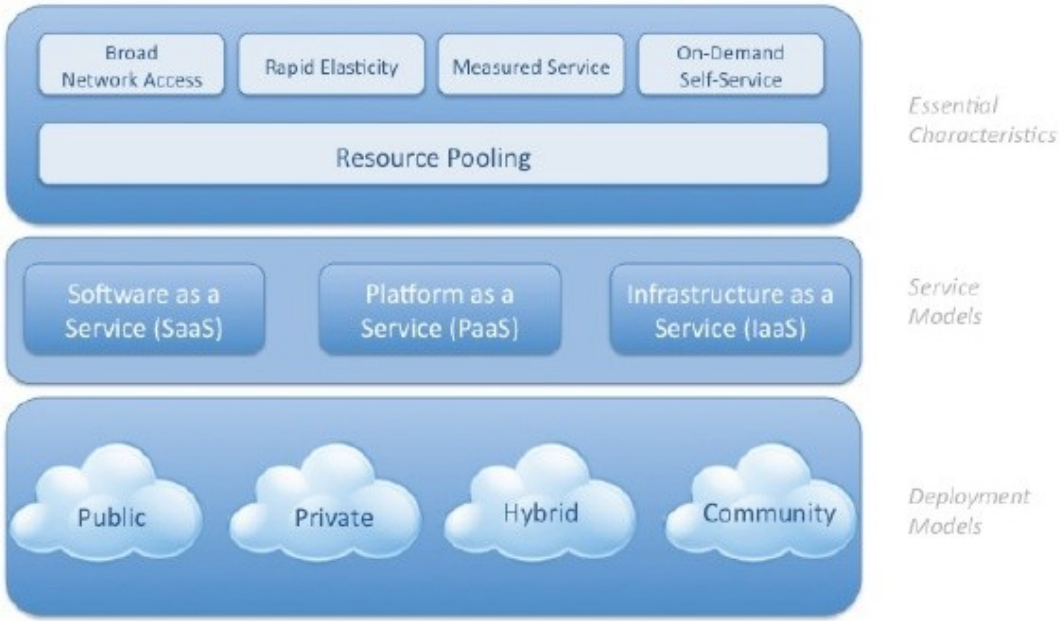
Modelo 5-3-4

El modelo de Cloud del NIST es conocido popularmente como 5-3-4

5 Características escenciales

3 Modelos de servicio

4 Modelos de despliegue



Infraestructura de seguridad a nivel de red

Es importante distinguir entre cloud privado y público

- **Cloud privado:** no hay consideraciones adicionales, ataques, vulnerabilidades o cambios específicos de la topología que la seguridad personal haya ya considerado
- **Cloud publico: las consideraciones de seguridad afectan la topología de la red debiendo revisarse 4 aspectos.**
  - **Asegurar la confidencialidad e integridad de los datos trasmitidos desde y hacia el proveedor de cloud**
  - **Asegurar un protocolo de control de acceso propio**
  - **Asegurar la disponibilidad de los recursos expuestos a Internet**
  - **Reemplazar el modelo establecido de zonas, niveles y dominios**

Infraestructura de seguridad a nivel de red

- **Asegurar la confidencialidad e integridad de los datos trasmitidos desde y hacia el proveedor de cloud**

- Muchos datos y recursos anteriormente confiados a una red privada ahora están expuestos a Internet y a una red compartida que pertenece a un proveedor externo.
- Un ejemplo de ello fue una falla en el algoritmo de firma digital quemostró la vulnerabilidad de AWS (Amazon Web Services) en 2008. Una consulta a SimpleDB sobre http mostro la vulnerabilidad del sistema. Si bien usar HTTPS en lugar de HTTP puede mitigar los riesgos de seguridad, permitir que los usuarios utilicen HTTP enfrento a los usuarios con un riesgo sobre la integridad de los datos.

Infraestructura de seguridad a nivel de red

- **Asegurar un protocolo de control de acceso propio**
  - **Los recursos están expuestos a Internet**
  - **Las organizaciones ven limitadas sus capacidades de revisión de logs.**
  - **Problemas del uso del mecanismo de reuso de direcciones IP y la desincronización de la reasignación y su actualización en los DNS.**
  - **Si bien hay productos para mitigar el riesgo de reuso de Ips, queda en manos del proveedor de cloud adoptarlos.**

Infraestructura de seguridad a nivel de red

- **Asegurar la disponibilidad de los recursos expuestos a Internet**
- **La exposición de recursos a Internet ha ido aumentando y se potencia en el cloud.**
  - **Secuestro de Prefijo**
  - **Ataque a DNS**
  - **Denegación de servicio**

Infraestructura de seguridad a nivel de red

- **Secuestro de Prefijo**
  - En inglés *prefix hijacking* de los BGP (Border Gateway Protocol, protocolo de ruteo entre dominio usado en Internet).
  - El secuestro de prefijo implica anunciar un espacio de direcciones de un sistema autónomo que pertenece a alguien más sin su permiso. Tales anuncios pueden ser errores de configuración o también por ataques. Ejemplo: youtube fuera de servicios por 4 horas en 2008

Infraestructura de seguridad a nivel de red

- **Ataques a DNS**
  - Es una práctica muy habitual y que se ve incrementada su complejidad en el cloud donde se reduce ampliamente la efectividad de la técnica de Split-horizont en DNS (provee distintas respuestas autorizadas a una misma consulta para asegurar la veracidad de los datos retornados por el DNS).

Infraestructura de seguridad a nivel de red

- Denegación de servicio
  - Es el intento de quitar de servicio un host logrado en general a través de la generación de requerimientos falsos con el objetivo de sobrecargar el sistema evitando que atienda los requerimientos legitimos.
  - Si bien esto es habitual aún sin una infraestructura cloud, en el caso de cloud se ve incrementado no solo sobre los recursos expuestos a Internet sino dentro mismo de su esquema interno, quitando de servicio los mismos AWS.
  - Asimismo, el uso de IaaS hace que la red interna del proveedor de cloud es un recurso compartido que cae en riesgo de ser denegado como servicio. En este caso es responsabilidad de cada cliente proteger sus instancias.

Infraestructura de seguridad a nivel de red

- **Reemplazar el modelo establecido de zonas, niveles y dominios**
  - **El modelo de aislamiento basado en zonas y niveles ya no es posible en cloud públicos tanto para IaaS como para PaaS.**
  - **Durante mucho tiempo la seguridad de la red se apoyo en la definición de zonas tales como intrenet vs extranet o entornos de producción vs entornos de desarrollo, de modo que separando el tráfico se garantizaba la seguridad y se basaba en la exclusión.**

Infraestructura de seguridad a nivel de red

- **Reemplazar el modelo establecido de zonas, niveles y dominios**
  - **SaaS cloud construida sobre IaaS o PaaS publicas requerirían un esquema de seguridad equivalente, sin embargo solo algunas SaaS publicas son construidas sobre IaaS privadas (ej Salesforce) y en ese caso siguen las mismas premisas de exclusión entre producción y desarrollo, pero hay muchas SaaS sobre IaaS publicas.**
  - **El modelo de zonas y niveles ha sido reemplazado en el cloud computing publico por "seguridad de grupos", "seguridad de dominios" y "virtualización", que poseen una separación lógica entre niveles pero son menos precisos y aportan menos protección que el esquema anterior.**

Infraestructura de seguridad a nivel de red

- **Reemplazar el modelo establecido de zonas, niveles y dominios**
  - **La funcionalidad de grupos de AWS permite a sus maquinas virtuales acceder unas a otras a través de firewall virtuales que filtran el tráfico basado en direcciones IP, tipos de paquetes (TCP,UDP o ICMP) y puertos o rango de puertos. Por ejemplo Google's App Engine provee un agrupamiento lógico de aplicaciones basado en nombres de dominio como *mytestapp.mydomain.com* y *myprodapp.prod.mydomain.com*. En entornos no-cloud esta separación se da físicamente en distintos host.**
  - **El modelo de separación de dominios en cloud ya no es físico sino lógico, más aún, la separación lógica de la red tampoco existe sino que los dominios lógicos pueden correr en el mismo host separados por los monitores de VM o hipervisores.**

Infraestructura de seguridad a nivel de red

- **Resumiendo …**

  ¿Como podemos mitigar los factores de riesgo? Primero notemos que los riesgos a nivel de red no son consecuencia del modelo de servicio, o sea del tipo de aaS sino que depende de si la organización usa un cloud publico, privado o hibrido, es decir del modelo de despliegue.

  - **Si la organización puede afrontar el costo de un cloud privado, los riesgos se verán decrementados.**
  - **La confidencialidad puede incrementarse utilizando encripción con implementaciones robustas de cifrado de datos en tránsito.**
  - **Los problemas de disponibilidad a nivel de red son más difíciles de mitigar, aun cuando su red privada no está montada sobre un proveedor de cloud externo, ya que igualmente conlleva riesgos a nivel de red. Un cloud publico no enfrenta problemas mayores que cualquier seguridad de red.**

Infraestructura de seguridad a nivel de host

- **Para revisar aspectos de seguridad a nivel de host, tanto del host en si, como de sus accesos, debemos considerar tanto el modelo de servicio (aaS) como el modelo de despliegue (publico o privado).**
- **Las nuevas amenazas a los host se relacionan con la virtualización (escapes de la VM, fallas en el sistema de configuración, amenzas por el débil control de acceso a los hipervisores).**
- **La naturaleza dinámica o elasticidad en el aprovisionamiento trae también consecuencias ya que la fugacidad de las instancias de VM no permite manejar las vulnerabilidades y actualizar rápidamente las correcciones o patches.**
- **El aprovechamiento del poder de miles de nodos con un sistema operativo homogéneo, hace q las amenazas se amplifiquen y se multipliquen más rápidamente. Esto da cuenta de los límites de confianza y responsabilidad que estamos delegando en los proveedores de cloud.**

Infraestructura de seguridad a nivel de host

- **Seguridad a nivel de host en SaaS y PaaS**
  - **En el contexto de SaaS y PaaS la seguridad de host es opaca a los clientes y la seguridad es total responsabilidad del proveedor. Generalmente el proveedor debe ofrecer garantía de NDA (Non-Disclouser Agreement o acuerdo de no divulgación) y asegurar controles preventivos y detectivos apropiados q se ajuste a la**
  - **SysTrust**
  - **ISO 27002.**

Infraestructura de seguridad a nivel de host

- **Seguridad a nivel de host en IaaS**

  - Seguridad del software de virtualización.

Los proveedores cloud gestionan el software de virtualización quese aloja sobre el hardware, los clientes no tienen visibilidad sobre ellos ni acceden a ese software. El hardware y SO de virtualización permiten compartir recursos de hardware a través de multiples VMs si interferir unas con otras y cada uno ejecuta sus aplicaciones al mismo tiempo en una única computadora.

La integridad y disponibilidad del hipervisor son fundamentales y son la clave para garantizar la integridad y disponibilidad del cloud publico construido sobre un ambiente virtualizado. Un hipervisor vulnerable podría exponer a todos los usuarios de intervenciones maliciosas.

Dado que el software de virtualización en cloud públicos son propietarios y de código cerrado (si bien algunos emplean software open source como Xen) el código fuente usado por el proveedor no está disponible para ser examinado.

Infraestructura de seguridad a nivel de host

- **Seguridad a nivel de host en IaaS.**

- Seguridad del servidor virtual.

Los clientes de IaaS tienen acceso completo a las VM que son alojadas y aisladas unas de otras por la tecnología de hipervisores, por lo tanto los clientes son responsables de la seguridad y su gestión de la VM.

Un IaaS publico como EC2 de Amazon, ofrece una API basada en WS para la gestión de aprovisionamiento, desmantelamiento y replicación de servidores virtuales. Estas funciones se orquestan ofreciendo un ciclo de vida dinamico q puede ser complejo si los servidores virtuales no están automatizados con procedimientos adecuados. Desde la perspectiva de la superficie, el servidor virtual (Windows, Solaris o Linux) puede ser accesible a cualquiera desde Internet. Por ello los proveedores de cloud bloquean todos los puertos de acceso y recomiendan usar el puerto 22 (Secure Shell) para administrar las instancias de los servidores virtuales.

Infraestructura de seguridad a nivel de host

- **Seguridad a nivel de host en IaaS. Seguridad del servidor virtual.**
  - **Algunas amenazas de seguridad en IaaS publico incluyen:**
    - **Robo de claves usadas para acceder a la administración**
    - **Ataques a servicios de escucha vulnerables sobre puertos estándar (como FTP)**
    - **Secuestro de cuentas no securizadas adecuadamente (password débiles)**
    - **Ataques al sistema no securizados por firewalls**
    - **Despliegue de troyanos embebidos en el software de la VM o en su imagen**

Infraestructura de seguridad a nivel de aplicación

- **La seguridad en aplicaciones y software es un punto critico en el cual las empresas que producen este software invierten parte de su tiempo. Desarrollar e implementar aplicaciones en el cloud requiere revisar las practicas habituales. El espectro de seguridad va desde simples aplicaciones stand-alone a sofisticados sistemas de e-commerce, pasando por las aplicaciones web como CMS, wikis, foros e incluso redes sociales.**

Infraestructura de seguridad a nivel de aplicación

- **Según SANS hasta 2007 eran pocos los ataques a sitios web vulnerables, pero luego, el incremento de cross-site scripting (XSS tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar (ej: VBScript), evitando medidas de control) y otros ataques demostraron q la programación web usada para penetrar en las organizaciones.**
- **Por eso nos centramos en la discusión de la seguridad en aplicaciones web en el cloud accedidas por browsers desde cualquier computadora conectada a Internet.**

https://www.sans.org/security-resources/posters/cloud-security-devsecops-practices/200/download

Infraestructura de seguridad a nivel de aplicación

- **Denegación de sostenibilidad**
  - **Se debe tomar conciencia a nivel de aplicación de los ataques de denegación de sostenibilidad inspeccionando un alto volumen de recargas de páginas, los requerimientos de los WS por HTTP o HTTPS. Dado q este tráfico malicioso viene incluido en el trafico valido es de difícil detección y además de alterar el servicio de cloud, también incrementa las tarifas de pago x uso de la red.**
  - **Por su parte la elección de cloud por parte de pequeñas y medianas empresas q no pueden asumir los costos de inversión, mantienen las barreras bajas de seguridad.**

Infraestructura de seguridad a nivel de aplicación

- **Seguridad de usuarios finales**

Las medidas de seguridad q adopten los usuarios finales como uso de antivirus, anti-malware, firewalls personales y parches de seguridad, contribuyen a mantener la seguridad y una navegación segura q impacta en la seguridad de las aplicaciones siendo q los browsers se han convertido en sistemas operativos ubicuos. Más aun, para asegurar una seguridad punta a punta en el cloud, es fundamental mantener una buena higiene de los navegadores.

Infraestructura de seguridad a nivel de aplicación

Seguridad de aplicaciones SaaS

- En un entorno SaaS el proveedor del servicio maneja la suite entera de la aplicación que se dispone a los usuarios, de modo q la seguridad también es su responsabilidad.
- El cliente suele ser responsable de la seguridad operacional incluyendo la gestión de usuarios y accesos que otorga el proveedor.
- Se suele realizar testing de penetración y poner atención extra a las características de autenticación y control de acceso.

Infraestructura de seguridad a nivel de aplicación

- **Seguridad de aplicaciones PaaS**

El uso de PaaS es aun muy incipiente y la recomendación es que las organizaciones que lo vayan a incorporar usen las mismas consideraciones que al adquirir un paquete de desarrollo de software tradicional.

Conclusión

Hemos revisado la seguridad en el cloud desde el aspecto de la red, de los host y de las aplicaciones.

A nivel de red, si bien es un desafío para cloud computing, ninguno de ellos es intrínseco del cloud en si mismo. Todos los aspectos de seguridad en la red están exacerbados x el cloud, pero no son causados por el.

En cuanto a la seguridad de host, se requiere incrementar la seguridad perimetral y dar entornos de virtualización seguros. Otra vez los aspectos de seguridad se ven exacerbados pero nos son causados por el cloud.

A nivel de aplicación se sugiere utlizar buenas prácticas de seguridad en el desarrollo y tomar las responsabilidades pertinentes de cada uno de los actores.

Fuente

Mather, Kumaraswamy, Latif. “Cloud Security and Privacy. An Enterprise Perspective on Risks and Compliance”. Editorial O ´Reilly. 2009. Cap. 3