**Seguridad de red en la nube**

En los últimos años, muchas organizaciones están utilizando servicios de red en la nube. Así que, además de proteger las redes locales, un analista de seguridad tendrá que proteger las redes en la nube. En un vídeo anterior, aprendió que una red en la nube es una colección de servidores u ordenadores que almacenan recursos y datos en un centro de datos remoto al que se puede acceder a través de Internet. Pueden alojar datos y aplicaciones de la empresa utilizando la computación en la nube para proporcionar almacenamiento bajo demanda, potencia de procesamiento y análisis de datos. Al igual que los servidores web normales, los servidores en la nube también requieren un mantenimiento adecuado realizado a través de varios procedimientos de endurecimiento de la seguridad. Aunque los servidores en la nube están alojados por un proveedor de servicios en la nube, estos proveedores no pueden evitar intrusiones en la nube, especialmente intrusiones de actores maliciosos, tanto internos como externos a una organización.

Una distinción entre el endurecimiento de red en la nube y el endurecimiento de red tradicional es el uso de una imagen de línea base del servidor para todas las instancias del servidor almacenadas en la nube. Esto permite comparar los datos de los servidores en la nube con la imagen de línea base para asegurarse de que no se han producido cambios no verificados. Un cambio no verificado podría proceder de una intrusión en la red en la nube. De forma similar al endurecimiento del SO, los datos y las aplicaciones de una red en la nube se mantienen separados en función de su categoría de servicio. Por ejemplo, las aplicaciones más antiguas deben mantenerse separadas de las más recientes, y el software que se ocupa de funciones internas debe mantenerse separado de las aplicaciones front-end que ven los usuarios.

Aunque el proveedor de servicios en la nube tiene una responsabilidad compartida con la organización que utiliza sus servicios, sigue habiendo medidas de seguridad que debe tomar la organización para asegurarse de que su red en la nube es segura. Al igual que las redes tradicionales, las operaciones en la nube deben estar protegidas.

**Asegure la nube**

Anteriormente en este curso, se le presentó la [computación en la nube](https://www.coursera.org/learn/networks-and-network-security/lecture/BGlnq/cloud-networks). La **computación en** la nube es un Modelo que permite un acceso cómodo y bajo demanda a través de la red a un conjunto compartido de recursos informáticos configurables. Estos Recursos pueden configurarse y liberarse con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios.

Al igual que cualquier otra infraestructura de TI, una infraestructura de Nube necesita estar protegida. Esta lectura abordará algunas consideraciones de seguridad principales que son exclusivas de la nube y le presentará el Modelo de responsabilidad compartida utilizado para la seguridad en la nube. Muchas organizaciones que utilizan recursos e infraestructuras en la nube expresan su preocupación por la privacidad de sus datos y recursos. Esta preocupación se aborda mediante la criptografía y otras medidas de Seguridad adicionales, que se tratarán más adelante en este curso.

**Consideraciones sobre la Seguridad de la nube**

Muchas organizaciones optan por utilizar los servicios en nube debido a la facilidad de implementación, la Velocidad de implementación, el ahorro de costes y la escalabilidad de estas opciones. La computación en la nube presenta retos de Seguridad Únicos que los analistas de Ciberseguridad deben conocer.

**Gestión del acceso a la identidad**

La gestión del acceso a la identidad**(IAM)** es un conjunto de procesos y tecnologías que ayuda a las organizaciones a gestionar las identidades digitales en su entorno. Este servicio también autoriza la forma en que los usuarios pueden utilizar los diferentes Recursos de la Nube. Un problema común al que se enfrentan las organizaciones cuando utilizan la Nube es la configuración poco precisa de los roles de usuario en la Nube. Un rol de usuario mal configurado aumenta el riesgo al permitir que usuarios no autorizados tengan acceso a operaciones críticas de la nube.

**Configuración**

El número de servicios en nube disponibles añade complejidad a la red. Cada servicio debe configurarse cuidadosamente para cumplir los requisitos de Seguridad y Cumplimiento normativo. Esto supone un reto particular cuando las organizaciones realizan una migración inicial a la nube. Cuando se produce este cambio en su red, deben asegurarse de que cada proceso trasladado a la nube se ha configurado correctamente. Si los administradores de red y los arquitectos no son meticulosos a la hora de configurar correctamente los servicios en la nube de la organización, podrían dejar la red abierta a un compromiso. Los servicios en la nube mal configurados son una fuente común de problemas de Seguridad de la nube.

**Superficie de ataque**

Los proveedores de servicios en la nube (CSP) ofrecen numerosas aplicaciones y servicios a las organizaciones a bajo coste.

Cada servicio o aplicación en una red conlleva su propio conjunto de riesgos y vulnerabilidades y aumenta la superficie de ataque global de una organización. Una mayor superficie de ataque debe compensarse con mayores medidas de Seguridad.

Las redes en la nube que utilizan muchos servicios introducen muchos puntos de entrada en la red de una organización. Sin embargo, si la red se diseña correctamente, la utilización de varios servicios no introduce más puntos de entrada en el diseño de la red de una organización. Estos puntos de entrada pueden utilizarse para introducir software malicioso en la red y plantear otras vulnerabilidades de seguridad. Es importante tener en cuenta que los CSP a menudo se decantan por opciones más seguras y han sido sometidos a un mayor escrutinio que una red tradicional in situ.

**Ataques de día cero**

Los ataques de Día cero son una importante consideración de seguridad para las organizaciones que utilizan soluciones de red en la nube o tradicionales en las instalaciones. Un ataque de **Día** cero es un exploit desconocido hasta ahora. Es más probable que los CSP sepan de un ataque de Día cero antes que una organización de TI tradicional. Los CSP disponen de métodos para parchear los hipervisores y migrar las cargas de trabajo a otras máquinas virtuales. Estos métodos garantizan que los clientes no se vean impactados por el ataque. También hay varias herramientas disponibles para parchear a nivel del sistema operativo que las organizaciones pueden utilizar.

**Visibilidad y Seguimiento**

Los administradores de red tienen acceso a todos los paquetes de datos que cruzan la red, tanto con redes locales como en la nube. Pueden husmear e inspeccionar los paquetes de datos para conocer el rendimiento de la red o comprobar posibles amenazas y ataques.

Este tipo de visibilidad también se ofrece en la nube a través de registros de flujos y herramientas, como la duplicación de paquetes. Los CSP asumen la responsabilidad de la Seguridad en la Nube, pero no permiten que las organizaciones que utilizan su infraestructura monitoricen el Tráfico en los servidores del CSP. Muchos CSP ofrecen fuertes medidas de Seguridad para proteger su infraestructura. Aun así, esta situación puede ser preocupante para las organizaciones que están acostumbradas a tener pleno acceso a su red y a sus operaciones. Los CSP pagan auditorías de terceros para verificar lo segura que es una red en la nube e identificar posibles vulnerabilidades. Las auditorías pueden ayudar a las organizaciones a identificar si alguna vulnerabilidad procede de la infraestructura local y si hay algún fallo de cumplimiento por parte de su CSP.

**Las cosas cambian rápido en la Nube**

Los CSP son grandes organizaciones que trabajan duro para mantenerse al día de los avances tecnológicos. Para las organizaciones que están acostumbradas a tener el control de cualquier ajuste que se realice en su red, esto puede suponer un reto potencial para mantenerse al día. Las actualizaciones de los servicios en la Nube pueden afectar a las consideraciones de Seguridad de las organizaciones que los utilizan. Por ejemplo, puede ser necesario cambiar las configuraciones de conexión en función de las actualizaciones del CSP.

Las organizaciones que utilizan CSP suelen tener que actualizar sus procesos informáticos. Es posible que las organizaciones continúen siguiendo las mejores prácticas establecidas para cambios, configuraciones y otras consideraciones de Seguridad. Sin embargo, es posible que una organización tenga que adoptar un enfoque diferente de forma que se alinee con los cambios realizados por el CSP.

Las redes en la nube ofrecen varias opciones que pueden parecer atractivas para una pequeña empresa, opciones que nunca podrían permitirse construir en sus propias instalaciones. Sin embargo, es importante tener en cuenta que cada servicio añade complejidad al perfil de seguridad de la organización, y que necesitarán personal de seguridad para supervisar todos los servicios en nube.

**Modelo de responsabilidad compartida**

Un principio de Seguridad de la nube comúnmente aceptado es el Modelo de responsabilidad compartida. El **Modelo de responsabilidad** compartida establece que el CSP debe asumir la responsabilidad de la seguridad que afecta a la infraestructura de la nube, incluidos los centros de datos físicos, los hipervisores y los sistemas operativos del host. La empresa que utiliza el servicio en nube es responsable de los recursos y procesos que almacena u opera en la nube.

El Modelo de Responsabilidad compartida garantiza que tanto el CSP como los usuarios están de acuerdo sobre dónde empieza y termina su responsabilidad en materia de Seguridad. Se produce un problema cuando las organizaciones asumen que el CSP se ocupa de una Seguridad de la que no se han responsabilizado. Un ejemplo de ello son las aplicaciones y configuraciones en la Nube. El CSP asume la responsabilidad de asegurar la nube, pero es responsabilidad de la organización asegurarse de que los servicios están configurados correctamente de acuerdo con los requisitos de seguridad de su organización.

**Puntos clave**

Es esencial conocer las consideraciones de seguridad que son exclusivas de la nube y comprender el Modelo de responsabilidad compartida para la seguridad de la nube. Las organizaciones son responsables de configurar correctamente y mantener las mejores prácticas de seguridad para sus servicios en la nube. El Modelo de Responsabilidad Compartida garantiza que tanto el CSP como los usuarios estén de acuerdo sobre de qué es responsable la organización y de qué es responsable el CSP a la hora de asegurar la infraestructura de la nube.

**Criptografía y Seguridad de la nube**

Anteriormente en este curso, se le presentaron los conceptos del Modelo de responsabilidad compartida y la Gestión de identidad y acceso (IAM). Al igual que las redes locales, las redes en la nube también deben protegerse mediante una combinación de prácticas de refuerzo de la seguridad y criptografía.

Esta lectura abordará las prácticas comunes de endurecimiento de la seguridad de la nube, lo que hay que tener en cuenta a la hora de implementar medidas de seguridad en la nube y los fundamentos de la criptografía. Dado que las infraestructuras en la nube son cada vez más comunes, es importante comprender cómo funcionan las redes en la nube y cómo protegerlas.

**Endurecimiento de seguridad de la nube**

Existen varias técnicas y herramientas que pueden utilizarse para proteger la infraestructura y los recursos de las redes en nube. Algunas técnicas comunes de endurecimiento de la Seguridad de la nube incluyen la incorporación de IAM, hipervisores, líneas de base, criptografía y borrado criptográfico.

**Gestión del acceso a la identidad (IAM)**

La gestión del acceso a la identidad (**IAM** ) es un conjunto de procesos y tecnologías que ayuda a las organizaciones a gestionar las identidades digitales en su entorno. Este servicio también autoriza la forma en que los usuarios pueden aprovechar los diferentes Recursos de la Nube.

**Hipervisores**

Un **hipervisor** abstrae el hardware del host del entorno del software operativo. Existen dos tipos de hipervisores. Los hipervisores de tipo uno se ejecuta en el hardware de la computadora anfitriona. Un ejemplo de hipervisor de tipo uno es ESXi de VMware®. Los hipervisores de tipo dos funcionan en el software de la computadora host. Un ejemplo de hipervisor de tipo dos es VirtualBox. Los proveedores de servicios en la nube (CSP) suelen utilizar hipervisores de tipo uno. Los CSP son responsables de gestionar el hipervisor y otros componentes de virtualización. El CSP se asegura de que los recursos y los entornos de la nube estén disponibles y proporciona parches y actualizaciones con regularidad. Las vulnerabilidades en los hipervisores o los errores de configuración pueden provocar escapes de máquinas virtuales (VM escapes). Un escape de VM es un exploit en el que un actor malicioso obtiene acceso al hipervisor principal, potencialmente a la computadora host y a otras VM. Como cliente de un CSP, rara vez tratará con hipervisores directamente.

**Línea de base**

La línea de base para las redes y operaciones en la nube cubre cómo se configura y establece el entorno de la nube. Una línea de base es un punto de referencia fijo. Este punto de referencia puede utilizarse para comparar los cambios realizados en un entorno de nube. Una configuración y puesta a punto adecuadas pueden mejorar en gran medida la seguridad y el rendimiento de un entorno de nube. Algunos ejemplos de establecimiento de una línea de base en un entorno de nube son: restringir el acceso al portal de administración del entorno de nube, habilitar la gestión de contraseñas, habilitar la encriptación de archivos y habilitar los servicios de detección de amenazas para las bases de datos SQL.

**Criptografía en la nube**

La criptografía puede aplicarse para asegurar los Datos que se procesan y almacenan en un entorno de nube. La criptografía utiliza sistemas de encriptación y de gestión segura de claves para proporcionar integridad y confidencialidad a los datos. La encriptación criptográfica es una de las formas clave de asegurar los Datos sensibles y la Información en la nube.

La encriptación es el proceso de convertir la información en texto cifrado, que no es legible para nadie sin la clave de encriptación. La encriptación se originó principalmente a partir de la codificación manual de mensajes e Información utilizando un algoritmo para convertir cualquier letra o número dado en un nuevo valor. La encriptación moderna se basa en el secreto de una clave, más que en el secreto de un algoritmo. La criptografía es una herramienta importante que ayuda a proteger las redes en la nube y los Datos en reposo para evitar accesos no autorizados. Aprenderá más sobre criptografía en profundidad en un próximo curso.

**Borrado criptográfico**

El borrado criptográfico es un método para borrar la clave de encriptación de los Datos encriptados. Cuando se destruyen Datos en la Nube, los métodos más tradicionales de destrucción de Datos no son tan eficaces. El borrado criptográfico es una técnica más reciente en la que se destruyen las claves criptográficas utilizadas para la desencriptación de los Datos. Esto hace que los Datos sean indescifrables e impide que nadie pueda desencriptarlos. Al cripto-triturar, todas las copias de la clave deben ser destruidas para que nadie tenga la oportunidad de acceder a los Datos en el futuro.

**Gestión de claves**

La encriptación moderna se basa en mantener seguras las claves de encriptación. A continuación se indican las medidas que puede tomar para proteger aún más sus Datos cuando utilice aplicaciones en la nube:

* Módulo de plataforma de confianza (TPM). El TPM es un chip de computadora que puede almacenar de forma segura contraseñas, certificados y claves de encriptación.
* Módulo de seguridad de hardware de la nube (CloudHSM). El CloudHSM es un dispositivo informático que proporciona almacenamiento seguro para claves criptográficas y procesa operaciones criptográficas, como la encriptación y la desencriptación.

Las organizaciones y los clientes no tienen acceso al proveedor de servicios en la nube (CSP) directamente, pero pueden solicitar auditorías e informes de seguridad poniéndose en contacto con el CSP. Los clientes no suelen tener acceso a las claves de encriptación específicas que los CSP utilizan para encriptar los Datos de los clientes. Sin embargo, casi todos los CSP permiten a los clientes proporcionar sus propias claves de encriptación, dependiendo del servicio al que acceda el cliente. A su vez, el cliente es responsable de sus claves de encriptación y de garantizar la confidencialidad de estas. El CSP está limitado en cuanto a cómo puede ayudar al cliente si las claves de éste se ven comprometidas o destruidas. Una ventaja clave del Modelo de responsabilidad compartida es que el cliente no es totalmente responsable del mantenimiento de la infraestructura criptográfica. Las organizaciones pueden evaluar y supervisar el riesgo que implica permitir que el CSP gestione la infraestructura revisando la auditoría y los Controles de seguridad de un CSP. Para los contratistas federales, FEDRAMP proporciona una Lista de CSP verificados.

**Puntos clave**

Endurecimiento de seguridad de la nube es un componente crítico por considerar al evaluar la seguridad de varios entornos de nube pública y mejorar la seguridad dentro de su organización. La gestión del acceso a la identidad (IAM), la correcta configuración de una línea de base para el entorno de la nube, la seguridad de los hipervisores, la criptografía y el borrado criptográfico son métodos que se pueden utilizar para aumentar la seguridad de la infraestructura de la nube.