Seguridad en la Nube

Contenido

1. Introduccion al Cloud Computing
   1.1. ¿Que es la nube?
   1.2. Tipos de nube y sus características

2. Implicaciones de la Seguridad en la nube
   2.1. Amenazas en la nube
   2.2. Buenas prácticas para evitar las amenazas en la nube

3. Caso particular
   3.1. Seguridad de Dropbox Business
   3.2. Caso de fallo de la seguridad en Dropbox Business

4. Conclusiones

Introduccion al Cloud Computing

¿Que es la nube?

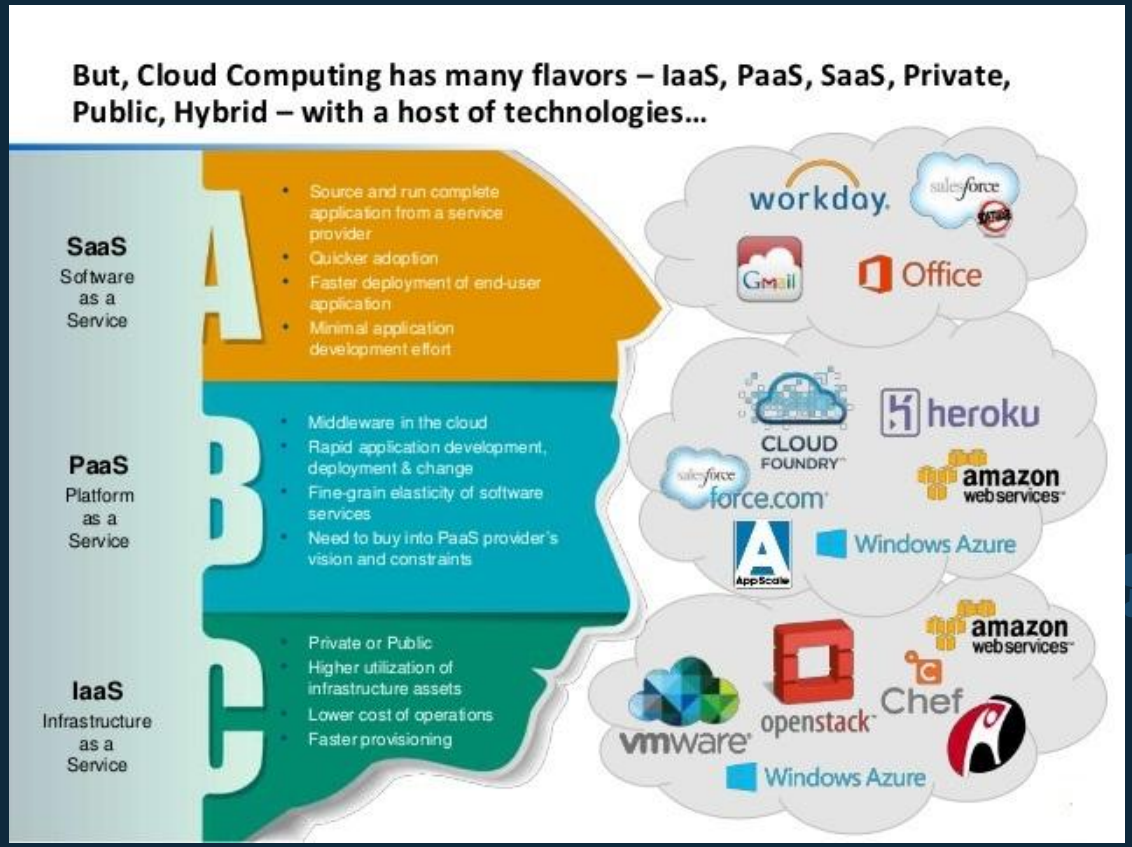
- Año 2006 aparición del término nube
- Cloud Computing conjunto de servicios informaticos ofrecidos a traves de internet
- Concepto desde 1970 “recursos de tiempo compartido”
- Definición oficial de la NIST

“Cloud computing’ es un modelo que permite el acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provisionados y liberados con un mınimo esfuerzo de gestión o de interacción con el proveedor de servicios.”

Tipos de nube y sus características

- Características esenciales
  - Autoservicio por demanda
  - Acceso amplio desde la red
  - Conjunto de recursos
  - Elasticidad
  - Servicio medido
- Modelos de servicio
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS
  - Infrastructure as a Service (IaaS)
- modelos de despliegue
  - nube privada
  - nube pública
  - nube híbrida

Modelos de Servicios de la nube



Implicaciones de la Seguridad en la nube

Amenazas en la nube

- Facilidad de uso
- Transmisión de datos vulnerable
- APIs inseguras
- Tecnología compartida
- Amenaza interna
- Pérdida de datos
- Brecha de datos
- Secuestro de cuenta/servicio
- Perfil de riesgo desconocido
- Denegación de servicio (DoS)
- Falta de comprensión

Buenas prácticas para evitar las amenazas en la nube

- Proveedores
  - Seguridad del data center
  - Seguridad del sistema operativo de la maquina Host
  - El Control del Hypervisor
  - Seguridad de la red
- Consumidores
  - Cortafuegos Hardware
  - Cortafuegos Software
  - Parches y copias de seguridad
  - Contraseñas
  - Seguridad de la maquina virtual

Caso particular Dropbox Business

- Arquitectura de Dropbox Business
  - Servicio de aplicación y cifrado
  - Servicio de almacenamiento
  - Servicio de metadatos
  - Servicio de notificaciones
- Otros puntos de la seguridad de la arquitectura
  - Centros de datos
  - Cifrado
  - Comprobación de certificado
  - Confidencialidad directa total
  - Administración de claves

Arquitectura de seguridad de Dropbox Business

Caso particular Dropbox Business

- Control y visibilidad
  - Integración de servicios de directorio activo
  - Inicio de sesión único (SSO)
  - Verificación en dos pasos
  - Dos cuentas Dropbox (personal y trabajo)
  - Permisos de carpetas y archivos compartidos
  - Recuperación e historial de versiones
  - Desvincular dispositivos
  - Borrado remoto
  - Transferencia de cuenta
  - Registro de actividades

Caso particular Dropbox Business

- Seguridad de la información
  - Políticas de seguridad
  - Control de acceso
  - Seguridad de la red
  - Administración de cambios

Conclusiones

Ya sabemos qué es la nube y cuáles son, en general, las ventajas y los riesgos de usar los servicios que ofrece. Todos los métodos que hemos visto para implementar la seguridad deberían hacer la nube un entorno lo suficientemente seguro para sobrepasar cualquier tipo de incidente, aunque el error humano puede provocar brechas en la seguridad. Remarcamos que la seguridad en la nube debería ser una relación entre los proveedores y los consumidores, donde cada uno tiene la responsabilidad de asegurar su entorno. Teniendo esto en cuenta, los servicios ofrecidos por la nube deberían ser mucho más flexibles y seguros que los métodos tradicionales. Pero como cada proveedor es diferente, tenemos que evaluar los áreas de seguridad que ofrecen antes de migrar a la nube.