ENCRIPTACIÓN POR SOFTWARE Y CUMPLIMIENTO DE LA REGULACIÓN: UNA SOLUCIÓN MENOS COSTOSA CON MAYORES RIESGOS DE SEGURIDAD

REQUERIMIENTOS REGULATORIOS Y DE CUMPLIMIENTO

La seguridad de la información solía estar relegada únicamente a los departamentos de TI, pero debido a las continuas violaciones de datos de los consumidores, los gobiernos de todo el mundo han impuesto cada vez más requisitos a las empresas para que encripten y protejan todos los datos que sean personalmente identificables.

Desde la HIPAA en la atención médica, hasta el GDPR en la EMEA y la CCPA en California, el encriptado de las clases de datos protegidos se está exigiendo a través de regulaciones. Las organizaciones de cumplimiento se han multiplicado exponencialmente en los últimos 3+ años, ya que estas regulaciones y sus multas asociadas y los riesgos de adjudicación legal se han disparado.

Con estos cambios, los departamentos de TI han hecho lo posible por mantenerse al día con la seguridad y el aumento de los costes. A causa de la pandemia de COVID, los presupuestos se están gastando en inversiones adicionales en hardware y firewalls, a expensas de centrarse en el encriptado de datos.

De hecho, el encriptado de software mediante Microsoft BitLocker® o el software de administración de endpoint (punto final) de empresas como Symantec, McAfee y otras está en auge. Algunas empresas y consumidores también utilizan dispositivos USB estándar con unidades de "bóveda" de software que proporcionan algunos proveedores.

ENCRIPTACIÓN Y DATOS EN TRÁNSITO

Los empleados y los consumidores tienen la necesidad de llevar su información consigo. Tienen opciones como el uso de:

1. Servicios en la nube: Lo cual es excelente, ya que se puede acceder a ellos desde cualquier dispositivo que pueda conectarse a Internet. Sin embargo, la flexibilidad tiene su precio. El almacenamiento de datos en la nube elimina el control de los datos por parte del usuario o de la empresa y tiene un riesgo potencial, ya que hemos visto que los servidores de nube se han dejado sin bloquear o han sido accedidos.
2. Dispositivos USB estándar: Aunque llevar un dispositivo USB parece más seguro, el riesgo de que los datos queden expuestos por la pérdida del dispositivo puede ser importante. Por ejemplo, abundan las historias de dispositivos USB perdidos que se encuentran con información secreta o de lavanderías con cajones llenos de dispositivos USB perdidos.
3. Dispositivos USB con encriptación por hardware: Estos dispositivos USB tienen arquitecturas personalizadas que incorporan un controlador de encriptación y control de acceso. La información está encriptada utilizando la encriptación general más fuerte AES-256 bits en el modo XTS, junto con otras posibles protecciones para mitigar los ataques físicos y basados en el firmware. Estos dispositivos son fabricados por empresas especializadas en dispositivos de seguridad y, aunque son más caros que los dispositivos USB estándar, ofrecen una mayor seguridad de los datos. Los dispositivos FIPS 197 o FIPS 140-2 de nivel 3 pueden agregar mayores niveles de protección y tranquilidad.
4. Dispositivos USB estándar con encriptación por software: Para garantizar la seguridad exigida por la normativa, se puede utilizar el cifrado por software con BitLocker u otras herramientas; son opciones decentes, ya que son relativamente baratas y ofrecen el mismo cifrado AES-256 XTS.

No es de extrañar que, en la mayoría de los casos, las empresas e industrias se inclinen por la opción 4, utilizando dispositivos USB estándar con encriptado por software, principalmente porque el encriptado por software como BitLocker u otras utilidades de bóveda de datos son "gratuitas."

LA ENCRIPTACIÓN DEL SOFTWARE NO CUMPLE CON LA NORMATIVA

Para un profesional de la seguridad empresarial, el encriptado por software puede ofrecer exactamente las mismas capacidades de encriptación que los dispositivos USB encriptados por hardware más caros. ¿Pero es el camino a seguir? El presupuesto es escaso, por lo que las empresas se deciden por el encriptamiento por software con fines de cumplimiento, sin ser conscientes del lado oscuro del encriptamiento basado en software.

¿Cuál es el problema del dispositivo USB encriptado por software? ¿La información en reposo y en tránsito no está encriptada en AES-256 XTS? En general, si lo está. El problema es que: El encriptamiento por software se considera "encriptamiento removible".

Espere - ¿removible? ¿Significa esto que un dispositivo USB encriptado por software puede tener su encriptación desactivada por un usuario?

La respuesta es: sí. Los usuarios pueden eliminar la función de encriptación por software de sus dispositivos USB. ¿Por qué lo harían, se preguntará? Porque pueden - y porque simplemente quieren acceder a los archivos sin usar una contraseña, o simplemente han olvidado la contraseña pero necesitan usar el dispositivo USB.

CÓMO ELIMINAR EL ENCRIPTADO POR SOFTWARE DE UN DISPOSITIVO USB ENCRIPTADO

Para un usuario que no quiera ocuparse de introducir contraseñas complejas o de otro tipo para acceder a sus datos, el proceso es sencillo:

1. Conecte el dispositivo encriptado por software a una computadora
2. Formatee el dispositivo
3. Después de formatear el dispositivo, se elimina todo el encriptado
4. Copie los archivos con información secreta o confidencial en el dispositivo para facilitar el acceso

Esto es fácil de hacer para los usuarios utilizando una computadora que no está restringida - Los departamentos de TI han restringido el uso de los comandos de formato en las computadoras de la empresa, pero esto se puede hacer en cualquier otra computadora que no sea de la empresa.

A efectos de cumplimiento - la facilidad para eliminar el encriptado de datos significa que el dispositivo proporcionado por la empresa está ahora sin encriptar, aunque los datos que estaban encriptados en el dispositivo se consideran perdidos para siempre una vez que se elimina el encriptado mediante el método anterior (las claves de encriptado están vinculadas a los datos). Cualquier dato copiado en el dispositivo una vez eliminado el encriptado se considera inseguro y potencialmente fuera de conformidad, lo que puede suponer una violación de las regulaciones de HIPAA, GDPR, CCPA, y muchas otras.

LAS CONSECUENCIAS DE LAS PÉRDIDAS DE DISPOSITIVOS SIN ENCRIPTAR

Si un dispositivo USB designado por la empresa se pierde y se encuentra, incluso si la empresa no es consciente al principio, pero se entera más tarde a través de los medios de comunicación social, los requisitos especiales de conformidad entran en vigor para la empresa, lo que posiblemente les obliga a:

1. Realizar una investigación forense para identificar qué información se perdió
2. Determinar si se ha producido un incumplimiento legal, en consulta con el Departamento Jurídico
3. Determinar si los clientes deben ser notificados

Aquí es donde la pérdida de un solo dispositivo USB puede salir muy caro. Con tarifas legales que superan los cientos de dólares por hora, este proceso de cumplimiento puede suponer miles y miles de dólares en gastos, además de posibles multas, demandas de clientes y otros, y la vergüenza de la exposición de la información.

Cuando se considera el encriptamiento por software por su bajo coste de implementación, no se tienen en cuenta estos riesgos y sus enormes consecuencias financieras.

Hay otro riesgo en permitir el uso de dispositivos USB sin encriptar en la red de la empresa. Se le conoce comúnmente como "BadUSB". BadUSB es una clase de malware que ha sido utilizada por actores maliciosos para violar el firewall de una empresa e introducir malware en las ciberdefensas de una empresa a través de dispositivos de almacenamiento USB.

BadUSB

Cuando se conecta un dispositivo USB a una computadora, el controlador del conjunto de chips de la computadora inicia un intercambio de información con el controlador de dispositivo USB a través del firmware. Este intercambio se produce antes de que el sistema operativo, como Microsoft/macOS/Linux, sea consciente de que se ha conectado un dispositivo USB. Todos los dispositivos USB tienen un firmware que se ejecuta cuando el dispositivo se conecta a un puerto USB.

Los agentes maliciosos han aprendido que pueden introducir malware a través de este mecanismo de intercambio de información sustituyendo el firmware que se ejecuta en la unidad USB por otro malicioso que inyecta malware en el sistema informático de destino mientras se comunica con el dispositivo USB. Un dispositivo USB estándar no tiene seguridad en su firmware interno que es ejecutado por su controlador, por lo que BadUSB nació como un arma cuando las buenas unidades USB para penetrar los firewalls y romper las defensas cibernéticas.

Muchas compañías intentan prohibir el uso de dispositivos USB en sus sistemas, o incluso llegan a rellenar los puertos USB con epoxi. Sin embargo, descubrieron que algunas clases de empleados necesitan llevar la información consigo en unidades USB. Por ejemplo, los ejecutivos quieren llevarse la información para trabajar en ella o proporcionarla a asesores legales o financieros externos que no están en la nube de la empresa; los contratistas de la empresa que necesitan información para trabajar, pero con acceso restringido a las bases de datos de la empresa; los analistas financieros que se están apresurando a cerrar los informes mensuales y necesitan trabajar en hojas de cálculo en casa.

Como se desprende del análisis anterior, existe un riesgo importante al utilizar esta solución estándar de dispositivo USB + software de encriptación. A primera vista, lo que parecía más barato resulta ser potencialmente muy dañino y mucho más caro. Sólo el coste de 2 o 3 horas de consulta con un abogado acerca de una posible violación de datos anula cualquier ahorro derivado del uso de la solución más barata.

LOS DISPOSITIVOS USB ENCRIPTADOS POR HARDWARE SON LA MEJOR OPCIÓN PARA EL CUMPLIMIENTO DE LA REGULACIÓN

Que hace que los dispositivos USB encriptados por hardware sean la mejor opción para estas aplicaciones reguladoras:

1. Los dispositivos USB encriptados por hardware tienen una encriptación que siempre está ACTIVADA: No hay forma de que los usuarios desactiven la encriptación, restablezcan las reglas de la contraseña (longitud mínima, complejidad) y desactiven los reintentos automáticos de la contraseña. A diferencia de la encriptación por software, que no impide que se adivinen las contraseñas repetidamente mediante ataques de software de diccionario, las versiones de hardware limitan los reintentos de contraseñas y bloquean los datos cuando se introducen contraseñas erróneas 10 veces o incluso menos. Esto es muy seguro en la era de las supercomputadoras.
2. Los dispositivos cifrados por hardware utilizan controladores de encriptación de primera calidad e incorporan numerosas funciones de seguridad: Aunque no siempre revelamos todas las contramedidas de seguridad, existe una contramedida para protegerse de BadUSB. En la fábrica, cuando el firmware se carga solamente en dispositivos encriptados por hardware, el firmware se firma y se carga digitalmente. Esto significa que, cuando se conectan estos USB encriptados, el controlador de encriptación comprueba primero la integridad del firmware a través de la firma digital, y sólo lo carga si supera la verificación. Cualquier intento de reemplazar el firmware bloqueará el dispositivo y este dejará de ser funcional, y este ya no supondrá una amenaza.
3. Los dispositivos USB encriptados por hardware pueden tener identificadores de producto (PID) personalizados para una empresa concreta: Estos dispositivos de primera calidad pueden tener un identificador digital programado para que, si un dispositivo se conecta al firewall interno o externo de la empresa, el dispositivo pueda ser identificado como un dispositivo emitido por la empresa. Por ejemplo, si un empleado pierde el dispositivo de la empresa y compra el mismo modelo en una tienda, el dispositivo recién adquirido no se validará en la red de la empresa. Esta personalización añade otra capa de seguridad al uso de los dispositivos USB.
4. Los dispositivos encriptados por hardware ahorran dinero muy rápidamente: La mera reducción y eliminación de riesgos hace que el ciclo de amortización sea muy corto.

Kingston es el mayor fabricante del mundo de dispositivos USB encriptados y ofrece familias de dispositivos con diversas características y precios. Póngase en contacto con Kingston directamente para hablar de cómo podemos ayudarle a cumplir con las soluciones de USB encriptado para ejecutivos, empleados, contratistas y más.

 MKF-956LATAM