CIFRADO BASADO EN SOFTWARE Y CUMPLIMIENTO NORMATIVO: SOLUCIÓN MÁS ECONÓMICA CON MAYORES RIESGOS DE SEGURIDAD

REQUISITOS LEGALES Y CUMPLIMIENTO NORMATIVO

La protección de los datos era un tema que solía quedar relegado exclusivamente a los departamentos de TI, aunque debido a las numerosas vulneraciones de datos de los consumidores, los gobiernos de todo el mundo han impuesto a las organizaciones cada vez más requisitos de cifrar y proteger todos los datos que puedan identificar a las personas.

Desde la HIPAA en el sector sanitario de EE.UU. hasta el RGPD en la UE y la CCPA, la legislación impone el cifrado de categorías de datos protegidos mediante instrumentos legales. Los departamentos de cumplimiento normativo se han multiplicado exponencialmente en los últimos 3 años, por cuanto las normativas, conjuntamente con las multas asociadas y los riesgos de sentencias judiciales, se han disparado.

Con estos cambios, los departamentos de TI se han esforzado por mantenerse al día con la seguridad y el incremento de costes. Durante la pandemia de la COVID, los presupuestos se han gastado en inversiones adicionales en hardware y cortafuegos, a expensas de concentrarse en el cifrado de los datos.

De hecho, sigue en aumento el cifrado basado en software utilizando Microsoft BitLocker® o software de administración de terminales de empresas como Symantec, McAfee y otros. Además, algunas empresas y particulares utilizan unidades USB normales con "cámara de seguridad" que suministran algunos proveedores.

CIFRADO Y DATOS EN TRÁNSITO

Los empleados y consumidores tienen necesidad de llevarse sus datos consigo. Para ello tienen diversas opciones, como usar:

1. Servicios en la nube: Que son excelentes, ya que es posible acceder a los mismos desde cualquier dispositivo que pueda conectarse a Internet. Sin embargo, esta flexibilidad tiene un precio. El almacenamiento de los datos en las nubes, el particular o la empresa dejan de controlarlos, y existe el potencial riesgo de que los servidores en la nube queden abiertos y sea posible acceder a los mismos
2. Unidades USB estándar: Aunque portar una unidad USB parece más seguro, el riesgo de que los datos queden expuestos en caso de perderla puede ser significativo. Por ejemplo, abundan las historias sobre unidades USB extraviadas, halladas con información secreta, o lavanderías con cajones llenos de estos dispositivos.
3. Unidades USB con cifrado por hardware: Estas unidades USB tienen arquitecturas personalizadas que incorporan un controlador de cifrado interno y control de acceso. En general, los datos son cifrados utilizando el potente cifrado AES de 256 bits en modo XTS, además de otras posibles salvaguardas para mitigar los ataques físicos y basados en firmware. Estas unidades son fabricadas por empresas que se especializan en dispositivos de seguridad que, aunque son más caros que las unidades USB estándar, ofrecen una mejor protección de los datos. Los dispositivos con homologación FIPS 197 o FIPS 140-2 de Nivel 3 pueden aportar mayores grados de protección y una tranquilidad que no tiene precio.
4. Unidades USB estándar con cifrado basado en software: A efectos de implementar las medidas de seguridad exigidas por la normativa, es posible utilizar el cifrado basado en software con BitLocker u otras herramientas. Se trata de opciones adecuadas, son relativamente económicas y ofrecen el mismo cifrado AES de 256 bits en modo XTS.

No es de sorprender que, en la mayoría de los casos, las empresas tienden a adoptar la opción 4, unidades USB estándar con cifrado basado en software, sobre todo porque el cifrado por software, como BitLocker u otras utilidades de protección de datos, son "gratuitos".

EL CIFRADO POR SOFTWARE NO CUMPLE LA NORMATIVA

Para un profesional de seguridad, el cifrado por software puede ofrecer exactamente las mismas capacidad de cifrado que las unidades USB con cifrado por hardware, más caras. Sin embargo, ¿esto es conveniente? Los presupuestos suelen ser ajustados, por lo cual las empresas apuestan por el cifrado por software a efectos de cumplimiento normativo, pero desconocen el lado oscuro de este método.

¿Cuál es el problema de las unidades USB con cifrado basado en software? ¿Los datos en reposo y los datos en tránsito no se cifran en XTS-AES de 256 bits? En general, sí. El problema es el siguiente: el cifrado por software se considera "cifrado extraíble".

¿Perdón? ¿Extraíble? ¿Eso quiere decir que un usuario puede desactivar el cifrado de una unidad USB con cifrado basado en software?

La respuesta es: sí. Los usuarios pueden quitar la función de cifrado por software de sus unidades USB. ¿Y por qué lo harían?, se preguntará usted. Porque pueden. Y porque querrían acceder a los archivos sin utilizar una contraseña, o sencillamente porque olvidaron la contraseña, pero necesitan utilizar la unidad USB.

CÓMO QUITAR EL CIFRADO POR SOFTWARE DE UNA UNIDAD USB CIFRADA

Para el usuario que no desea tener que vérselas con la introducción de contraseñas complejas o de otra índole para acceder a los datos, el proceso es muy sencillo:

1. Conecte la unidad con cifrado de software a un ordenador
2. Formatee la unidad
3. Una vez formateada, el cifrado quedará eliminado
4. Copie los archivos con información secreta o confidencial a la unidad para un fácil acceso

Es fácil para los usuarios hacerlo con un ordenador que no esté restringido. Los departamentos de TI han restringido el uso de comandos de formateo en los equipos de la empresa, pero esto puede hacerse en cualquier otro ordenador que no sea de la empresa.

A efectos de cumplimiento normativo, la facilidad para eliminar el cifrado implica que la unidad facilitada por la empresa queda desprotegida. No obstante, los datos que estaban cifrados en la unidad se consideran perdidos para siempre una vez eliminado el cifrado con el método explicado (las clave de cifrado están vinculadas a los datos). Todos los datos copiados en el dispositivo una vez retirado el cifrado se consideran desprotegidos y, potencialmente, en riesgo de incumplir la normativa, establecida por instrumentos como la HIPAA, el RGPD, la CCPA y muchos otros.

LAS CONSECUENCIAS DE PERDER UNIDADES NO CIFRADAS

Si una unidad USB de una empresa se extravía y es hallada, incluso si al principio la entidad no lo sabe pero llega a su conocimiento a través de las redes sociales, debe implementar una serie de requisitos especiales de cumplimiento normativo, que posiblemente requiera que:

1. Efectúe una investigación forense para identificar qué datos se perdieron
2. Determine si se ha producido una vulneración legal, en consultas con su Departamento Jurídico
3. Determine si los clientes deben ser notificados

Es justamente por eso que cuando una única unidad USB se pierde, puede resultar muy caro. Con honorarios de abogados superiores a varios centenares de dólares por hora, este proceso de cumplimiento puede conllevar gastos por muchos centenares de miles, además de las potenciales multas, demandas de parte de clientes y otras, y la vergüenza de ver los datos públicamente expuestos.

Cuando se considera el bajo coste de implementación del cifrado por software no suelen considerarse estos riesgos ni sus enormes consecuencias financieras.

Existe otro riesgo en permitir el uso de unidades USB cifradas en una empresa. Normalmente se denomina "BadUSB", o USB malicioso. BadUSB es un tipo de malware utilizado para traspasar los cortafuegos de una entidad e introducir malware en sus ciberdefensas mediante dispositivos de almacenamiento USB.

USB malicioso

Cuando se inserta una unidad USB en un ordenador, el controlador de conjuntos de chips del mismo ejecuta un protocolo de señales con el controlador de dicha unidad a través del firmware. Este intercambio se produce antes de que el sistema operativo, como Microsoft/macOS/Linux, incluso tengan conocimiento de que se ha conectado una unidad USB. Toda unidad USB tiene un firmware que se ejecuta al insertarla en un puerto USB.

Los usuarios maliciosos han aprendido que pueden introducir malware mediante este mecanismo de protocolo de intercambio sustituyendo el firmware que se ejecuta en la unidad USB por otro firmware, más malicioso, que se introduce en el sistema informático de destino al comunicase con la unidad USB. Una unidad USB estándar no tiene protección en el firmware interno que ejecuta su controlador, por lo cual las USB maliciosas empezaron como unidades USB normales que se contaminaron para penetrar los cortafuegos y vulnerar las ciberdefensas.

Muchas organizaciones intentan prohibir el uso de unidades USB en sus sistemas, e incluso llegan tan lejos como taponar los puertos USB de los ordenadores con epóxido. Sin embargo, siempre existen categorías de empleados que tienen que portar los datos consigo en unidades USB. Por ejemplo, los ejecutivos que se llevan datos consigo para trabajar, o los asesores jurídicos o financieros externos que no están conectados a la nube de la entidad; contratistas externos que necesitan datos para trabajar, pero con acceso restringido a las bases de datos de la empresa; analistas financieros ajetreados por cerrar los informes mensuales y necesitan trabajar con hojas de cálculo en casa.

Como lo demuestran análisis anteriores, existen significativos riesgos en el uso de la solución de unidades USB estándar + cifrado por software. A primera vista, lo que aparentemente era más económico tiene el potencial de ser tremendamente perjudicial y muchísimo más caro. Solamente el coste de 2-3 horas de asesoramiento con un abogado acerca de las potenciales consecuencias de una vulneración de datos cubre el ahorro de utilizar la solución más barata.

LAS UNIDADES USB CON CIFRADO POR HARDWARE SON LA MEJOR OPCIÓN PARA EL CUMPLIMIENTO NORMATIVO

Por qué las unidades USB con cifrado por hardware son la mejor opción para cumplir los requisitos normativos:

1. En las unidades USB con cifrado por hardware, el cifrado está SIEMPRE activado: no existe manera para que los usuarios desactiven el cifrado, modifiquen las reglas de contraseña (longitud mínima, complejidad) y supriman la limitación de introducción de contraseñas erróneas A diferencia del cifrado por software, que no impiden repetidos intentos de adivinar la contraseña mediante ataques de diccionario, las versiones de hardware limitan los reintentos de contraseña, y bloquean los datos si se introducen contraseñas erróneas 10 veces, o incluso menos. En esta era de superordenadores, se trata de una medida muy segura.
2. Las unidades de cifrado basado en hardware utilizan los más avanzados controladores de cifrado e incorporan numerosas funciones de protección: Aunque no siempre desvelamos todas las contramedidas de seguridad, existe una que protege contra las USB maliciosas. En fábrica, cuando se carga el firmware solamente en las unidades con cifrado por hardware, el firmware se firma digitalmente y se carga. Esto implica que, al insertar estas USB cifradas en un equipo, el controlador de cifrado primero verifica la integridad del firmware mediante la firma digital, y solamente se carga si pasa dicha verificación. Todo intento de sustituir el firmware bloqueará la unidad, que dejará de estar funcional y, por consiguiente, de suponer una amenaza.
3. Las unidades USB con cifrado por hardware pueden tener ID de producto (PID) establecidos para una organización específica: Estas unidades pueden tener programadas en ellas un identificador digital, de tal modo que, si se insertan en el cortafuegos interno o externo de una organización, pueda ser identificada como propia. Por ejemplo, si un empleado pierde la unidad que la empresa le facilitó y compra el mismo modelo en una tienda, la unidad recientemente adquirida no será validada por la red de la organización. Esta personalización incorpora otra capa más de protección en el uso de las unidades USB
4. Las unidades con cifrado por hardware permiten ahorrar dinero muy rápidamente. Con solamente reducir y eliminar los riesgos, el ciclo de amortización es muy breve.

Kingston es el mayor fabricante mundial de unidades USB cifradas, y ofrece series con diversas características, funciones y niveles de precios. Póngase en contacto con Kingston y le explicaremos cómo puede seguir cumpliendo los requisitos normativos con soluciones de USB cifradas para ejecutivos, empleados, contratistas, etc.