SOPHOS
Security made simple.

Next-Gen Encryption: El enfoque de Sophos

Las fugas de datos siguen siendo una gran preocupación para todas las organizaciones; no hay nadie en el mundo que sea inmune, independientemente de su ubicación, tamaño o sector. Según Privacy Rights Clearing House, aunque la mitad de las filtraciones de datos en 2014 tuvieron que ver con piratería o malware, la divulgación no intencionada de información fue la segunda causa más común (16%).

Al mismo tiempo, el entorno de trabajo ha cambiado sustancialmente en los últimos años. Las empresas de hoy necesitan protegerse frente a las fugas de datos (respetando la legislación vigente relativa a la protección de datos), a la vez que se aseguran de que sus empleados puedan ser lo más eficientes posible en un entorno tan competitivo como el actual.

La estrategia de Next-Gen Encryption de Sophos se ha diseñado específicamente para satisfacer estas necesidades. Este monográfico explica la necesidad de Next-Gen Encryption y cómo funciona, y demuestra la forma en que sophos simplifica a las organizaciones de todos los tamaños la protección de sus datos al tiempo que mantienen la productividad de sus usuarios.

Situación actual

El entorno de trabajo de hoy en día es muy distinto al de hace cinco o diez años. Las diferencias en el panorama de dispositivos y amenazas son significativas. Echemos un vistazo a dos grandes cambios que han repercutido en la protección de datos.

El dispositivo no es móvil; el usuario, sí

Un usuario final medio tiene, de media, tres dispositivos. Mientras que antes solía haber ordenadores de sobremesa y un portátil de vez en cuando, el panorama se ha ampliado y ha pasado a incluir tabletas y dispositivos móviles. Piense en sus usuarios finales. Es muy probable que tengan un portátil y un teléfono móvil; otros puede que tengan también una tableta o dos.

Los dispositivos móviles a menudo contienen la misma cantidad de información confidencial, o incluso más, que un portátil. Además, pueden perderse con mucha más facilidad. Esto significa que la superficie de ataque potencial aumenta a medida que los usuarios tienen más dispositivos que contengan datos corporativos.

El empleado medio es móvil y se espera que se mantenga productivo mientras se desplaza. En último término, la productividad significa poder acceder a los datos corporativos en el dispositivo de su elección, desde cualquier lugar y en cualquier momento.

Es medianoche. ¿Sabe dónde están sus datos?

¿Sabe dónde están los datos de su empresa? Se encuentran en servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, tabletas y dispositivos de medios extraíbles, así como con proveedores de almacenamiento en la nube. Los datos corporativos confidenciales se hallan fuera de los límites tradicionales de la empresa, principalmente porque la noción de límite de una empresa ha desaparecido.

¿Cómo se define el límite de una empresa para los datos si se encuentran en una amplia gama de dispositivos móviles y soluciones de almacenamiento? Estos dispositivos no están administrados o bien pasan poco tiempo en la red de una empresa. O, en el caso de un proveedor de almacenamiento en la nube, es posible que ni sepa dónde se guardan sus datos físicamente y quién tiene acceso a ellos realmente. Todo esto pone de manifiesto que es necesario proteger los datos donde los usuarios los almacenan.

Definición de la estrategia de Next-Gen Encryption

A la hora de elaborar nuestra estrategia de Next-Gen Encryption, hemos estudiado varias áreas en las que nuestra cartera de clientes podría verse afectada por pérdidas o filtraciones de datos, lo que podría llevar a infracciones de normativas. Nuestra estrategia considera las áreas siguientes:

1. Impacto de los dispositivos perdidos o robados
2. Cómo utilizan los datos los usuarios
3. Divulgación no intencionada de información causada por fallos humanos
4. Ataques de piratería o malware
5. Simplicidad

Aunque en esta lista podríamos incluir los ataques dirigidos (en vez de los ataques oportunistas que usan, por ejemplo, programas maliciosos o pesca de información), la probabilidad estadística de que una pyme sea la víctima de un ataque dirigido es bastante baja. A menos que su empresa sea una organización de gran tamaño, como Sony o Target, o disponga de información muy especializada o confidencial, los malos simplemente no le dedicarán el esfuerzo necesario para un ataque dirigido.

Impacto de los dispositivos perdidos o robados

El usuario medio tiene tres dispositivos, que pueden robarse o perderse con gran facilidad. Un usuario quizá se deja el teléfono en el tren de camino al trabajo, o se deja sin querer el portátil en los controles de seguridad del aeropuerto al salir corriendo porque va a perder su vuelo. Los dispositivos son pequeños y los accidentes ocurren. El cifrado de disco completo es útil para la protección de los datos en reposo y es una buena primera línea de defensa. Pero no es suficiente para proteger los datos corporativos que se basan en el comportamiento por sí solo de los usuarios de hoy día.

¿Cómo utilizan los datos los usuarios?

Observe a sus usuarios finales durante una hora y vea cómo utilizan los datos. Los crean, en forma de documentos, presentaciones, etc. Copian archivos en recursos compartidos de red o unidades USB o los suben a un proveedor de almacenamiento en la nube. El usuario final trabaja con archivos y los archivos se mueven entre dispositivos y las distintas opciones de almacenamiento. En estos tipos de situaciones, la protección de datos es imprescindible.

Simples errores humanos

Todos somos humanos. Todos cometemos errores. Todos hemos creado un correo, adjuntado el archivo equivocado y enviado el correo (o enviado el archivo correcto al destinatario equivocado). Existen muchos ejemplos de simples errores humanos que pueden provocar pérdidas o filtraciones de datos. Los navegadores web y clientes de correo electrónico son buenos ejemplos de herramientas de productividad que los usuarios finales utilizan para compartir datos, pero que pueden accidentalmente exponer datos corporativos a la nube o a la persona equivocada.

Ataques de piratería o malware

El análisis de Privacy Rights Clearinghouse de las filtraciones de datos en 2014, que está clasificado por tipos de filtraciones, reveló que la piratería o el malware representaban el 51% de las filtraciones de datos. Los programas maliciosos no dejan de crecer en número y complejidad. Aquí también se incluye el robo oportunista de datos. El malware no es digno de confianza y definitivamente no debería tener acceso a los datos cifrados.

Simplicidad

El cifrado funciona mejor cuando nadie sabe que está ahí. Proporciona protección de forma silenciosa sin afectar a la productividad del usuario final. Por ejemplo, pensemos en el protocolo HTTPS. La S significa seguro, y quiere decir que todas las comunicaciones entre el navegador y el sitio web están cifradas. Pero la mayoría de usuarios no perciben la diferencia en la dirección URL que visitan.

El cifrado debe ser fácil de utilizar tanto para el administrador como para el usuario final para poder conseguir un alto nivel de aceptación.

Presentación de Sophos Next-Gen Encryption

La estrategia de Sophos Next-Gen Encryption parte de dos afirmaciones:

1. Todos los datos que crea un usuario final son importantes y deben protegerse (cifrarse). Esto se conoce como cifrado "siempre activo" o cifrado por defecto.

2. El cifrado debe ser persistente dondequiera que un archivo se ubique, copie o mueva.

En general, se considera que el cifrado es una de las mejores formas de proteger los datos. Tanto si el usuario está creando un documento donde explica su nueva idea para patentar o una hoja de cálculo para justificar un nuevo concepto de negocio, todos ellos son datos importantes y deben cifrarse de forma automática y transparente. Un usuario no debería preocuparse por tener que decidir si cifrar un archivo o no en función de la impresión que tenga de lo importante que es. De hecho, es posible que los usuarios ni se den cuenta de que los datos están cifrados. Esto permite que el usuario se mantenga productivo y sus datos estén seguros al tiempo que sigue flujos de trabajo existentes.

Una vez se cifra el archivo, debe permanecer cifrado. Independientemente de lo que le pase al archivo, ya sea que lo muevan, copien o cambien de nombre, y de si el archivo permanece dentro de los límites del dispositivo, el cifrado debe ser persistente. Si un usuario pierde sin querer un archivo, se perderá en su forma cifrada, haciéndolo inservible/ilegible para cualquier persona que no tenga permiso para verlo.

¿Qué hay de la DLP?

Cuando pensamos en la protección de datos, a menudo nos viene a la cabeza la prevención de pérdida/fuga de datos (DLP, por sus siglas en inglés). Históricamente, la DLP y el cifrado han ido de la mano. Aunque la DLP es una gran tecnología, existen muchos ejemplos de empresas que fallan a la hora de implementar una estrategia DLP después de gastar una cantidad considerable de tiempo o dinero en el esfuerzo. El problema es la complejidad de la tarea. Hay que establecer reglas para datos que quizá no haya creado todavía. Una problemática común es que los administradores definen reglas demasiado estrictas y luego tienen que hacer frente al volumen de trabajo generado por los falsos positivos. A veces, los administradores hacen las reglas más flexibles y entonces los datos salen de la organización a pesar de los sistemas DLP. Sophos le da la vuelta a la DLP al eliminar la necesidad de clasificar los datos. Esta simplificación ayuda enormemente tanto al usuario final como al administrador.

Esto no quiere decir que la DLP no sea importante. Sigue teniendo un papel dentro de Next-Gen Encryption. Sin embargo, debería ser la excepción, no la norma. Cuando el usuario quiere descifrar datos, suprimir la protección de un archivo es una decisión consciente. Ese es el momento para que se ejecuten las reglas DLP si se desea. Si no se generan señales de alerta, el usuario obtiene el permiso para descifrar el archivo porque no contiene nada que se considere delicado. No obstante, si se genera algún tipo de alerta, se deniega la solicitud para descifrar el archivo. Este enfoque es un mecanismo a prueba de fallos para garantizar que los archivos permanezcan cifrados. Además, se registran y auditan todas las solicitudes de descifrado de archivos.

El uso de este enfoque simplifica enormemente la DLP y, puesto que la evaluación de las reglas DLP pasa a ser la excepción (usadas solo cuando los datos se descifran), reduce considerablemente los requisitos de procesamiento.

Synchronized Encryption

Partiendo del hecho de que todos los datos del usuario se cifran, el siguiente elemento importante que proteger son las claves de cifrado que han cifrado todos esos datos.

La idea fundamental de las claves de cifrado es que solo los dispositivos, aplicaciones y usuarios de confianza deben tener acceso a los datos cifrados.

Para lograrlo, Sophos fusiona los conocimientos y funcionalidades de los productos Sophos Endpoint y Sophos SafeGuard Encryption (SafeGuard) para convertir el cifrado en una tecnología de protección contra amenazas. Sophos Endpoint se encargará de aquello en lo que siempre ha destacado: determinar el estado de seguridad del equipo en cuestión y decidir si los procesos en ejecución son de confianza. Y el producto de protección de datos hará lo que siempre se le ha dado mejor: cifrar datos y proteger el acceso a las claves.

A la hora de determinar cuándo se emiten las claves y se permite el acceso al contenido cifrado, triangulamos y sincronizamos la identidad del usuario, el dispositivo y la aplicación o proceso.

Para poder considerarse de confianza y acceder a los datos cifrados, el usuario debe utilizar un dispositivo de confianza, ser un usuario de confianza y usar un proceso o aplicación de confianza para acceder a los datos.

Estas tres condiciones deben validarse para poder acceder a la clave de cifrado y visualizar los datos.

En casi todos los casos, un usuario corporativo legítimo puede acceder a los datos de forma transparente mediante un dispositivo de confianza (es decir, un dispositivo proporcionado por la empresa) y aplicaciones de confianza. Si no se cumple una o varias de estas condiciones, se le denegará el acceso a la clave y, aunque podrá ver el archivo cifrado, no podrá ver su contenido. De este modo, es posible que los programas maliciosos que roban datos puedan exfiltrar un archivo, pero ese archivo se quedará inutilizado sin la clave de acceso.

Dispositivo de confianza

Existen muchas formas de determinar si un dispositivo es de confianza. Por ejemplo, puede ser porque los productos de Sophos adecuados están instalados. O quizá porque el agente Sophos Endpoint ha evaluado el sistema y ha calificado su estado como correcto (o un Heartbeat™ verde). Además, un dispositivo de confianza puede ser un dispositivo móvil que esté administrado por la solución EMM de la empresa y, por consiguiente, cumpla con la política de seguridad de la organización. Por otro lado, un administrador puede indicar explícitamente que un sistema no es de confianza, como un caso de uso de contratista.

Si un portátil Windows o Mac se encuentra en estado de infección activa, dado que la estación está en proceso de eliminar malware, el sistema probablemente no debería considerarse de confianza. Para un dispositivo móvil, como un iPhone o teléfono Android, si no cumple la política de cumplimiento corporativa (por ejemplo, si un dispositivo está desbloqueado o no tiene una contraseña para la pantalla de bloqueo), tampoco se debería considerar de confianza.

Usuario de confianza

Al igual que existen muchas formas de determinar si un dispositivo es de confianza, hay muchas maneras de establecer si un usuario es de confianza. Puede ser en función de su identidad o simplemente porque haya podido iniciar sesión en el sistema correctamente. Existen casos de uso, como cuando un usuario deja una empresa, en los que los usuarios pueden iniciar sesión en su dispositivo correctamente pero no deberían tener acceso a los datos cifrados.

Proceso de confianza

Sophos Endpoint será el principal encargado de determinar si un proceso es de confianza o no. Los pormenores exactos sobre cómo conseguirlo, tanto con como sin Sophos Endpoint, están fuera del alcance de este documento.

De forma genérica, la lógica interna no considera de confianza las PUA (aplicaciones no deseadas), el malware, los virus, los navegadores web o los clientes de correo electrónico. Sin embargo, hay otros tipos de aplicaciones, como los programas de torrents, que quizá las empresas instintivamente no consideren de confianza para acceder a los datos cifrados. Por defecto, los navegadores web y los clientes de correo electrónico no son de confianza, ya que constituyen formas en las que los usuarios pueden compartir o perder datos accidentalmente. Esto ayuda a protegerse contra los simples errores humanos.

¿Por qué hablamos de procesos y no de aplicaciones? En primer lugar, esta cuestión gira en torno a garantizar que se mantenga la productividad del usuario final. Al bloquear solamente el proceso que realmente pone en peligro la seguridad, se permite que todos los procesos de confianza se ejecuten sin obstáculos.

Pasemos a ver tres ejemplos de un proceso que no es malware ni virus y veamos si pueden considerarse de confianza.

1. **Bloc de notas**

   El Bloc de notas es una aplicación autónoma y simplista. Se puede considerar de confianza ya que es simple y no contiene ninguna actividad maliciosa. Dado que se considera que el Bloc de notas es de confianza, puede acceder a una clave de cifrado. Esto permite que los documentos creados con el Bloc de notas se cifren por defecto, así como mostrar documentos de texto sin formato cifrados.

2. **Internet Explorer**

   Internet Explorer cuenta con un amplio historial de vulnerabilidades de seguridad y es un método habitual para introducir programas maliciosos en un dispositivo. Como tal, por defecto no debe considerarse de confianza. Dado que Internet Explorer no es de confianza, no puede acceder a una clave de cifrado y, por consiguiente, solo puede acceder a los archivos en su forma cifrada. No puede abrir ni visualizar el contenido, pero puede subir un archivo cifrado a un servicio de intercambio de archivos en la nube.

3. **Microsoft Word**

   Microsoft Word se encuentra en una zona gris: puede ser tanto un proceso de confianza como no de confianza. Word puede comportarse de forma totalmente correcta y ser de confianza, por lo que cuando un usuario lo utiliza para crear un documento, este se puede cifrar por defecto. El usuario solo tiene que hacer doble clic en los archivos cifrados para leerlos y editarlos. El proceso es completamente transparente. Esto se debe a que Word actualmente es de confianza para acceder a claves de cifrado para realizar procesos de cifrado/descifrado en un segundo plano. No obstante, Word también puede estar infectado con algo parecido a un virus de macro, momento en el que Word deja de considerarse de confianza para acceder a la clave de cifrado y no puede leer los datos cifrados.

Estos son solo tres ejemplos sencillos de determinar la confianza de un proceso que ponen de relieve la necesidad de que Synchronized Encryption supervise la integridad continuamente.

Supervisión continua de integridad antes de otorgar confianza

En general, uno quiere que la tecnología de protección de datos supervise continuamente el estado de seguridad, la integridad y la confianza del proceso o aplicación del sistema. El objetivo es mantener la productividad de los usuarios al tiempo que se garantiza la seguridad de los datos. Como se ha mencionado anteriormente, si un proceso no es de confianza solo puede acceder al archivo en su forma cifrada pero no a la clave de cifrado para descodificar el contenido. La mayor parte del tiempo los usuarios finales no se darán cuenta de que esto se está produciendo. Sin embargo, si el proceso es malicioso, como el malware, evidentemente no debería ejecutarse en absoluto. Y, si el sistema se encuentra en un estado de infección activa, no debe considerarse de confianza. La confianza del proceso es la primera reacción ante la integridad, pero el estado general de seguridad del sistema también desempeña un papel importante.

Volvamos al concepto del mantenimiento de la productividad de los usuarios. Uno quiere impedir que los procesos que no son de confianza accedan a datos de texto sin formato y evitar que se ejecuten. Pero, por ejemplo, si se tienen abiertos dos documentos de Word – el primero con documentación importante en la que se está trabajando y el segundo un archivo enviado por un amigo o compañero – si el segundo documento resulta ser malicioso, solamente bloquearíamos el proceso del segundo documento. Permitiríamos que el usuario siguiera trabajando en el primer documento.

Si el sistema del usuario se ve gravemente infectado por uno o más programas maliciosos y está en proceso de limpiarse, Synchronized Encryption puede, como último recurso, revocar temporalmente las copias locales de las claves de cifrado. La revocación de claves garantizaría que no haya nada en el sistema que pueda descifrar ningún fichero o datos. Esto sí afecta a la productividad del usuario, ya que no puede acceder a los datos cifrados, pero realmente esa es la cuestión. ¿Queremos que un usuario (y las aplicaciones o procesos que utiliza) acceda a los datos cifrados en un sistema infectado? No. Cuando las infecciones de malware se hayan eliminado y el sistema obtenga el visto bueno, se devuelven las claves de cifrado al sistema y el usuario puede seguir trabajando productivamente.

¿Es malo un proceso que no sea de confianza?

Si un proceso no es de confianza, ¿significa que es malo? No, no necesariamente. Hay muchos casos de uso en los que se puede querer que un proceso acceda a los archivos pero solo de forma cifrada. Por ejemplo, los usuarios pueden utilizar un cliente de correo electrónico como Outlook para enviar un archivo adjunto. El cliente Outlook no es de confianza, pero puede acceder a los archivos en su forma cifrada para llevar a cabo las funciones de adjuntar y entregar. Pero una vez llega al destinatario, Outlook pide a una aplicación de confianza como Word o Excel que abra la aplicación. A los ojos del usuario final, el proceso es totalmente transparente y, al mismo tiempo, los adjuntos están cifrados y, por consiguiente, seguros durante la transmisión.

Esto también ilustra por qué el concepto de Sophos Synchronized Encryption es distinto de las listas blancas de aplicaciones. Se puede confiar en las aplicaciones incluidas en las listas blancas para que se ejecuten, pero eso no significa que deban tener acceso a los datos cifrados. Con Synchronized Encryption, lo que se hace es determinar si se confía lo suficiente en una aplicación de confianza en ejecución para que vea la versión de texto sin formato de los datos cifrados.

Synchronized Encryption sin Sophos Endpoint

Para sacar el máximo partido de Sophos Synchronized Encryption, los clientes necesitan tanto Sophos Endpoint como Sophos SafeGuard. Pero, ¿qué sucede con el concepto si Sophos Endpoint no está presente? La misma lógica sigue siendo cierta; no obstante, la validación del estado del sistema y de la confianza del proceso pasa de dinámica a estática. El producto SafeGuard no puede detectar malware, de modo que debe realizarse una evaluación diferente del estado del sistema. La confianza del proceso se basa en algo más cercano a una lista de procesos con un nombre seguro que el administrador define como de confianza. Por defecto, cualquier elemento que no aparezca en esa lista no es de confianza.

Opciones de colaboración con Next-Gen Encryption

Los usuarios finales deben colaborar, tanto dentro como fuera de una empresa, para realizar sus tareas diarias y ser productivos. Next-Gen Encryption garantiza la protección de todos los datos que hayan creado y solamente un elemento de confianza podrá acceder a ellos. ¿Cómo funciona la colaboración hoy en día? De nuevo, el principal objetivo es permitir que los usuarios se mantengan productivos y conserven sus flujos de trabajo. Veamos las dos categorías con más detalle.

Colaboración interna

De hecho, la colaboración interna es la experiencia más sencilla y fluida. Todos los usuarios dentro de la empresa tienen acceso a las claves de cifrado. Todos los datos que se crean se cifran. Se comparten en su forma cifrada y todo el mundo puede acceder a los datos.

1. **Jaime crea un documento de Word y lo guarda.** Quiere saber la opinión de Sandra. Cuando Jaime guarda el documento, este se guarda y cifra automáticamente (cifrado por defecto). Jaime no tiene que hacer nada especial para cifrar el documento de Word.
2. **Jaime abre Outlook y crea un correo electrónico** para Sandra. Siguiendo su flujo de trabajo habitual, Jaime adjunta el archivo al correo. Escribe el mensaje y lo envía. Outlook es un cliente de correo electrónico y, de manera genérica, no es de confianza. Como no se considera de confianza, no cumple con uno de los tres pilares (no es un proceso de confianza). Cuando Outlook lee el documento de Word para adjuntarlo, el archivo se adjuntará en estado cifrado.
3. **A continuación, se envía el correo a Sandra,** que lo recibe y lo abre. El archivo adjunto en el correo de la carpeta Enviados de Jaime está cifrado. El archivo adjunto en el correo de la Bandeja de entrada de Sandra está cifrado. El archivo adjunto se cifra mientras se envía de Jaime a Sandra.
4. **Sandra hace doble clic en el documento de Word** del correo y el archivo se abre sin ningún problema en Word, donde Sandra lo puede revisar y hacer comentarios. Outlook no es de confianza, así que cuando se guarda el documento en una ubicación temporal lo hará en su estado cifrado actual. A continuación, Outlook inicia Word y le pide que abra el archivo temporal que acaba de crear. Word es de confianza y dispone de acceso a la clave. Dado que Sandra es de confianza, su dispositivo es de confianza y MS Word también es de confianza, puede descifrar el documento, leerlo y presentárselo correctamente a Sandra en texto sin formato.

   Asimismo, si Sandra lee ese correo electrónico en un dispositivo móvil protegido con Sophos Mobile Control, puede guardar el adjunto cifrado en Secure WorkSpace (un contenedor cifrado) y, puesto que ese contenedor comparte la misma clave, podrá ver el contenido del documento mientras lo mantiene seguro.

Ni Jaime ni Sandra han tenido que cambiar su comportamiento habitual y todas sus interacciones han estado cifradas. Tienen una experiencia fluida y pueden colaborar sin problemas.

Colaboración externa

La colaboración externa sí cambia cuando todos los datos están cifrados. Existen dos formas de que los usuarios colaboren a nivel externo. Son las siguientes:

1. Archivo protegido por contraseña (envuelto en un archivo HTML5)
2. Archivo descifrado

Colaboración externa con un archivo descifrado

Hay casos de uso válidos para compartir datos en forma descifrada. Por ejemplo, información pública como un folleto. Al tratarse de información pública que debe ser accesible para todos, no hay ningún problema en descifrarla. El descifrado de datos es la única vez en que Next-Gen Encryption hará "acto de presencia" para el usuario. Este deberá confirmar que toma la decisión consciente de descifrar el archivo.

Un usuario tomará conscientemente la decisión de descifrar el archivo antes de que se envíe. Después, como se ha mencionado antes, el archivo puede, opcionalmente, pasar por la DLP para analizar su contenido y, si no se generan alertas, se descifra el archivo. Además, el cifrado, o en este caso el descifrado, es persistente de modo que permanecerá así. Toda esta actividad se registra y audita para que el administrador pueda monitorizar los comportamientos maliciosos de los empleados. Una vez se descifra el archivo, puede retomarse el flujo de trabajo normal del usuario.

Colaboración externa con un archivo protegido por contraseña

¿Qué pasa si tiene un contrato que quiere compartir de forma segura con un destinatario externo pero debe permitirle descifrarlo y usarlo sin saber si tiene instalado algún software de cifrado?

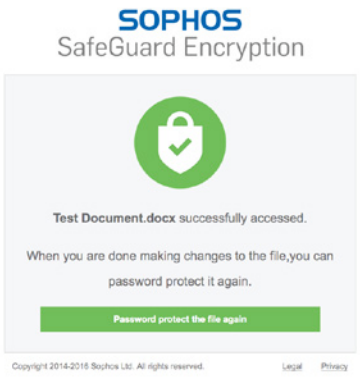
Basta con que el usuario cree un archivo protegido por contraseña y defina una contraseña. En esencia, el software vuelve a cifrar el archivo del documento del contrato (llamémosle contrato.doc) con la contraseña que ha asignado el usuario y lo coloca en un envoltorio HTML5. Así se crea un archivo llamado contrato.html. La contraseña tendrá que compartirse con el destinatario. El resultado es un solo archivo HTML que cualquier sistema operativo o navegador compatible con HTML5 puede interpretar. Ese archivo HTML consta de tres partes bien diferenciadas:

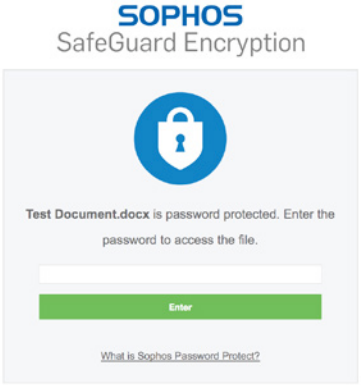
1. La capa de presentación (lo que verá el destinatario en su navegador web cuando abra el archivo)
2. El código para descifrar la carga adjunta
3. El archivo cifrado (contrato.doc en este ejemplo)

El usuario enviará por correo al destinatario el archivo contrato.html en lugar del archivo contrato.doc. Cuando el destinatario haga doble clic en el archivo HTML en su cliente de correo, se abrirá el navegador y le pedirá la contraseña. Partiendo del hecho de que introduzca la contraseña correctamente, el navegador ejecutará el código para descifrar el archivo y, a continuación, se guardará localmente en el equipo del destinatario en una forma descifrada.

Esto permite enviar el archivo confidencial en un modo cifrado y, posteriormente, que se descifre sin problemas cuando el destinatario lo abra.

Si el destinatario necesita devolver un archivo actualizado, el envoltorio HTML también puede usarse como contenedor. El destinatario solo tiene que actualizar el archivo y volver a colocar el archivo actualizado en la pantalla HTML. Así se crea una colaboración segura en dos sentidos con un usuario externo que no disponga de Sophos SafeGuard Encryption.





Hacer la vida más fácil a sus usuarios

Para facilitar la vida de sus usuarios, Sophos ofrece elementos, como un complemento de Outlook, que pueden detectar que se está enviando correo fuera de la organización con un archivo adjunto. Puede informar al usuario de que está a punto de enviar un archivo cifrado y preguntarle qué opciones quiere elegir para la colaboración externa e indicarle las medidas adecuadas que tomar. Otra posibilidad es que un administrador especifique una acción predeterminada, a través de una política, que se realizaría de forma automática.

Acceso a datos en múltiples plataformas

Para permitir que los usuarios finales se mantengan productivos, la funcionalidad de Next-Gen Encryption debe ejecutarse en todos los dispositivos de uso habitual entre los usuarios. Esta funcionalidad funciona en Windows, OS X, iOS y Android.

Antes hemos mencionado que los usuarios tienen una media de tres dispositivos. Si el equipo Windows se ve gravemente infectado por un programa malicioso, se bloquea y pasa a considerarse de no confianza, el usuario puede seguir trabajando y mantenerse productivo con su Mac o iPad, independientemente de si está en la oficina o fuera de ella. Si un dispositivo se ve afectado es inoportuno, pero el usuario puede simplemente utilizar otro dispositivo.

Protección de datos y contra amenazas de última generación

Con Sophos, los clientes pueden conseguir una seguridad aún mejor al combinar Next-Gen Encryption con nuestra oferta más amplia de seguridad sincronizada. Si un cliente tiene Sophos Endpoint, Sophos UTM/Firewall y Sophos SafeGuard, los tres productos trabajarán de forma conjunta no solo para ofrecer una fantástica solución que detecte y elimine las amenazas con mayor eficacia, sino también para asegurarse de que las amenazas no puedan acceder a los datos cifrados. Es la protección de última generación para su empresa.

Conclusión

Next-Gen Encryption cambia el paradigma de la protección de datos. El cifrado siempre activo, a diferencia del cifrado tradicional de archivos y carpetas, permite que los usuarios finales se libren de tener que decidir qué es importante y qué debe cifrarse. En consecuencia, se le facilita la vida al usuario al cifrar y descifrar archivos de forma transparente y automática sin afectar a su flujo de trabajo. Para proteger los datos contra las amenazas, Synchronized Encryption revoca las claves de los sistemas infectados y deniega el acceso a las aplicaciones maliciosas o que no son de confianza. Todo ello garantiza que se mantenga la productividad del usuario al tiempo que sus datos, y su organización, están seguros.

Más de 100 millones de usuarios en 150 países confían en Sophos para obtener la mejor protección contra amenazas complejas y fugas de datos. Nuestro objetivo es ofrecer soluciones de seguridad completa fáciles de desplegar, administrar y utilizar con el coste total de propiedad más bajo del sector. Sophos ofrece soluciones galardonadas de cifrado y protección para estaciones, web, correo electrónico, móviles, servidores y redes con el respaldo de SophosLabs, nuestra red de centros de investigación de amenazas. Infórmese mejor en www.sophos.com/es-es/products.

Ventas en España:
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

2016-08-1 WP-ES (NP)