Q1 Labs®
Total Security Intelligence

# DEFINICIÓN DE MEJORES PRÁCTICAS

## para la Seguridad de TI dentro de un Mundo en la Nube

### - Fases para Construir una Estrategia de Seguridad para la Nube

En los últimos años, se ha hablado mucho del aumento de la computación en nube. El concepto de que la tecnología de la información se puede incluir en un modelo de utilidad altamente escalable genera exaltación tanto en los clientes como en los proveedores. No obstante, todavía hay una gran preocupación con respecto a la seguridad.

Chris Poulin
Jefe de Seguridad
Q1 Labs

En los últimos años, se ha hablado mucho del aumento de la computación en nube. El concepto de que la tecnología de la información se puede incluir en un modelo de utilidad altamente escalable genera exaltación tanto en los clientes como en los proveedores. No obstante, todavía hay una gran preocupación con respecto a la seguridad.

**Por ejemplo, en la Octava Encuesta Anual sobre Seguridad Global de la Información, que realizaron las revista CSO y CIO, junto con PriceWaterhouseCooper, se descubrió que el 62 por ciento de los encuestados no confiaban en su capacidad para asegurar todos los datos en la nube.** Incluso el 49% de los que ya habían implementado la computación en nube, más de un tercio (39 %), tiene serias dudas con respecto a la seguridad. La encuesta, realizada por más de 12.000 ejecutivos de negocios y tecnología en todo el mundo, es uno de los muchos estudios similares que se realizan y todos indican las mismas inquietudes de seguridad que existen sobre la computación en nube.

## Nueva tecnología, seguridad a la moda antigua

El riesgo más grande que presenta la estrategia en nube es la pérdida de control. Pero el grado en que esto es un factor depende de si usted es el cliente o proveedor de la nube. En muchos casos, pueden ser las dos opciones, ya que la virtualización estuvo en los 3 principales de Gartner durante el 2010, y se espera que tenga un impacto estratégico en el 2011 y que ayude a pagar los proyectos de TI.

Si usted es consumidor, puede darle al proveedor un voto de confianza. Demás está decir que deberá investigar, asegurarse de que el proveedor haya implementado los controles de seguridad y privacidad apropiados, que sus datos cuenten con la protección correcta, y tener un contrato mediante el cual se responsabilice al proveedor. Se habla mucho de la infraestructura de la seguridad en la que invierten los proveedores de nube, pero se garantiza el dicho "confíe, pero corrobórelo". Los proveedores públicos de nubes lo analizan desde el punto de vista del marco de seguridad tradicional: ofrecer protección en la nube con firewalls, IDS/IPS, soluciones de seguridad del host y otras soluciones de punto. Para que quede claro, estos son controles de seguridad, pero la seguridad en profundidad no llega tan lejos en un entorno de nube; no podemos depender solamente de los mecanismos de protección, independientemente de la cantidad de capas.

Si nada más confirma la teoría, la computación en nube ha dejado un espacio abierto en el perímetro de la red y, ahora, hay que enfocarse en la visibilidad y la inteligencia de seguridad. La seguridad de la información en la nube debe proteger los datos y la infraestructura. Para esto, es necesario comprender los datos y el valor que estos tienen en el negocio del cliente. Cloud 1.0 no tiene en cuenta esto, ya que las fuerzas del mercado demandan un rápido desarrollo y una implementación temprana. Los proveedores de nube no han definido un modelo de seguridad en nube totalmente integral y desarrollado.

Una de las principales preocupaciones es la ubicación de los datos del cliente, lo cual genera muchas preguntas interesantes. Por ejemplo, ¿cómo reaccionan los proveedores de nubes cuando un mal cliente suscita una investigación por delito? ¿Existe la posibilidad de que los datos caigan en manos de un delincuente y estén sujetos a escrutinio por orden judicial?. ¿Qué sucede si un cliente tiene un servicio que aumenta el riesgo de atraer amenazas avanzadas persistentes (APT) o un ataque del sistema operativo de disco (DoS)? ¿De qué manera los proveedores de nubes entienden el contexto de los datos del cliente y cómo proporcionan controles de mitigación personalizados? Hay muchas preguntas difíciles de responder, pero ninguna es imposible de resolver.

## Comience siempre con la evaluación de riesgos

A la nube se la considera una tecnología nueva, sin embargo, usted puede argumentar que solo es la evolución de servicios administrados o el hospedaje de aplicaciones web en Internet. Como sucede con los cambios, tales como adaptarse al modelo del servidor del cliente, en un análisis minucioso, resulta que la nube también requiere el mismo análisis que se necesita en cualquier tecnología nueva: las organizaciones tienen que definir los riesgos y beneficios de la nube e implementar los procesos y las tecnologías necesarias para mitigar y ejecutar la política de gestión de riesgos elegida.

Acordemos una suposición básica que establece que, antes de definir una política de seguridad aplicable que abarque la TI interna, la nube y los entornos alojados, usted debe conocer los detalles de los datos, los procesos comerciales y el flujo de información, y realizar una evaluación de los riesgos. Solo después de realizar un análisis minucioso de los riesgos, podrá definir la estrategia de la nube.

## Fase uno: Descubrimiento

El primer paso para adoptar la nube es determinar qué datos deben quedar bajo su total control y cuáles pueden alojarse en la nube. Este proceso comienza con eDiscovery: encontrar los datos que tiene y dónde están. El proceso de eDiscovery puede ser difícil, y muchas organizaciones se sorprenden con los resultados: por lo general, los datos están mezclados y disipados. La Información de Identificación Personal (PII), como los registros de empleados, debe almacenarse en los servidores con órdenes para actividades de marketing y controles de seguridad poco apropiados para proteger la información confidencial; los registros financieros o los códigos fuentes deben almacenarse en computadoras portátiles sin cifrar.

## Fase Dos: Clasificación

Una vez que sepa dónde están los datos, deberá clasificarlos. Su sistema de clasificación debe estar basado en el esquema que usa el Departamento de Defensa de EE. UU.: "Sin clasificar", "Privado", "Confidencial" y "Altamente confidencial"; también puede usar un esquema más simple, como "PII y No PII", o "verde, amarillo y rojo". Después, debe organizar los datos de los sistemas que alojan datos que tienen la misma clasificación y que están configurados con controles de seguridad asociados. Solo con este paso se puede mejorar la postura de seguridad de la organización, y acercarlo mucho más para satisfacer muchos de los requisitos de conformidad.

## Fase tres: Tránsito de datos

Después de realizar la clasificación de datos, es indispensable definir una política de tránsito de datos a para decidir qué datos estarán bajo su control y cuáles colocará en la nube. La solución de Información de Seguridad y Gestión de Eventos (SIEM) controla los puntos finales, firewalls, soluciones de DLP, usuarios, contenido y actividad de la red para monitorear los datos que van a la red y determinar si están permitidos. Gracias a los registros de firewall y proxy o la actividad de la red, esto se puede hacer a través de simples reglas de combinación de fuente/destino o mediante la identificación inmediata del contenido. Por ejemplo, puede crear una regla que determine que los servidores PCI no envíen datos a la nube.

Con el perfil de red sensible al contenido, también puede controlar los números de seguridad social o de tarjetas de crédito en línea y advertir sobre coincidencias, características típicamente encontradas en las soluciones de Prevención de Pérdida de Datos (DLP). Y si tiene una aplicación de DLP específicamente diseñada, puede ser incluso más granular y transferir los resultados de ella a la SIEM para realizar correlaciones complejas comparadas con otras transferencias inteligentes, incluso aquellas propias de la SIEM. A través del software de protección de punto final o de la auditoría de objetos de Windows, la solución SIEM puede controlar el acceso a archivos y directorios y relacionarlo con el registro de firewall o la actividad de la red. Son muchos los casos en los que se usa la solución SIEM como elemento base para proporcionar inteligencia de seguridad central para defender la seguridad y la nube.

## Construcción de la visibilidad

En la implementación tradicional in situ de TI, las organizaciones pueden definir, implementar y controlar las políticas operativas y de seguridad. El flujo de información se controla completamente. En un entorno de nube, la información de seguridad es más difícil de recopilar. Aunque para los usuarios la seguridad en la nube es casi inadvertida, la SIEM se puede usar para controlar los datos en tránsito y detectar violaciones a las políticas.

Si usted es proveedor, piense en construir la visibilidad orientada al cliente. Esto significa permitir el acceso a la aplicación, identidad y eventos del sistema relevantes a su propiedad y, en lo posible, a la inteligencia de la infraestructura de la actividad de la red.

Las soluciones de SIEM de próxima generación (lo que en Q1 Labs llamamos Plataformas de Inteligencia de Seguridad) ofrecen, incluso, una versión virtual de la capacidad del perfil de la aplicación desarrollada para los entornos virtuales. Y según cómo divida la infraestructura, puede permitir que los clientes tengan acceso para ver sus datos y cargar el servicio.

## SIEM como nube

Desde otra perspectiva, la SIEM brinda capacidad de nube. Creo que en las medianas y grandes empresas, la SIEM puede manejarse como una nube de inteligencia de seguridad interna.

El rol de la SIEM es recopilar la mayor cantidad de datos de muchos grupos internos, incluso elementos organizativos, con diferentes intereses:

- El grupo de gestión de firewall puede transmitir registros a la solución SIEM para alertar sobre eventos de seguridad, como la exploración de puertos en múltiples firewalls, lo cual puede indicar un intento constante de violar el perímetro.

- El grupo de gestión de sistemas puede transmitir los eventos de Active Directory de Microsoft Windows a la solución SIEM para advertir sobre las fallas de inicio de sesión del usuario, indicar un ataque de fuerza bruta de contraseña o intentos de escalamiento de privilegios.

• El grupo de gestión de redes puede transmitir el flujo de datos a la SIEM para detectar ataques de negación de servicios o solucionar problemas de enrutamiento asimétrico.

Aunque muchos grupos trasmitan datos a la solución SIEM, el grupo de gestión de riesgos o seguridad es el encargado de gestionarlos. Esto es análogo a los servicios de la nube, los cuales tienen consumidores y proveedores. Cuando los dos están en diferentes organizaciones, hay una clara división de roles y responsabilidades. Los proveedores comprenden que los datos pertenecen al consumidor, sus clientes y, por lo tanto, los proveedores tienen que cumplir las siguientes obligaciones:

• Proteger los datos bajo su control con un modelo de confidencialidad, integridad y disponibilidad ampliamente usado.

• Segmentar los datos entre clientes.

• Ofrecer los controles apropiados para proteger los datos del cliente contra el acceso no autorizado de entidades externas y entre clientes que comparten la misma nube.

• Evitar el acceso a los datos del cliente para uso o en beneficio del proveedor, salvo que se cuente con la autorización específica del cliente.

• Satisfacer las necesidades de los clientes, como por ejemplo, mediante la creación de informes o la incorporación de nuevos usuarios.

Recordar la existencia de SalesForce.com o Google Mail: estos brindan servicios en nube y tienen muchos clientes. Deben cumplir, contractualmente, los preceptos anteriores. Si hubiera una diferencia entre los tradicionales servicios públicos en nube y la nube en SIEM interna, generalmente, se debe a que el proveedor de la SIEM está encargado de expandir los datos de todos los grupos. Por ejemplo, el grupo de gestión de seguridad y riesgos necesita relacionar los registros de firewall con las alertas de IPS y la actividad de la red para detectar amenazas. Aún así, la diferencia es mínima porque Google no lee los correos electrónicos de los clientes, pero sí proporciona filtros antispam, realiza el seguimiento de estadísticas de utilización y busca intentos de intrusión. Los defensores de la privacidad pueden verlo como una violación, pero la mayoría de los consumidores están conformes con este nivel de acceso.

No obstante, los consumidores no estarían de acuerdo si Google comenzara a enviar los correos electrónicos a otros clientes que no son de la nube. Con una SIEM que proporcione un contexto completo, o una Inteligencia de Seguridad, el grupo de gestión de riesgos y seguridad puede detectar amenazas de seguridad, violaciones a las políticas u otros incidentes procesables que deben escalarse.

Cuando diferentes grupos se encargan de diferentes áreas y gestionan y consumen datos de diferentes comunidades de usuarios, el proceso de escalamiento debe gestionarse con diplomacia y seriedad. Al igual que los proveedores públicos de nube, el proceso de escalamiento debe estar bien definido, y el proceso debe incluir la incorporación de los propietarios de los datos. De esta manera, se garantiza el cumplimiento de la cadena de responsabilidades y permite que el grupo responsable de gestionar el incidente solucione los problemas.

El objetivo es que la SIEM acorte la brecha existente entre los silos de seguridad de una organización. Debe haber un contrato claro entre las funciones de gestión operativas y los consumidores de SIEM. El contrato debe diferenciar las responsabilidades de la entidad de gestión y prescribir un proceso con el que se manejarán los incidentes y las violaciones a las políticas que facultan a los propietarios de los datos, de la misma manera en la que se obligaría al proveedor. Cuando se gestiona correctamente, la solución SIEM como nube genera confianza y cooperación y, a largo plazo, beneficia a los consumidores y al negocio de SIEM.

## Nube lista para SIEM

Quizás el mensaje no se conozca mucho en nuestra industria, pero algunos expertos sostienen que la solución SIEM no es una solución lista para la nube. Yo no estoy de acuerdo. Si se puede trasladar la telemetría a la SIEM, se puede usar para proporcionar visibilidad de la seguridad de manera eficaz. En este punto, no es que la SIEM tenga la inteligencia de seguridad en la nube, es que las nubes todavía no están listas para SIEM. Para eso tendremos que esperar hasta que salga Cloud 2.0. Mientras tanto, proteja todos los datos.

**Q1 Labs, 890 Winter Street, Suite 230, Waltham, MA 02451 USA info@Q1Labs.com**