FORTRA

Ebook (GoAnywhere)

Control en la nube: Resuelva sus problemas de datos con MFT

Introducción

En los dos últimos años, el rápido e inesperado cambio en las operaciones empresariales ha expuesto nuevos desafíos para la Seguridad. Mientras muchos han sufrido con la logística de mantener los datos seguros al adoptar tecnologías en la nube, otros han reconocido el valor de una buena solución de transferencia segura de archivos. Hablamos con un grupo de expertos en la materia de varias empresas y sectores que nos han compartido sus historias para que usted se introduzca en la nube de la forma más fluida, segura y eficaz posible.

La transformación digital ha cambiado sustancialmente la forma de dirigir un negocio. Gran parte de esta transformación se está produciendo en el ecosistema de la nube. Las implementaciones en la nube están teniendo lugar en todos los sectores y todas las industrias. Con la nube, empezamos a entender las ventajas de los servicios de valor añadido implementados en el ecosistema de la nube mediante una gestión eficiente de los datos. Otras ventajas de gestionar y almacenar datos en un entorno de nube son el ahorro de costos, la flexibilidad, la movilidad, la mejora de la seguridad de la información, el aumento de la colaboración y los nuevos conocimientos que ofrece un activo de datos empresarial.
(Reza Alavi | Senior Manager, Technology and Digital Risk | LinkedIn)

Trabajar desde casa ha acelerado la adopción de la tecnología en la nube, pero a pesar del incremento de las aplicaciones colaborativas basadas en la nube, los métodos de transferencia de archivos no han cambiado tanto. Al parecer, esto se debe más a la necesidad de actualizar o sustituir un determinado sistema y trasladarlo a la nube. Esto fue sin duda el catalizador para nosotros. Estábamos trasladando un sistema crítico para la empresa desde un modelo *on-premise* (local) a un sistema en la nube, y necesitábamos asegurarnos de que los datos estuvieran protegidos. La Transferencia Segura de Archivos nos permite mover archivos con la flexibilidad y el control que necesitamos.
(Matthew Hankinson | Infrastructure manager | LinkedIn)

Pregunta 1: Desafíos *on-premise*

¿Cuáles son algunos de los principales retos a la hora de transferir datos on-premise y en la nube? ¿Cómo ayuda disponer de la tecnología adecuada en cuanto a productividad, Seguridad y cumplimiento de la normativa?

Funso Richard | Information Security Officer | LinkedIn

El principal desafío que afrontan las organizaciones es una gestión ineficaz de los datos. El uso de protocolos *on-premise* para transferir archivos entre organizaciones y a terceros externos plantea importantes retos, como la falta de Seguridad y de movilidad, los problemas de rendimiento, el costo del mantenimiento, el impacto en la productividad y la deficiente experiencia del usuario. Una alternativa ha sido migrar la transferencia de datos a la nube. Sin embargo, una planificación ineficiente, el costo económico, una configuración incorrecta y la deficiente experiencia del usuario son algunos de los desafíos que plantea la transferencia de datos en la nube. Debido a la deficiente experiencia del usuario, los empleados usan soluciones de transferencia de archivos no aprobadas para trasladar los archivos. Este es un riesgo grave que expone a las empresas a la pérdida y filtración de datos.

Para garantizar la protección de los datos y optimizar la productividad, es crucial invertir en la tecnología de transferencia de archivos adecuada para que la empresa siga funcionando eficaz y eficientemente. Al incrementarse la adopción del trabajo a distancia y la dependencia de la cadena de suministro, las organizaciones necesitan una tecnología de transferencia de archivos dinámica, fiable y flexible para mover datos a través de múltiples protocolos, plataformas y entornos. Esta tecnología es la Transferencia Segura de Archivos (MFT, por sus siglas en inglés). MFT se crea con controles de seguridad, sin menoscabar la productividad y el rendimiento. Las ventajas de utilizar MFT son la reducción de los costos, la gestión centralizada de los datos, la escalabilidad, la integración, el cumplimiento normativo, el acceso rápido a los datos, la mejora en la toma de decisiones y una experiencia positiva del usuario.

Gary Hibberd | Security Consultant | LinkedIn

Hay un desafío fundamental en la transferencia de datos, ya sea on-premise o en la nube, y es el del control, quién tiene acceso a los datos y cómo se transfieren. Por supuesto, la cantidad de datos que procesamos es cada vez mayor, y compartirlos de forma segura a través de nuestra infraestructura es clave para cualquier organización.

Los desafíos a los que nos enfrentamos se reducen a la gestión y el control de estas transferencias, y cuando se producen, debemos aplicar soluciones técnicas apropiadas, como la Transferencia Segura de Archivos (MFT). Contar con una función de transferencia segura de archivos garantiza que los datos se gestionan y monitorean para garantizar que llegan a su destino de forma segura. Una buena solución MFT reduce los riesgos de cumplimiento de la normativa al garantizar que se mantenga la integridad de los datos. Más allá del cumplimiento de las normas, también aumentará la productividad, ya que reduce la sobrecarga en la red y aumenta la velocidad de transferencia, así como su fiabilidad.

Michael Barford | Solutions Engineer | LinkedIn

En el caso de las transferencias de datos *on-premise*, los principales desafíos siguen siendo la elevada complejidad asociada al desarrollo y mantenimiento de soluciones personalizadas para gestionar transferencias de alto volumen y gran complejidad. Sin embargo, actualmente muchas organizaciones confían en scripts o en soluciones desarrolladas internamente para gestionar las transferencias internas. Esto conlleva grandes costos de mantenimiento y funcionamiento. Normalmente, los errores conllevan un gran costo. Cuando se pierde un archivo, muchos se dan cuenta días después, y hay que movilizar distintos recursos informáticos solo para diagnosticar qué ha pasado, dónde está el archivo, procesarlo manualmente y arreglar el "script" para que el problema no se repita en el futuro. El problema se agrava cuando las personas que desarrollaron la solución personalizada se trasladan a otro puesto o empresa, o cuando hace falta ampliar esta solución personalizada para gestionar nuevos casos de uso, con cada vez más casos relacionados con la nube.

Otro desafío suele estar asociado a los requisitos de seguridad o cumplimiento normativo. Es difícil y costoso cumplir con la normativa sin una solución creada específicamente que esté actualizada con los últimos protocolos de Seguridad y que ofrezca cifrado, auditoría, reportes y segregación de roles de forma completa.

Al pasar a la nube, es importante comprobar si el MFT puede interactuar con muchas plataformas en la nube, así como con las API REST, que evolucionan constantemente para cubrir futuros casos de uso.

Debido a la cantidad de plataformas e interfaces con las que trabajan las empresas actualmente, la Seguridad, la auditoría y el mantenimiento de las transferencias de datos son cada vez más difíciles. Tradicionalmente, los procesos de transferencia de archivos se configuran y luego, se dejan ejecutar, lo que funcionaba bastante bien en una época en la que solo había transferencias SFTP o FTP, al poder usar el mismo proceso para múltiples socios de negocio. Las dificultades surgen cuando es necesario adaptar el proceso, lo que suele ser el punto de inflexión para que los clientes opten por una solución MFT.

Utilizando la tecnología adecuada, las empresas pueden adaptarse más fácilmente a los cambiantes requisitos de transferencia de archivos a los que puedan enfrentarse.

Ray Sutton | Technical Consultant | LinkedIn
La transferencia de datos plantea muchos desafíos, sobre todo a la hora de exponer estos servicios a terceros externos, posiblemente a través de Internet. Estos desafíos giran en torno al mantenimiento de un entorno bueno y seguro y, en la mayoría de los casos, a tener que sobredimensionar la solución para proteger las redes y los sistemas de su organización. No obstante, quizá sea justo decir que este desafío también existe en la nube, donde hay que atender aún más la seguridad del data center basado en la nube donde se conectan y protegen los datos. Tener un equilibrio adecuado es clave para garantizar que se cumplan los requisitos de productividad, Seguridad y cumplimiento de la normativa por parte de los empleados. Cualquiera que interactúe con sus sistemas también necesita asegurarse de que usted cumple todos los requisitos de seguridad, pero que también tiene un proceso fácil de seguir para transferir datos. Esto es crucial para mantener un alto nivel de seguridad. Saltarse este paso, o poner procesos o sistemas difíciles, podría provocar que algunas personas busquen alternativas más rápidas, lo que, a su vez, podría causarle más riesgos en la forma de dar soporte a sus soluciones en la nube u *on-premise*.

Matthew Hankinson | Infrastructure manager | LinkedIn
El desafío de la transferencia segura de datos es ese delicado equilibrio entre lograr lo que la empresa requiere y demanda, y cumplir los requisitos de ciberseguridad. Debe satisfacer las necesidades de la empresa y, a la vez, cumplir con la normativa. La transferencia segura de datos debe abordar las inquietudes de todos, y la ciberseguridad es necesaria, no solo desde un punto de vista práctico, sino también desde el punto de vista normativo.

Tradicionalmente, las principales diferencias entre trasladar archivos *on-premise* y en un entorno de nube siempre se habían centrado en el control. Con la nube, existe ese territorio desconocido de tener que confiar en algún tercero en cierto modo. Debe asegurarse de que el proveedor de servicios en la nube cumpla sus normas de seguridad. También debe estar al tanto del tipo de datos que envía. Si los datos contienen información de identificación personal (PII, por sus siglas en inglés), hay que asegurarse de disponer de protecciones adicionales en el proceso. La gente no se pregunta con demasiada frecuencia qué se está transmitiendo. Solo se les pide que muevan un archivo de un lugar a otro, pero ¿qué hay realmente en esos datos? ¿Es algo que causará más de un problema a la empresa si se filtra? Es importante contar con una solución fiable de transferencia segura de archivos que incluya esas funciones de seguridad. Gran parte del desafío consiste en romper viejos hábitos. La gente ha estado transfiriendo información libremente durante muchos años, pero ahora tiene que pensar en los datos que contienen esos archivos o podría estar infringiendo las leyes de privacidad. Trabajamos para educar a los usuarios y que reflexionen sobre lo que envían. Intentamos tener un proceso estándar y algunos puntos de control iniciales sobre lo que se requiere.

Soulos Panagiotis | Global Information Security Manager | LinkedIn

Algunos de los principales desafíos a la hora de transferir datos *on-premise* son:

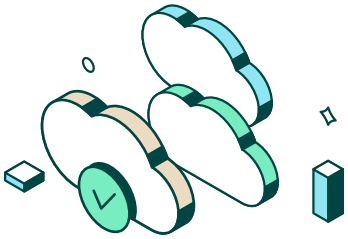
Debilidades de la Seguridad: Las soluciones tradicionales de transferencia de archivos *on-premise*, como FTP y SFTP/FTPS, no cubren todas las necesidades actuales de seguridad para la empresa. El FTP ni siquiera se diseñó pensando en la Seguridad, ya que carece de controles de seguridad básicos, como un canal de autenticación encriptado. La encriptación, como la de transferencia y almacenamiento para proteger la información en tránsito y en reposo, es una idea posterior que requiere pasos adicionales y conocimientos informáticos, lo que convierte el envío y almacenamiento de archivos de forma segura en algo difícil, caro y lento. Además, estas soluciones no gestionan el intercambio de credenciales de los usuarios y debe realizarse con procedimientos externos y normalmente manuales, que pueden carecer de medidas de seguridad, lo que aumenta la posibilidad de revelar las credenciales.

Automatización: Las soluciones tradicionales no ofrecen automatización ni programación de las operaciones de transferencia de archivos. Por lo general, hace falta scripting manual o soluciones adicionales para satisfacer esas necesidades, lo que conlleva un aumento de los costos y de la experiencia del personal informático.

Alertas automáticas: Las soluciones tradicionales no ofrecen notificaciones automáticas y deben combinarse con otras soluciones para notificar a los usuarios cuando ha fallado una transferencia de archivos.

Continuidad del Negocio: Los planes de recuperación ante desastres deben diseñarse e implementarse manualmente, ya que las soluciones tradicionales no incorporan mecanismos automatizados de DRP. Además, los procedimientos de recuperación cuando falla el servicio se realizan manualmente.

Problemas de capacidad: Las soluciones *on-premise* pueden tener problemas al transferir archivos de gran tamaño, lo que puede ocurrir por pequeños cortes y errores en la red.



Los principales desafíos a la hora de transferir datos en la nube son:

Cumplimiento Normativo: Según el tipo de organización, puede ser necesario cumplir con normas industriales y/o reglamentos específicos. La soberanía de los datos también debe tenerse en cuenta al almacenarlos y transferirlos en la nube.

Pérdidas/filtraciones de datos: Si el proveedor de la nube se ve expuesto, pueden producirse pérdidas o filtraciones de datos.

Acceso/Denegación de servicio: El acceso a los servicios puede prohibirse si el proveedor de la nube sufre un ataque de denegación de servicio, o si la organización ha perdido el acceso a Internet.

Infección por malware: Se requieren controles antimalware para minimizar el riesgo de que el malware infecte los archivos almacenados y transferidos en la nube.

Dependencia (lock-in)/suspensión (lock-out) del proveedor y portabilidad de los servicios: Se debe evaluar el uso de los servicios en la nube para evitar la dependencia y la suspensión del proveedor y que sean, en la medida de lo posible, fácilmente transferibles a otro proveedor de servicios en la nube. Depender del proveedor (lock-in) sería la situación en la que el costo de cambiar de proveedor es tan elevado que la organización se tiene que quedar con el proveedor actual. La suspensión del proveedor (lock-out) se refiere a la situación en la que el proveedor cierra su negocio y deja de prestar sus servicios.

Con la tecnología adecuada, una organización puede abordar estos desafíos asegurándose de que la tecnología elegida pueda mejorar la productividad y la eficiencia de la organización. Las soluciones en nube aprovechan características de la nube como la agrupación de recursos, la rápida elasticidad y el servicio medido. Además, las soluciones en la nube se diseñan e implementan teniendo en cuenta la Seguridad, proporcionando mecanismos de cifrado apropiados para proteger los datos en tránsito y en reposo. Las soluciones en la nube incorporan certificaciones apropiadas, capacidades de auditoría y procedimientos transparentes con los que se logra cumplir en ciertos aspectos.

Casos de uso

Es fácil hablar en términos teóricos de los beneficios de un sistema superior de transferencia segura de archivos. Sin embargo, hay casos de gran éxito en la implementación de GoAnywhere MFT en la nube que dan vida a la narrativa. Los tres casos de uso que siguen a continuación son un ejemplo.

Importante empresa multinacional de salud

Una de las tareas informáticas más importantes de esta organización internacional de salud fue la de migrar servicios a la nube para diseñar un modelo más híbrido.

Cuando contactamos con ellos, tenían una necesidad a largo plazo de actualizar su MFT, que estaba plagado de procesos obsoletos e inmanejables que, si se dejaban, podían suponer una amenaza para la Seguridad en un futuro próximo. También querían madurar su infraestructura de nube, que seguía siendo un proyecto prioritario para ellos en los doce meses siguientes.

Su solución MFT actual había cumplido su vida útil y ya no recibía soporte, lo que dificultaba la actualización de las tareas existentes. Además, el soporte de la nube era limitado y suponía un verdadero problema para su estrategia de migrar más servicios a la nube, por lo que -a principios de este año- completamos la implementación de GoAnywhere en su entorno de nube privada.

Distribuidor de gas natural

Cuando hablamos con esta organización, preseleccionaron GoAnywhere MFT como solución de MFT simplemente porque teníamos una oferta para la nube.

Tenían el objetivo de mantener internamente el mayor número posible de servicios integrados en sus flujos de trabajo de DevOps, y eso significaba que cualquier servicio nuevo que implementaran debía ser compatible con sus contenedores o su infraestructura de AWS.

Nuestra oferta de contenedores estaba en aquel momento aún por desarrollarse, por falta de conocimiento en el Reino Unido, por lo que decidimos apostar por la implementación en AWS.

Para ellos, uno de los valores clave de usar AWS era que les permitía automatizar una parte sustancial de la implementación con los procesos existentes.

Distribuidor internacional de productos

Otra organización buscaba minimizar el espacio ocupado por su hardware y quería adoptar un plan SaaS utilizando MFTaaS.

Utilizaron muy bien los agentes GoAnywhere para implementar un modelo híbrido creando un vínculo de confianza entre las instalaciones on premise y la nube, lo que ayudó a complementar su estrategia a largo plazo de eliminar los servicios *on-premise* locales.

Tenían un requisito clave para la seguridad, que conseguimos cumplir con MFTaaS, gracias, en parte, a la certificación SOC-2 de tipo 1 que hemos obtenido.

En la mayoría de las demostraciones, los clientes consideran seriamente MFTaaS o la implementación en su nube privada.

Pregunta 2: Desafíos de la nube

¿Qué implica una transferencia segura de archivos cuando se traslada a la nube? ¿Qué áreas de la empresa hay que tener en cuenta?

Funso Richard | Information Security Officer | LinkedIn
Adoptar una estrategia en la nube requiere una planificación exhaustiva para evitar la interrupción del negocio. Es igual cuando las organizaciones se plantean trasladar la transferencia segura de archivos (MTF) a la nube. Una migración de MFT a la nube mal implementada podría provocar la pérdida o filtración de datos, multas por infracciones, importantes costos económicos, ineficacia en la toma de decisiones por el retraso en el acceso a los datos, pérdida de rendimiento y productividad, interrupción de la cadena de suministro y una experiencia negativa para el usuario. Para evitar estos efectos adversos, es importante contar con una estrategia bien pensada.

Mover datos a la nube es más una decisión empresarial que un proceso informático. Aunque la tecnología es responsabilidad del departamento informático, antes de la migración de los datos deberá tenerse en cuenta cómo afecta a la empresa. Las necesidades de la empresa son algo clave a considerar. Sí, los datos son el combustible que hace funcionar el motor de la empresa, pero para tener un rendimiento optimizado, ese combustible debe tener la calidad adecuada. Desde la recolección, el almacenamiento, la protección, la transmisión, el acceso, la gestión y la destrucción de los datos, se debe tener en cuenta el objetivo empresarial para seleccionar una herramienta MTF y una estrategia de migración de datos. Esto es innegociable. No cabe duda de que MFT en la nube ofrece escalabilidad de datos, movilidad, visibilidad, interoperabilidad y facilidad de uso en un ecosistema empresarial altamente móvil e interconectado. No obstante, el costo de la implementación y los recursos son cuestiones importantes a considerar por la empresa. Para las organizaciones que están muy reguladas, los requisitos de cumplimiento tienen un papel importante cuando se trasladan los datos a la nube. Para abordar los problemas de cumplimiento, las organizaciones deben seleccionar soluciones MFT que incorporen controles de cumplimiento y seguridad.

Soulos Panagiotis | Global Information Security Manager | LinkedIn
Al pasar a una solución de transferencia segura de archivos en la nube, deberán tenerse en cuenta ciertas cuestiones clave. La seguridad de los datos -en reposo y en tránsito- junto con el cumplimiento de la normativa, encabezan la lista. No puede haber posibilidad alguna de que la introducción de una solución de archivos gestionados en la nube dé lugar a incumplimientos legales, normativos ni de ningún tipo. También deberá tenerse en cuenta el rendimiento del servicio. La interoperabilidad y la portabilidad son factores clave para adoptar la solución en nube. Debe asegurarse de que la migración del servicio tendrá el menor impacto en el funcionamiento de la organización y, si es posible, ningún impacto en absoluto, ni siquiera en los canales de comunicación actuales con las organizaciones colaboradoras y los clientes. Los acuerdos de nivel de servicio (SLAs) deben revisarse a fondo, incluirse en el contrato y cubrir todas las necesidades de la empresa.

También deberá tenerse en cuenta la formación de los usuarios, ya sean usuarios empresariales o personal de IT, para minimizar el riesgo de fallos operativos por falta de conocimientos del personal, y así poder aprovechar todo el potencial del servicio en la nube.

Se debe involucrar a los usuarios finales del servicio, el personal de seguridad de la información, el personal de riesgos operativos, el personal de cumplimiento y jurídico, y el personal de tecnología de la información para garantizar que el servicio en la nube cubra todas las necesidades empresariales.

Gary Hibberd | Security Consultant | LinkedIn
Para que la solución de MFT funcione eficazmente, la organización debe comprender qué datos posee y cómo se utilizan. Una vez entendido esto, hay que desarrollar una estrategia para implementar MFT y comunicarla a toda la empresa, porque lo más probable es que haya que tener en cuenta todas las áreas de la empresa.

Debe darse prioridad a las áreas de la empresa que actualmente transfieren grandes cantidades de datos personales o sensibles por email o FTP, ya que verán las ventajas y los controles que se están empleando. Una buena solución MFT mejorará la seguridad de los datos, y también su privacidad.

Al implementar la MFT, las organizaciones pueden consolidar y gestionar las transferencias de datos a través de una plataforma controlada y supervisada de forma centralizada. Esto ofrece visibilidad sobre qué datos se están transfiriendo, cuándo y por quién. Gracias a esta supervisión, los sistemas MFT ayudan a aportar pruebas que se pueden utilizar en el proceso de auditoría interna.

Ray Sutton | Technical Consultant | LinkedIn

Cuando se migran servicios a la nube, hay que tener en cuenta el riesgo, la Seguridad y el rendimiento. Si al trasladarlo a la nube, el sistema funciona mal o tiene problemas de espera, sus clientes y usuarios de ese servicio podrían dejar de utilizarlo o, en el peor de los casos, encontrar medios alternativos para copiar los archivos. Esto podría causar problemas de Seguridad y exponer información confidencial. La migración a soluciones en la nube no es un realojamiento "lift and shift", especialmente cuando hablamos de datos personales o confidenciales. Recientemente, hemos sido testigos de algunos fallos de seguridad que podrían haberse evitado si se hubieran planificado y comprendido los factores de riesgo.

Algunas áreas clave que tendrá que abordar son el conocimiento de sus datos y las precauciones de seguridad que hay que adoptar. No importa si está migrando a la nube o almacenando datos *on-premise*; las reglas son las mismas. Es vital crear un marco de Seguridad para los datos donde poder manejarlos y protegerlos. Por ejemplo, busque una solución que encripte en tránsito y ofrezca la posibilidad de encriptar en reposo. Hay que proteger esos datos cuando llegan al destino final. Además, hay que ir más allá y, posiblemente, ver cómo aplicar un ciclo de vida a sus datos donde pueda controlar quién puede verlos, editarlos y quizás, incluso imprimirlos.

La nube ofrece un mundo de posibilidades, pero es importante comprender la naturaleza de sus datos y cómo debe proteger este bien tan valioso.

Preguntas y respuestas: Michael Barford | Solutions Engineer | LinkedIn

Migrar a la nube no es un proyecto sencillo. Hay diversos factores que influirán en este evento de habilitación para la empresa. Parte de la diligencia debida consiste en formular las preguntas adecuadas para encontrar la solución que mejor se adapte a su visión empresarial:

- **¿Dónde tienen lugar nuestros flujos de trabajo más importantes, *on-premise* o en la nube?**
  Eso podría ayudarle a optar por una solución MFT alojada en la nube o local, híbrida o ambas.
- **¿Necesitamos una solución MFT que sea "transparente", independientemente de que los flujos de información se produzcan *on-premise*, en la nube o de forma híbrida?**
  Actualmente, es más habitual que los flujos de trabajo automatizados combinen tecnologías tradicionales como SFTP y FTPS con proveedores de servicios en la nube comunes. Probablemente desee poder crear automatizaciones complejas abstrayéndose del conjunto de tecnologías implicadas, de modo que no requiera recursos informáticos con conocimientos de bajo nivel de cada una de ellas.
- **¿Vamos a pasar a una infraestructura de nube pura, o seguiremos operando de forma híbrida a medio/largo plazo?**
  La gran mayoría de las empresas tendrán casos de uso que interconectan la nube con sistemas locales *on premise*. En esos casos, poder implementar la MFT cuando queramos (*on-premise*/nube) y que los agentes automaticen los procesos en los sistemas cada vez que se implementan, puede ser una capacidad crítica. La solución MFT con agentes permitirá automatizar de forma transparente los flujos de trabajo en los que intervienen sistemas *on-premise*, en la nube e incluso en las redes de clientes/socios. Esta estrategia permite una migración fluida a la nube la cual no se produce de la noche a la mañana.
- **¿Necesitamos una solución MFT como servicio en la nube, o debemos poner en funcionamiento una por nuestra cuenta?**
  En caso de que decida poner una por su cuenta, quizá desee evaluar si la solución se ajustará a su estrategia de implementación existente. Es decir, que pueda ser implementada en contenedores/dockers, pueda expandirse, con equilibrio de carga, entre otros aspectos.
- **¿Qué tipo de datos vamos a procesar?**
  Deberá comprobar que las transferencias de información se realizan con los niveles de seguridad/cumplimiento apropiados. En la nube, esto puede ser más difícil, por lo que podría beneficiarse de proveedores que ofrezcan certificaciones, así como funciones como el encriptado en reposo y otras características que satisfagan sus requisitos empresariales.

Buenas y malas prácticas

Como en todas las iniciativas de Seguridad, hay una forma de cumplir la normativa sin estar en realidad seguros. A veces, es fácil satisfacer una lista de cumplimiento normativo, pero tiene el potencial de dejar vulnerable a la organización. Para dar los pasos adecuados, nuestros expertos ofrecen consejos, tanto sobre lo que hay que evitar como sobre lo que hay que procurar.

✕ MALAS PRÁCTICAS: Christos Syngelakis | Chief Information Security Officer | LinkedIn

Cuando se trabaja con transferencias seguras de archivos, son muchos los desafíos a superar. El reto no es tanto dentro de una empresa, sino cuando la empresa debe realizar actividades fuera de su entorno. Por ejemplo, un centro médico que necesite transferir archivos de gran tamaño a los pacientes, o una empresa de marketing que deba compartir archivos fuera de la organización.

Muchas empresas no cuentan con personal informático especializado, ni con algún responsable para este tipo de operaciones. En muchos casos, el destinatario solamente tiene una cuenta pública para transferir correo y nada más. Las herramientas corporativas de las que dispone para gestionar este tipo de transacciones y que, además, cumplan sus políticas organizativas no encajan bien en este escenario.

A veces, puede tener la capacidad de crear una cuenta que dé acceso al destinatario a los productos de Seguridad que utiliza usted, pero por lo general, estas herramientas de comunicación inmediata no son asequibles. No solo conllevan costos humanos, sino posiblemente el costo de la licencia para este tipo de actividad. Las grandes herramientas corporativas de colaboración pueden soportar las transferencias de archivos de empresa a empresa porque hay mecanismos establecidos entre ambas partes, pero, la capacidad bajo demanda puede ser un gran problema.

Otro desafío es la disparidad de poderes entre las empresas. A veces, la otra parte puede ser una autoridad gubernamental que quiere transferir datos y no tiene una forma segura de comunicar todos estos datos, pero insiste en trasladar datos sensibles. A veces hay limitaciones de tiempo y los empresarios quieren que la información se transmita ya. El usuario final va a utilizar cualquier tipo de software disponible públicamente para realizar la tarea.

Hay una enorme necesidad de disponer de una solución que sea fácil de implementar y utilizar sin necesidad de que el usuario final o la otra parte hagan nada. Existen algunas soluciones, pero no son asequibles ni, a menudo, fáciles de gestionar. Todas las empresas lo necesitan porque hay muchos documentos diferentes que contienen información y no interesa que estén disponibles para todo el mundo.

✓ BUENAS PRÁCTICAS: Chris Hodgson | Business Development Manager | LinkedIn

Hay muchos protocolos y métodos para transferir datos a clientes y socios comerciales, todos con sus ventajas e inconvenientes. Disponer de métodos tan dispares para compartir datos puede resultar confuso y difícil para gestionarlos, mantenerlos y cumplir con la normativa. Lo que una solución como GoAnywhere proporciona es una solución centralizada de transferencia segura de archivos que puede ayudar a mover datos desde cualquier endpoint a cualquier endpoint, ya sea *on-premise*, en la nube o en un híbrido de ambos. GoAnywhere proporciona a los usuarios y administradores un marco de Seguridad basado en funciones para iniciar sesión y acceder al sistema, con autenticación de dos factores y encriptación de todos los archivos y datos, en tránsito y en reposo. Esto ayuda a las empresas a automatizar y agilizar sus intercambios de datos sensibles sin dejar de cumplir las normas del sector.

El paso a la nube suele ser el catalizador para que la gente busque una solución de transferencia segura de archivos. Las plataformas en la nube disponen de algunas herramientas muy buenas para mover datos dentro de su propio entorno, pero les falta la capacidad de enviar datos entre diferentes tenencias en la nube. Una solución como GoAnywhere puede ayudar a agilizar el intercambio de datos entre plataformas dispares en la nube, todo desde una interfaz de usuario centralizada. Los departamentos financieros también están muy interesados en explorar las ventajas de las transferencias seguras de archivos a medida que migran a nuevos sistemas ERP basados en la nube y necesitan una forma segura de integrar archivos y datos con los sistemas restantes posteriores o con los socios comerciales.

Conclusión

La transferencia de archivos es un tema profundo. Ahora tenemos muchas formas de transferir datos. Tener la capacidad de supervisión de ello es particularmente desafiante. Hemos dejado atrás los tiempos del Protocolo de Transferencia de Archivos (FTP) y el Protocolo Seguro de Transferencia de Archivos (SFTP), y hemos adoptado nuevos métodos y productos en donde todos los proveedores están basados en la nube. Esto crea elementos dispares; algunas organizaciones están utilizando tácticas más antiguas; todavía utilizan SFTP, y otras están utilizando API, que están obteniendo (pull) y empujando (push) datos todo el tiempo a diferentes terceros y diferentes soluciones en la nube y SaaS. Dada la complejidad de todas estas facetas y las distintas formas de trabajar, no existe una solución única. Mantener un método coherente es un gran desafío porque cada organización tiene su propia manera de hacer lo que considera correcto.

Luego, también es importante poder comprobar la integridad de los archivos que se transmiten. Existen buenas soluciones que sirven para validar los archivos. Si consume muchos datos y obtiene muchos datos de los diferentes servicios web que proporciona, puede escanearlos antes de que se transfieran usando una herramienta de escaneado en línea.

La transferencia de archivos no siempre es un simple movimiento de un archivo desde A a B. Es necesario garantizar la Seguridad en cada paso de la transacción. Si el CEO le pide enviar las hojas de presupuesto a otra ubicación, usted no lo va a hacer por email. Existen buenas herramientas que permiten clasificar los archivos y bloquearlos.
(Goher Mohammad | Head of InfoSec | LinkedIn)

"La transferencia de archivos es compleja, independientemente de si es en la nube, *on-premise* o híbrida. ¿Restringe en función de la extensión, o escanea cada dato que entra en busca de malware para garantizar la integridad de sus datos, entre otros componentes? Además de imponer un conjunto de controles de seguridad sobre la forma de realizar esto, también es importante disponer de patrones reutilizables para que la implementación sea coherente en todos los proyectos e iniciativas que necesiten desarrollar este tipo de soluciones de transferencia de archivos. Tanto si se trata del SFTP tradicional, como si se utiliza el SDK y el conjunto de API de un proveedor para trasladar a algo como un contenedor (bucket) S3 con estrictos controles de acceso, ninguna implementación consiste simplemente en mover. La clasificación de esos datos, dónde residen y los controles de seguridad en torno a esa implementación son igual de importantes".
(Lidia Guiliano | Information Security Professional | LinkedIn)

Tanto si su organización acaba de embarcarse en su aventura por la nube como si ya ha establecido una sólida presencia en ella, la Seguridad debe ser una prioridad para la empresa. La Seguridad es algo más que asegurarse de que sus datos no estén expuestos en Internet. Los datos no son una entidad estática, ni están aislados en un único ámbito. Necesitan moverse para que la empresa funcione. Nunca se insistirá lo suficiente en la importancia de tener una solución de transferencia segura de archivos. Nuestros expertos han presentado muchas ideas sugerentes para ayudar a su empresa a prosperar y crecer, de forma segura, en la nube.

Para saber más sobre cómo controlar la Seguridad de sus transferencias de archivos, contacte con nosotros aquí.

FORTRA

Fortra.com/es

Sobre Fortra

Fortra es una compañía de Ciberseguridad como ninguna otra. Creamos 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

