FORTRA

La verdad Sobre La Seguridad En La Nube

La nuble: Un Arma De Doble Filo

La nube ha traído nuevas posibilidades, y nuevos desafíos, a los equipos de IT de todo el mundo. Con entusiasmo, muchos han expandido sus capacidades a través de servidores en la nube o con enfoques híbridos de entornos locales y en la nube.

De hecho, 2019 ha mostrado que una gran mayoría de organizaciones ahora confían en la nube. De acuerdo a **una publicación del blog** de Dave Bartoletti, Vicepresidente, Analista Principal de Forrester, se esperaba que casi el 60 por ciento de las empresas norteamericanas dependieran de plataformas de nube pública en 2019, un aumento de casi el 10 por ciento respecto al año anterior.

Desde almacenamiento de datos y transferencias a alojamiento de sitios web y ejecución de aplicaciones, la nube proporciona expansión y flexibilidad para muchas funciones de IT, a un costo eficiente.

Desafortunadamente, a pesar de todos los beneficios de la nube, muchos de ellos han producido puntos ciegos en lo referido a la Seguridad.

El **Informe de Seguridad en la Nube 2018** de Cybersecurity Insiders revela que nueve de cada diez profesionales de Ciberseguridad están preocupados por la Seguridad en la nube, un aumento del 11 por ciento respecto al año anterior. Además, según el informe, el 43 por ciento informó que la visibilidad de la Seguridad de la infraestructura en la nube es un desafío continuo, mientras que el 35 por ciento indicó que tiene dificultades para establecer políticas de Seguridad consistentes en los entornos cloud.

La realidad es que la nube no es esencialmente segura, ni siquiera si está trabajando con reconocidos proveedores de servicios, como pueden ser Amazon Web Services (AWS), Google, HP, Microsoft, o IBM.

Estas plataformas tienen funcionalidades y configuraciones de Seguridad, pero los equipos de Seguridad de IT muchas veces fracasan al realizar chequeos, configurarlas correctamente o actualizarlas a lo largo del tiempo. customer trust, and legal fees.

La más mínima fisura en su configuración de Seguridad en la nube puede traer consecuencias desastrosas. Un simple error o mala configuración puede exponer información confidencial a atacantes o empleados que no debían acceder a ella. Una filtración como esa puede costarle a su empresa millones de dólares en multas, daños en su reputación, pérdida de la confianza de los clientes y costos legales.

90%

de profesionales de Ciberseguridad están preocupados por la Seguridad en la nube

La verdad es que cuando se trata de usar efectivamente la nube para proteger la información, es importante que los equipos de IT, proveedores de servicios en la nube, y socios de Negocio, trabajen en conjunto para establecer e implementar políticas que protejan la información con el grado máximo de Seguridad posible.

La Nube Nos Ha Proporcionado Una Falsa Sensación De Seguridad

Los profesionales de IT suelen ser las personas más ocupadas dentro de cualquier organización. Suelen tener escaso personal y una creciente falta de experiencia en Seguridad Informática. El resultado es que el equipo a cargo de la información sensible puede no saber cómo manejar la Seguridad en este cambiante mundo de amenazas informáticas, hackers, y algunos datos almacenados en servidores ubicados en la habitación contigua y otros en la otra punta del mundo, en la nube.

Es muy común contar con programadores o desarrolladores habilitando un nuevo servidor, partición, o instancias, sin entender las políticas predeterminadas de Seguridad que deben aplicarse antes de que pueda ser utilizado para almacenar datos de forma efectiva y Segura. Es ahí donde todo empieza a desmoronarse.

Aunque pueda parecer obvia la importancia de chequear la configuración de Seguridad de los servidores en la nube, recientes incidentes demuestran que los profesionales de IT creen, erróneamente, que los datos en la nube son más seguros por naturaleza.

Los últimos años han visto un aumento en las filtraciones de datos de alto perfil y filtraciones de información almacenada en la nube. Muchos de esos incidentes fueron causados por poco más que un error humano, una serie de equivocaciones que nos recuerda que, simplemente, una mala configuración puede generar tantos eventos imprevistos como hackers maliciosos ejecutando ataques informáticos.

A continuación, encontrará algunas de las historias que han sacudido a empresas y despertado a sus clientes debido a una caída en el uso de la nube.

Exposición de bases de datos de consumidores: La firma de análisis de datos Alteryx y su socio de Negocio, la agencia de generación de reportes de crédito de consumidores Experian, dejaron expuesto un repositorio de datos basado en la nube, que contenía información sensible de más de 120 millones de ciudadanos de Estados Unidos. Este repositorio estaba accesible para cualquiera con una cuenta en AWS que conociese la URL. Ningún nombre fue expuesto, pero cada registro contenía 248 campos de datos (incluidos dirección e ingresos), haciendo muy sencillo relacionar los datos con las personas.

Filtración de datos de Capital One: la filtración de datos de Capital One de 2019 afectó a más de 100 millones de clientes, según The New York Times. Los datos de las solicitudes de tarjetas de crédito entre 2005 y 2019, incluidos los números de Seguridad Social y los números de cuentas bancarias, fueron robados o comprometidos, en uno de los mayores robos de datos jamás reportados en la industria bancaria.

Interrupción de AWS: La interrupción de Amazon Web Services ostensiblemente "rompió" Internet, luego de que un empleado ejecutara un mantenimiento bien intencionado con códigos erróneos. Fue un error tipográfico. El apagón afectó a compañías de renombre como Netflix y Airbnb y demostró claramente el impacto de este tipo de errores simples.

Datos del Pentágono: Un analista de Seguridad Informática descubrió que una base de datos de 1.800 millones de posteos en internet del Comando Central de los Estados Unidos (Centcom) y el Comando Pacífico de los Estados Unidos (Pacom) sacados de redes sociales, noticias y otros foros, estaban abiertos en AWS. Más allá de que la información disponible no era sensible, el hecho de que el Gobierno de los Estados Unidos no hubiera asegurado evidencia de sus prácticas de seguimiento generó dudas acerca de cómo se estaban administrando otras prácticas de Seguridad.

Filtración de datos de los votantes del Comité Republicano Nacional: El trabajo de la Convención Nacional Republicana con la empresa de datos Deep Root Analytics terminó de forma desastrosa después de descubrir una base de datos desencriptada con información de 198 millones de votantes en los Estados Unidos. Como si fuera poco, la base de datos estaba almacenada en un servidor AWS no asegurado. La filtración podría haber sido prevenida si la empresa primero hubiera evaluado las debilidades de Seguridad de la nube.

Filtración de Verizon: PINs, nombres, direcciones e información de cuentas de más de 6 millones de usuarios de Verizon estuvieron disponibles abiertamente durante el mismo mes debido a una mala configuración del repositorio de datos. A la empresa le tomó más de una semana resolver el problema, que causó un daño incalculable a la marca.

¿Cómo Se Desconfiguraron Sus Configuraciones De Seguridad?

Según Gartner, el 95% de los problemas o fallas de Seguridad de los servicios en la nube en 2020, serán responsabilidad del propio usuario, en lugar del proveedor.

Esto es una llamada de atención para los equipos de IT que se sienten confiados en que su socio de servicios en la nube cubre sus espaldas cuando se trata de asegurar la información almacenada en la nube.

A diferencia de otros casos que involucran violaciones de datos gubernamentales, el caso en Suecia no parece involucrar un hackeo u otro tipo de ataque malicioso. En cambio, la atención se ha centrado en una aparente ausencia de Seguridad y supervisión adecuadas.

Lo que suele ocurrir es que, a pesar de que las políticas de Seguridad estén configuradas correctamente desde el comienzo, pueden ser modificadas accidental o intencionalmente, en cualquier momento. Estos cambios pueden pasar inadvertidos por días, semanas o años. Mientras tanto, la información que su equipo de IT cree que está protegida, realmente está accesible para cualquiera que tropiece con ella en la nube pública o que la busque con malas intenciones.

¿Es Una Buena Idea Externalizar La Seguridad En La Nube?

Al subir su información a la nube, básicamente, está tercerizando su Seguridad a su proveedor de servicios en la nube y conserva todos los riesgos al mismo tiempo. Usted tiene la responsabilidad de asegurarse que su servidor en la nube esté configurado de forma apropiada.

Ser negligente con la configuración de Seguridad en la nube puede traer desastrosas consecuencias. Un claro ejemplo de esto sucedió cuando el mundo entero descubrió que la Agencia de Transporte sueca fue responsable de **una filtración masiva de información confidencial,** incluyendo datos sobre la infraestructura sueca y la posible identidad de agentes encubiertos. Esto ocurrió cuando un proveedor, contratado para administrar bases de datos con información sensible, no adoptó las protecciones apropiadas para la Seguridad en la nube. De hecho, tuvieron la libertad de sobrepasar la Seguridad para otorgar credenciales a cualquier usuario que consideraban adecuado, debido a la total deferencia de liderazgo en la Agencia de Transporte. Esto habilitó a los empleados del proveedor en Europa del Este a acceder a información clasificada sin ningún inconveniente.

El Primer Ministro sueco, Stefan Lofven, calificó la violación de información como “un colapso total”. Él dijo: “Es increíblemente serio. Es una violación de la ley y pone a Suecia y sus ciudadanos en peligro “

Las Consecuencias De Una Seguridad Débil En La Nube

La filtración de datos en la Agencia de Transporte sueca puso en riesgo la Seguridad nacional, y las filtraciones de información en el sector privado también pueden acarrear serias consecuencias. De acuerdo al Estudio sobre el Costo de Filtraciones de Datos 2019, de Ponemon, el costo promedio de una filtración de datos es de 3.92 millones de dólares, y el tiempo total que lleva contener la filtración es de 279 días.

El reporte también incluye al sector Salud y señala que es la industria que sufre mayores consecuencias económicas, ya que las filtraciones de datos le cuestan, en promedio, 6.45 millones de dólares. En una de las filtraciones de datos más infames de los últimos años en el gigante de venta minorista Target, sufrió un ciberataque que le costó aproximadamente 292 millones de dólares, según **el informe financiero anual de Target**. Desde entonces, las violaciones de datos han continuado apareciendo en los titulares, incluido el ejemplo mencionado anteriormente de Capital One, Facebook y British Airways, según **informó Forbes**.

Filtraciones de datos

Cuando hackers externos o personas internas sin autorización ganan acceso a información protegida, usted sufre una filtración de datos. Según qué datos estuvieron expuestos, se le solicitará cumplir con las notificaciones de las leyes de filtraciones, un proyecto costoso y que consume mucho tiempo, al que se le suma el daño que causa sobre la reputación de su organización.

Pérdida o robo de IP

La información de su empresa, ya sea que incluya especificaciones de producto, iniciativas estratégicas, información de empleados, o contactos de clientes, no es algo que desee que esté disponible para que todo el mundo vea.

Infringir las normativas de Cumplimiento

Los requerimientos regulatorios como Sarbanes-Oxley (SOX), GDPR, HIPAA, y PCI DSS significan que se necesita tomar medidas específ cas para proteger los datos confidenciales. Infringir estas reglas puede tener como consecuencia directa penalidades económicas, despidos, auditorías y acciones legales.

Pérdida de confianza de los clientes

Ya sea que su empresa tenga un nombre reconocido o sea una marca confiable en un mercado de nicho, sus clientes deben tener la confianza de que usted está haciendo todo lo que está en su poder para proteger su información sensible. Lo último que quisiera es que sus clientes sepan que su empresa ha descuidado los estándares de Seguridad o que su información protegida ha sido abierta al público en Internet. Existen mejores o peores formas de manejar una filtración de datos, pero la prevención es siempre el mejor camino.

Pérdida de ganancias

Luego de una noticia de filtraciones de datos u otro incidente de Seguridad, lo más probable es que los clientes se mantengan alejados, al menos por un tiempo. Para los sitios web alojados en la nube, el costo de una interrupción puede ser enorme. **Un reporte** estima que una hora de interrupción le costó a Netflix 200.000 dólares.

Costo de resolución

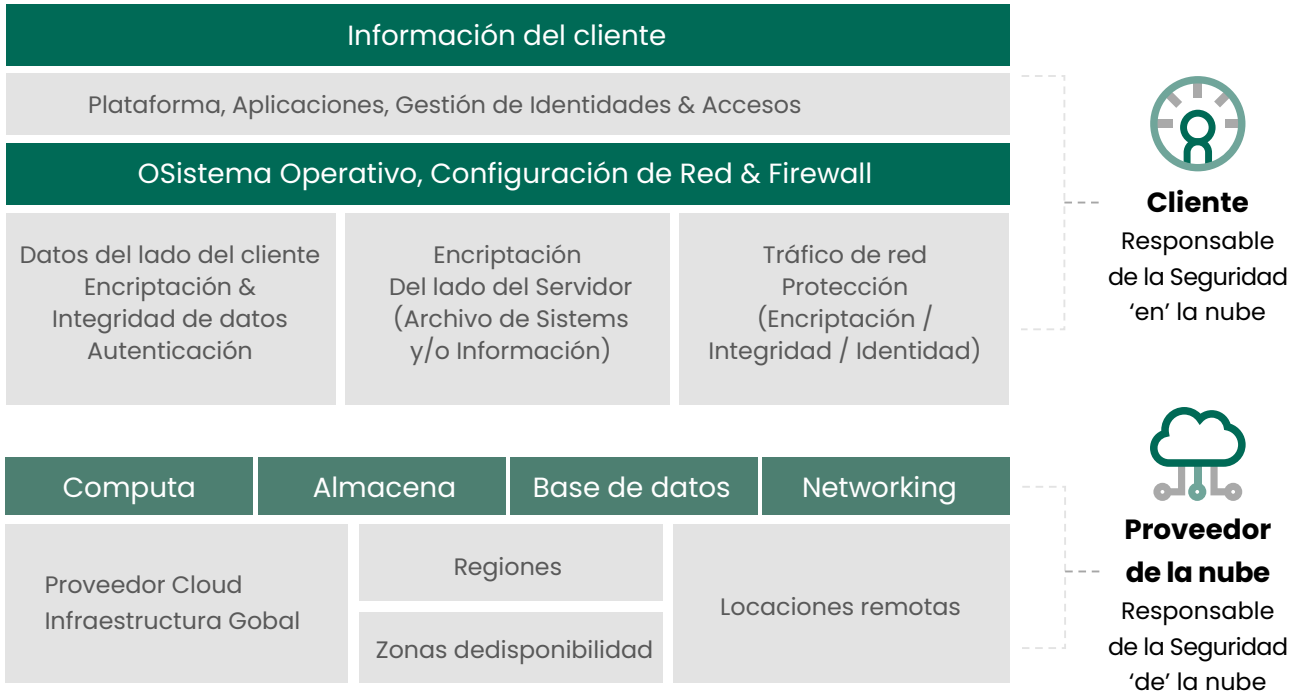
La filtración de datos de Equifax de 2017 derivó en una multa de 700 millones de dólares, anunciado por la Comisión Federal de Comercio en julio de 2019. La violación de datos, que impactó a casi 147 millones de personas, según el sitio web **Equifax Data Breach Settlement** y **reportado por Los Angeles Times**, es una de las mayores multas derivadas de casos de filtración de datos jamás registrado.

¿Los Proveedores De Servicios En La Nube Ofrecen Seguridad Sólida?

Proveedores como AWS (Amazon Web Services) difunden orgullosamente sus funcionalidades de Seguridad como firewalls, encriptación de datos y control de identidad de accesos a sus sitios. AWS también analiza las últimas noticias en su blog de Seguridad. Lo importante es recordar que solo porque los proveedores de la nube ofrezcan niveles de Seguridad altos, eso no siempre significa que las políticas de Seguridad estén configuradas y aplicadas todo el tiempo.

Con el paso del tiempo, las configuraciones pueden modificarse de forma inadvertida, a medida que más personas tienen acceso a la infraestructura en la nube. Piense en la Seguridad de la nube como una responsabilidad conjunta del proveedor y su equipo de IT (así como de los terceros de confianza con los que trabaja). Esto se llama “modelo de Seguridad compartido”.

Como se muestra en el gráfico, AWS o su proveedor de servicios en la nube es responsable de la Seguridad de la nube y usted, como usuario final, es responsable de su propia Seguridad en la nube.



Las Configuraciones De Seguridad Requieren Atención Constante

Como con cualquier otro servidor, la Seguridad en la nube no es un proyecto que se pueda configurar para luego olvidar. Los servidores en la nube requieren de atención constante para garantizar que estén configurados correctamente. Tener una política de Seguridad documentada es un paso importante en el proceso, e incluir a los servidores en la nube junto a las instancias locales, significa que no serán ignorados durante el chequeo periódico.

El monitoreo regular de la configuración de Seguridad de todos los servidores significa que cualquier configuración alterada puede ser identificada de manera temprana, y rectificada, antes de que cause un daño o una intrusión potencial. Este paso también ayuda a eliminar errores humanos, sobre todo cuando está instalado un software de detección automatizada.

Para ayudarlo a comenzar, a continuación, encontrará una lista de cuestiones a considerar al momento de administrar su configuración de Seguridad en la nube:

Configuraciones de usuario y grupo

- ¿Quién puede acceder a su sistema, desde dónde, y qué permisos le han sido otorgados?

Configuración de red

- ¿Cómo pueden acceder las personas a sus sistemas y servicios? ¿A través de qué puertos y protocolos?

Estado de servicios de sistemas críticos

- ¿Sus servicios críticos, como restricciones de auditoría y firewalls, están activos?
- ¿Los servicios que no son necesarios están deshabilitados y en una blacklist?

Políticas de registros privilegiados y contraseñas

- ¿Quién tiene acceso a la ejecución de funciones administrativas?
- ¿Sus políticas de credenciales están aseguradas al nivel requerido según la criticidad de sus datos?

Transferencia de datos y protección de malware

- ¿Sus transferencias de datos se realizan de una forma segura y auditable?
- ¿Su sistema permite realizar transferencias de archivos desencriptados de cualquier tipo?
- ¿Sus sistemas están protegidos frente a ataques de ransomware o malware con soluciones de antivirus nativas?

Discovery de infraestructura y documentación

- ¿Su equipo de DevOps está implementando sistemas sin su conocimiento?
- ¿Se implementan los controles de Seguridad apropiados a todos los sistemas, a medida que son creados?
- ¿Cuenta con una herramienta de discovery automático y documentación de todos sus activos en la nube?
- ¿Recibe una notificación inmediata cada vez que un nuevo sistema es creado en su entorno en la nube?

Auditoría y generación de reportes

- ¿Puede producir un reporte de auditoría que demuestre el estado de la Seguridad de sus sistemas?
- ¿Puede producir el mismo reporte para todos los sistemas, incluso los implementados recientemente?
- Histórico: ¿Cómo se veía la Seguridad la semana o el mes pasado?

Controle La Seguridad En La Nube Con Confianza

Con frecuencia, los administradores de IT están sobrepasados de tareas o les falta la experiencia en Seguridad necesaria para las crecientes demandas provenientes de administrar infraestructuras en la nube. Con nuevas instancias en la nube incorporadas todos los días, es imposible mantener un control manual de las configuraciones de Seguridad.

Una solución simple es recurrir a herramientas probadas que automaticen las tareas de administración de Seguridad y cumplimiento, al mismo tiempo que gestionen scripts a través de servidores locales y en la nube. **Powertech Security Auditor** de Fortra es una solución de administración de Seguridad y generación de reportes de cumplimiento para Linux, IBM AIX, y Windows, que simplifica y automatiza las tareas de administración de Seguridad y generación de reportes de cumplimiento desde una consola basada en web, fácil de usar.

Security Auditor le permite:

- Documentar sus políticas de Seguridad automáticamente
- Automatizar la adherencia de políticas de Seguridad
- Hacer cambios en múltiples servidores al mismo tiempo, manual o automáticamente
- Gestionar el cumplimiento con las políticas de Seguridad desde una única pantalla

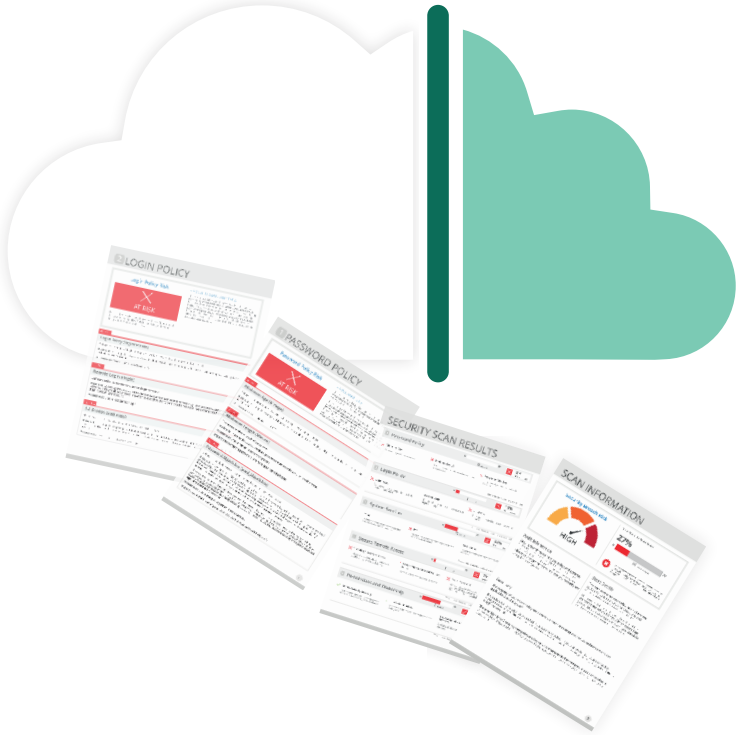
Security Auditor me recuerda diariamente las excepciones a las políticas, para que nada se nos escape. Estamos haciendo más con menos. No queremos salir a buscar lo problemas, sino que ellos vengan a nosotros. Security Auditor permite que hagamos eso.

Steve Mulder,
Especialista en Sistemas de Soporte, Amway

Conclusión

Los servidores en la nube ofrecen una forma efectiva y escalable para proporcionar acceso a la información de su empresa, pero usted no puede ignorar la necesidad de protegerlos con políticas de Seguridad administradas apropiadamente.

Así mismo, con la incidencia de malas configuraciones y errores humanos, sumada a hackers en busca de vulnerabilidades, los equipos de Seguridad de IT deben estar a la ofensiva. Es crítico evaluar continuamente la Seguridad de los entornos en la nube para asegurar que la configuración sea la apropiada y que se hayan tomado todas las precauciones necesarias. La información confidencial que almacena, así como la reputación de su organización están en juego.



Solicite Un Security Scan Gratuito

Fortra puede ayudarlo a simplificar y automatizar su enfoque de Seguridad en entornos locales, en la nube o híbridos. Solicite un **Security Scan** gratuito para identificar errores y vulnerabilidades en su configuración de Seguridad.

FORTRA

Sobre Fortra

Fortra es una compañía de Ciberseguridad como ninguna otra. Hemos creado un futuro más simple y sólido para nuestros clientes. Nuestro equipo de expertos junto con el mejor portfolio de soluciones integradas y escalables aportan equilibrio y control a organizaciones en todo el mundo. Somos impulsores del cambio positivo y su aliado de confianza para darle tranquilidad en cada paso de su camino de Ciberseguridad. Conozca más en fortra.com/es

fta-cs-gd-es-1122-r1-79d