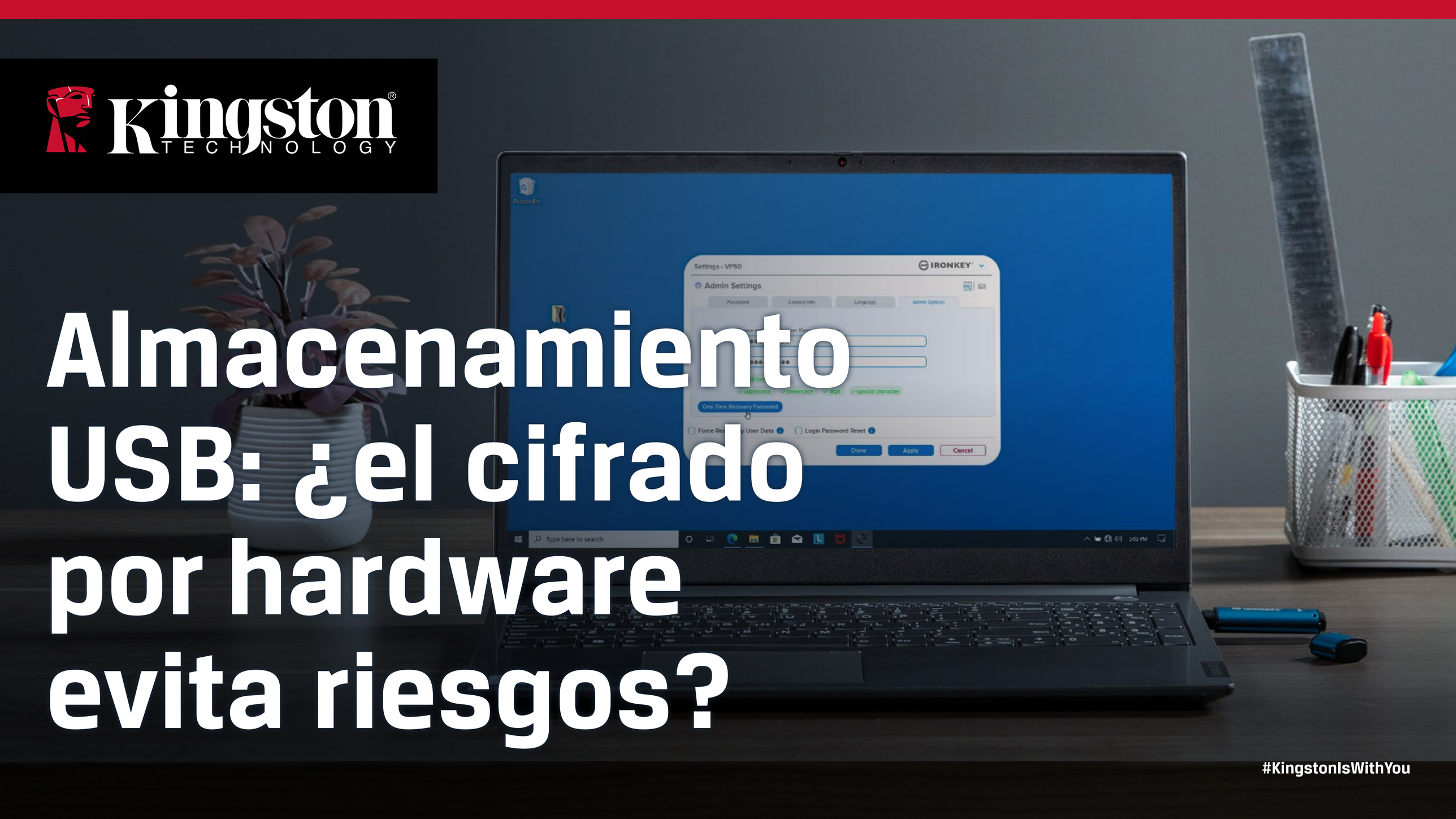
Almacenamiento USB: ¿el cifrado por hardware evita riesgos?



#KingstonIsWithYou

Almacenamiento USB: ¿el cifrado por hardware evita riesgos?

Prólogo y contenido

La ciberseguridad preocupa hoy a las empresas mucho más que antes, aunque demasiadas organizaciones carecen de información adecuada y no están preparadas para hacer frente a las amenazas. En Estados Unidos, solamente el 50% de las empresas tienen implementado un plan de ciberseguridad. De ellas, el 32% no ha actualizado sus planes desde el comienzo de la pandemia de la COVID-19, cuando tantas organizaciones se pasaron a modelos de trabajo remoto o híbrido, según UpCity. Y la frecuencia de los ciberataques se incrementa continuamente a nivel global: el número de empresas afectadas por ataques de ransomware ha aumentado desde el 37% en 2020 al 66% en 2021[1].

La ciberseguridad en riesgo puede tener efectos devastadores para una empresa: además del costo monetario de los ciberataques, la pérdida de datos, la seguridad y la reputación pueden perjudicar a las organizaciones de muchas maneras, tanto a corto como a largo plazo.

Un vehículo habitual de las amenazas contra la ciberseguridad son las unidades USB. Son dispositivos que han llegado a ser ubicuos en muchas organizaciones por su sencillez: solamente insertarlos en un equipo y ya están listos para usar. Sin embargo, es precisamente su simplicidad la que los hace tan vulnerables a los ataques: basta con una unidad extraviada o robada para que algún protagonista malicioso pueda tener acceso a datos sensibles. Aquí es donde el cifrado puede jugar un papel significativo, convirtiendo a las unidades USB en dispositivos de uso seguro y mitigando los consiguientes riesgos para personas y organizaciones. En este libro electrónico intentaremos responder a los siguientes interrogantes básicos:

- Por qué las unidades USB cifradas son tan fundamentales para protegernos de los ciberataques
- Cuáles son los puntos en que se hacen vulnerables las organizaciones
- Qué pueden hacer para protegerse

Índice	Páginas

Almacenamiento USB: ¿el cifrado por hardware evita riesgos?

Colaboradores

Este libro electrónico ha sido creado con la colaboración de importantes especialistas en TI y en tecnologías emergentes, conjuntamente con nuestros propios expertos.

David Clarke

David está considerado uno de los 10 principales influentes según la lista "30 principales líderes de pensamiento y pensadores sobre redes sociales, gestión de riesgos, cumplimiento normativo y tecnología regulatoria más influyentes del Reino Unido" de Thompson Reuter, y en la lista de 30 principales expertos globales de Kingston Technology.

Pasi Siukonen

Pasi es responsable de un equipo de expertos que apoyan a diversos departamentos de Kingston, como RR.PP., Marketing, Ventas de campo, Asistencia técnica y Atención al cliente. Está centrado principalmente en las líneas de productos Flash y SSD.

La diferencia entre las unidades del montón y las unidades cifradas

Mientras que a las unidades del montón (no cifradas) resulta extremadamente fácil acceder y utilizar, el cifrado por hardware inserta diversas capas de protección —tanto físicas como digitales— que convierten al almacenamiento en USB en extremadamente seguro. La fácil disponibilidad, el bajo coste y la portabilidad de las unidades del montón no cifradas implica que, aunque resultan muy cómodas para el usuario, también lo son para los actores maliciosos que pretenden robar datos sensibles, insertar malware o ransomware en las redes de una organización, y cosas todavía peores. Como las unidades USB se utilizan con tanta frecuencia, las oportunidades de ciberataques se multiplican exponencialmente. Las unidades del montón conllevan dos riesgos fundamentales:

- **Ataques de ransomware:** estos ataques basados en las USB consisten en inyectar malware en las redes de las organizaciones, secuestrando sus datos y/o sistemas cifrándolos, y pedir un rescate por su liberación. Normalmente, son causados por BadUSB y se han convertido en el tipo de software malicioso más habitual.
- **Robo de datos:** todo lo que hace falta es una unidad extraviada, robada o desatendida, carente de las medidas de protección adecuadas, para que un actor malicioso acceda fácilmente a los datos almacenados en la misma, tanto si se trata de información de clientes como de códigos fuentes o datos financieros o comerciales sensibles.

BadUSB: se trata de un ataque que puede aprovecharse de la vulnerabilidad de las unidades USB con firmware desprotegido, que pueden entonces programarse con software malicioso. Estas herramientas maliciosas son increíblemente habituales y fácilmente disponibles para los ciberdelincuentes, aunque debido a que existe una mínima concienciación sobre su existencia, los ataques con las mismas resultan demasiado fáciles, como por ejemplo sustituyendo el firmware de una unidad del montón por firmware pirateado y utilizando la unidad como reflejo del teclado y, básicamente, ejecutar secuencias de comandos para atacar el cortafuegos. Dado que tantos ciberataques se ejecutan a través de usuarios internos, con o sin malas intenciones, es de fundamental importancia que las organizaciones utilicen unidades cifradas que incorporen firmware protegido con firma digital para evitarlos, lo cual puede reducir las probabilidades de éxito de los ciberdelincuentes.

> **El coste de reconstruir una infraestructura, e incluso de pagar un rescate u otras extorsiones, es abrumador, en comparación con el coste de unidades USB administradas. - David Clarke**

¿Por qué utilizar unidades USB cifradas?

Las unidades cifradas han sido específicamente diseñadas para proteger los datos que contienen, así como a los dispositivos a los cuales sean conectadas, lo cual las convierte en herramientas valiosas del arsenal informático de cualquier organización. A medida que las amenazas de ciberseguridad han ido ganando en sofisticación, las funciones de las unidades cifradas han hecho lo propio, con lo cual van por delante de los ciberdelincuentes que pretenden aprovecharse de estos dispositivos. Como ya hemos visto en la línea de productos cifrados por hardware Kingston IronKey™, con el transcurso del tiempo se han desarrollado funciones tales como el cifrado AES de 256 en el modo XTS más potente, resistentes carcasas inmunes a la manipulación, firmware firmado digitalmente, modos de contraseña compleja o frase de contraseña para garantizar que los usuarios estén bien y debidamente protegidos contra todo tipo de ataques.

Como normalmente los ciberriesgos no son un tema muy comprendido, muchas organizaciones pueden optar por las unidades del montón, a pesar de las diversas vulnerabilidades que conllevan. Su fácil disponibilidad, su bajo coste y su uso de cifrado por software juegan aquí un papel importante, al igual que la ausencia de un proceso de aprobación corporativo de unidades Flash. Las más de las veces no existen políticas o procesos de buenas prácticas que obliguen a cumplir diversas normas informáticas y de seguridad, como ISO27001, RGPD, SOC2 y WISP. En consecuencia, estos riesgos suelen evaluarse sobre la base de opiniones, en lugar de pruebas, con lo cual muchas organizaciones quedan vulnerables a ataques.

Si bien algunos pueden utilizar unidades del montón con las actuales herramientas de cifrado por software, esta suele ser una medida de falsa economía, ya que muchas unidades cifradas por software pueden ser pirateadas con herramientas gratuitas o de pago disponibles en Internet. Además, el cifrado por software puede ser eliminado por el usuario con un simple reformateo de la unidad, simplemente para manejarla de manera más sencilla o para utilizarla en plataformas de sistemas operativos incompatibles. Por su parte, las unidades USB de cifrado por hardware mantienen siempre un cifrado que no puede desactivarse. Incorporan a su diseño carcasas resistentes a las manipulaciones que dejan en evidencia cualquier intento de intrusismo, así como firmware firmado digitalmente que garantiza la autenticidad e integridad de la unidad. La limitación de los intentos de introducción de contraseña (protección contra ataques de fuerza bruta) y los teclados virtuales (protección contra grabación de pulsaciones de teclado y de pantalla) son otras dos funciones que caracterizan a las unidades cifradas como IronKey VP50. De este modo, son compatibles con las buenas prácticas del sector e impiden a los piratas extraer contraseñas de usuarios inocentes.

> Si la unidad IronKey detecta que el firmware ha sido manipulado, bloqueará la unidad e impedirá su arranque, reforzando así la ciberseguridad.
> - Pasi Siukonen

¿Quiénes están en riesgo?

Lo cierto es que las que están en riesgo son las organizaciones incapaces de controlar el acceso a sus USB. Y, a menudo, desconocen exactamente cuáles son dichos riesgos. Sin embargo, existen factores que pueden hacer que determinadas organizaciones sean objetivos más atractivos —y vulnerables— a los ciberataques.

En el caso de las organizaciones de los sectores sanitario y financiero, no solamente que sus datos son mucho más atractivos para los ciberdelincuentes, sino que además las afectan, a ellas y a sus clientes, de maneras más graves. En el Reino Unido, un ciberataque que se produjo en 2017 contra el NHS (el sistema sanitario nacional) causó la cancelación de 19.000 citas, y costó a la entidad 92 millones £ en pérdidas de productividad, además de los gastos incurridos para el restablecimiento de datos y sistemas. No solamente que los pacientes afectados no recibieron la atención sanitaria necesaria, sino que además el NHS fue muy criticado por no responder de manera bastante rápida o sustancial a anteriores alertas de ciberamenazas. Aunque TODAS las organizaciones deberían estar actualizadas y bien informadas acerca de la ciberseguridad, las que manejan información sensible —en particular datos de categoría especial— deberían estar mucho más vigilantes a los ciberriesgos.

Cuando mayor el valor de una organización —medido por su facturación—, mayor será el botín que se lleven los atacantes. Y, por consiguiente, mayor el riesgo de ciberataques al que se exponen. No obstante, esto no implica que a las organizaciones más pequeñas no debería preocuparles la ciberseguridad. Mientras que las grandes empresas pueden ser objetivos más atractivos para los ataques, suelen también disponer de recursos y de personal dedicado para hacerles frente. Por el contrario, muchas pymes carecen de equipos de ciberprotección y hacen excepciones para los altos ejecutivos para evitar la administración de USB, lo cual las hace particularmente vulnerables... con resultados desastrosos. Algunos estudios demuestran que, en este momento, las pymes están más en riesgo de ciberataques.

El riesgo es todavía mayor para los empleados que ocupan altos cargos ejecutivos. Se trata de personas fácilmente accesibles que, por lo general, tienen privilegios ejecutivos en sus organizaciones. Ello implica que los cibercontroles —como los procedimientos de administración de unidades USB— no se les aplican, lo cual las convierte en objetivos lucrativos para los ciberdelincuentes. Es en este aspecto en el cual las unidades cifradas por hardware, conjuntamente con estar bien informados en ciberseguridad y seguir buenas prácticas y procesos, pueden suponer una enorme ventaja a la hora de reducir riesgos y proteger contra ataques.

> Muchas de las vulneraciones de seguridad más recientes han sido obra de protagonistas maliciosos que se especializan en aprovechar la ayuda —tanto voluntaria como inconsciente —de usuarios internos.
> - David Clarke

¿Quiénes están en riesgo?

> Las organizaciones que no hacen lo suficiente para contrarrestar amenazas contra la ciberseguridad. - David Clarke

La cadena de suministro es otro potencial punto de vulnerabilidad de las organizaciones, y los ataques contra la misma son demasiado habituales. En 2013, la cadena comercial estadounidense Target fue objetivo de una de las mayores vulneraciones de datos de la historia del sector, que dejó expuestos los datos de las tarjetas de débito y de crédito de más de 40 millones de clientes. Aunque la propia Target se ocupaba mucho de la ciberseguridad —había instalado un amplio sistema unos 6 meses antes del ataque—, los ciberdelincuentes se infiltraron a través de uno de los proveedores de Target, a través del cual accedieron a la red principal de datos de la compañía. El resultado fue que se presentaron 90 demandas contra Target y que la empresa perdió $61 millones para responder al ataque. Aunque no se la consideró responsable directa del ataque, la vulnerabilidad de la ciberseguridad de su cadena de suministro fue suficiente para causarle este perjuicio, tanto financiero como reputacional.

También los atajos de empleados puede ser una fuente de vulnerabilidad. Aunque estos atajos pueden permitirles ser más eficientes en su trabajo cotidiano, con demasiada frecuencia se pasan por alto procesos básicos de seguridad, como la administración de contraseñas. Aunque las directrices del NCSC (Centro Nacional de Ciberseguridad británico) y de la CISA (Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE.UU.) son bastante sencillas, en la práctica pueden ser más difíciles de implementar, en especial para equipos no familiarizados con la TI y la ciberseguridad. Aunque sin duda contar con un equipo de ciberseguridad dedicado puede ser de ayuda, el proporcionar a los empleados las herramientas adecuadas —como unidades cifradas por hardware— contribuye enormemente a mitigar los riesgos de los atajos.

> Hoy en día, las unidades USB cifradas por hardware resultan más fáciles de adoptar e integrar dentro de las políticas de ciberseguridad existentes: desde la diversidad de interfaces (gráficas, teclados, pantallas táctiles) hasta la compatibilidad con sistemas operativos, y capacidades a la medida de las necesidades de cada organización. - Pasi Siukonen

¿Cómo pueden las organizaciones reducir los riesgos de ciberataques?

Desde un punto de vista organizativo existen varias cosas que pueden hacerse para proteger los terminales y los datos. Sin políticas de GRC (gobernanza, riesgos, cumplimiento normativo), la ciberseguridad está condenada a fracasar. En consecuencia, familiarizarse con los siguientes procesos es increíblemente importante para que las organizaciones puedan protegerse. También contar con un software sólido de protección de terminales puede neutralizar diversas ciberamenazas, además de poder responder lo antes posible a la hora de taponar cualquier vulnerabilidad.

> **Adoptar políticas de cifrado forzado o no es tan significativo, o quizá MÁS significativo, para la gestión de riesgos como lo es hacer, o no, copias de seguridad de sus datos.** - Pasi Siukonen

Sin embargo, a nivel individual, el cifrado por hardware puede reducir drásticamente las vulnerabilidades frente a las amenazas de ciberseguridad. Con el incremento y perdurabilidad del trabajo remoto e híbrido, en especial acoplado al aumento de ciberataques en el último año, asegurarse de que los empleados de todos los niveles de la organización manejen, transfieran y lean de manera segura los datos ha adquirido mayor importancia que nunca.

Las unidades USB cifradas mediante hardware permiten a los usuarios seguir beneficiándose de la portabilidad y sencillez de los dispositivos Flash y, al mismo tiempo, reducir enormemente los riesgos que ello conlleva. Mientras que una unidad el montón extraviada o robada puede significar la pérdida de datos, dinero, reputación y mucho más, las unidades cifradas por hardware están diseñadas para proteger a los datos sensibles contra una amplia diversidad de ataques. Y a medida que los ciberdelincuentes desarrollan nuevos métodos de ataque, las unidades cifradas continuarán evolucionando para hacerles frente.

En síntesis, el costo de los ciberataques puede ser enorme. De hecho, en tanto que la adopción y uso de unidades cifradas a nivel organizaciones puede requerir un procedimiento de aprobación e implementación más complejo, a largo plazo puede suponer un enorme ahorro de dinero, tanto en términos de costos de extorsión como de lucro cesante y pérdida de reputación. Solamente las costas legales de una vulneración cubren con creces el coste añadido de las unidades USB cifradas por hardware.

> **Mediante un compromiso a largo plazo de ofrecer soluciones USB cifradas, la cartera de productos de Kingston permite a cualquier organización cumplir sus objetivos de configuración de ciberseguridad: cifrado por hardware forzado, diseños compatibles con políticas de protección de terminales y funciones de administración de dispositivos.** - Pasi Siukonen

Resumen

En Kingston estamos siempre atentos a la evolución del universo de la ciberseguridad y nos aseguramos de que nuestras unidades cifradas IronKey estén siempre actualizadas con los requisitos más recientes para atender a las necesidades de ciberseguridad de las organizaciones, tanto grandes como pequeñas. Mientras la ciberseguridad siga siendo una creciente preocupación a nivel global, confiamos que, con las herramientas y los conocimientos adecuados a su disposición, las organizaciones estén bien equipadas para hacer frente a estos retos, protegiéndose a sí mismas, a sus empleados y a sus clientes.

Acerca de Kingston

Con más de 35 años de experiencia, Kingston cuenta con los conocimientos necesarios para identificar y resolver sus retos de datos móviles, facilitando a sus empleados trabajar con seguridad desde cualquier lugar sin comprometer a su organización.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021