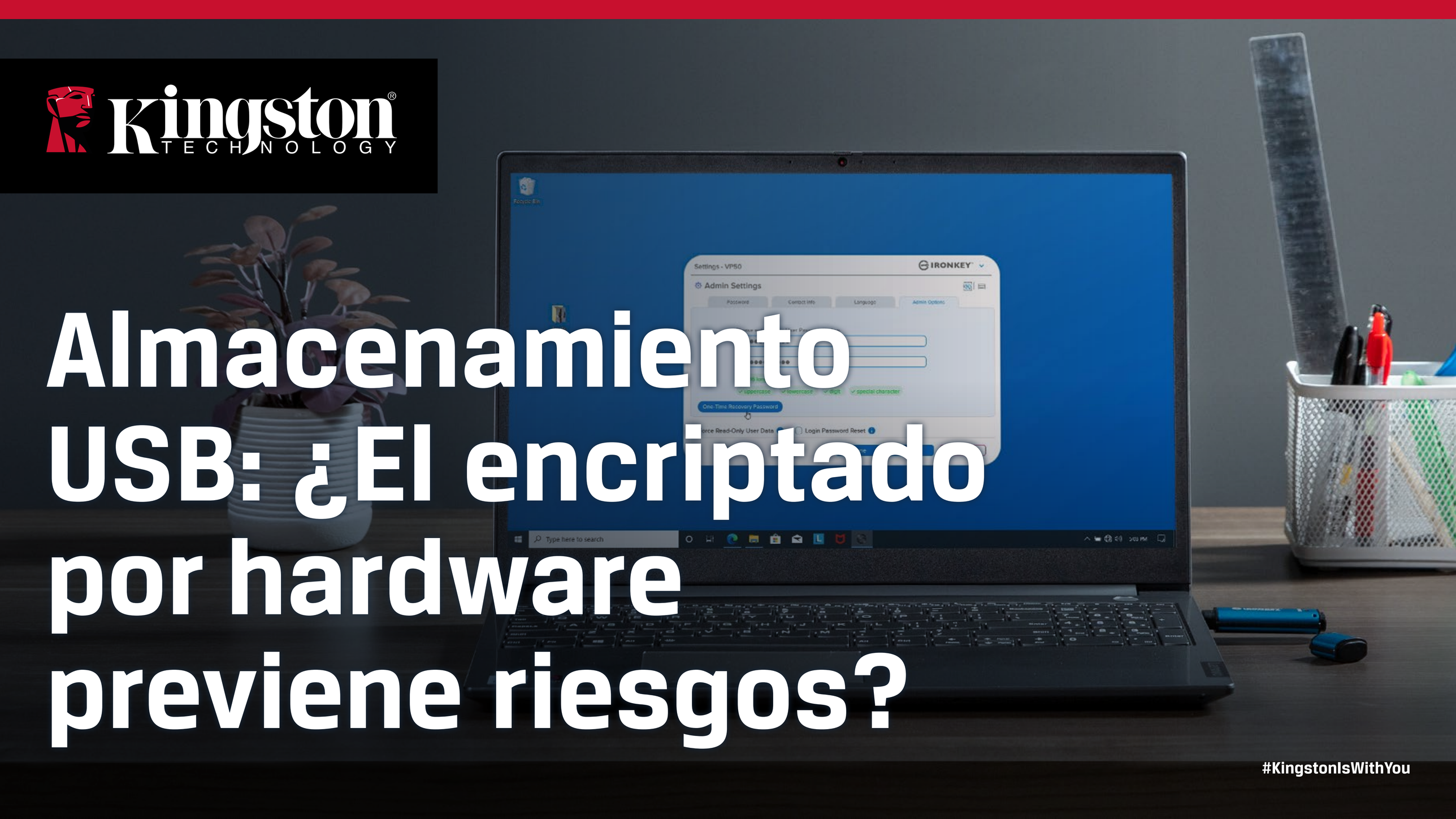
Almacenamiento USB: ¿El encriptado por hardware previene riesgos?



#KingstonIsWithYou

Almacenamiento USB: ¿El encriptado por hardware previene riesgos?

Prólogo y contenido

La ciberseguridad es una mayor preocupación para las empresas que nunca, pero demasiadas organizaciones están desinformadas y mal preparadas contra las amenazas de ciberseguridad. En los Estados Unidos, solo el 50% de las empresas tienen un plan de ciberseguridad; de ellas, el 32% no ha actualizado sus planes de ciberseguridad desde el inicio de la pandemia de COVID-19, tiempo que vio a muchas organizaciones pasar a modelos de trabajo remotos o híbridos según UpCity. Y la frecuencia de los ciberataques solo está aumentando: a nivel mundial, el número de empresas afectadas por ataques de ransomware aumentó del 37% en 2020 al 66% en 2021[1].

La seguridad cibernética que se compromete puede tener efectos devastadores en una empresa: aparte del coste monetario de los ciberataques, la pérdida de datos, seguridad y reputación puede afectar negativamente a las organizaciones de muchas maneras, tanto a corto como a largo plazo.

Un vehículo común para las amenazas de ciberseguridad son los dispositivos USB. Estos se han vuelto omnipresentes en muchas organizaciones debido a su simplicidad: solo conéctelos a una máquina y estarán listos para su uso. Sin embargo, es exactamente esta simplicidad lo que deja a los dispositivos USB tan vulnerables a los ataques: todo lo que se necesita es un dispositivo extraviado o robado para que un actor malicioso acceda a datos potencialmente confidenciales. Aquí es donde el cifrado puede desempeñar un papel importante para hacer que los dispositivos USB sean seguros para su uso y mitigar los riesgos asociados para el individuo y la organización. En este libro electrónico ofrecemos respuestas a las siguientes preguntas clave:

- ¿Por qué los USB encriptados son tan cruciales para proteger contra ciberataques?
- ¿Dónde se están haciendo vulnerables las organizaciones?
- ¿Qué pueden hacer para protegerse?

Tabla de contenidos	Páginas
Colaboradores	3
La diferencia entre los productos básicos y los dispositivos encriptados	4
¿Por qué usar USB encriptados?	5
¿Quién está en riesgo?	6-7
¿Cómo pueden las organizaciones reducir el riesgo de ciberataques?	8
Resumen y sobre Kingston	9

Almacenamiento USB: ¿El encriptado por hardware previene riesgos?

Colaboradores

Este eBook ha sido creado en conjunto con figuras líder de la industria en TI y tecnologías emergentes, así como por nuestro propio experto técnico.

David Clarke

David es reconocido como uno de los 10 principales influencers por Thompson Reuter "Los 30 líderes de opinión y pensadores más influyentes en las redes sociales, en gestión de riesgos, cumplimiento y tecnología de la regulación en el Reino Unido" y está en la lista de los 50 mejores expertos globales de Kingston Technology.

Pasi Siukonen

Pasi es responsable de liderar un equipo de expertos que asisten a los departamentos de Kingston, tales como relaciones públicas, mercadotecnia, ventas de campo, soporte técnico y servicio al cliente en los productos de Kingston. Su enfoque principal de producto son las líneas de productos Flash y SSD.

La diferencia entre los productos básicos y los dispositivos encriptados

Si bien los dispositivos básicos (no encriptados) son extremadamente fáciles de acceder y usar, el encriptado por hardware agrega varias capas de seguridad, tanto física como digital, que hacen que el almacenamiento USB sea mucho más seguro. La fácil disponibilidad, bajo costo y portabilidad de los dispositivos no encriptados básicos significa que, si bien son muy convenientes para el usuario, también son convenientes para los actores maliciosos que tienen como objetivo robar datos confidenciales, introducir malware o ransomware en una red de la empresa, y más. Como los USBs se utilizan con tanta frecuencia, las oportunidades para los ciberataques son muchas. Hay dos riesgos principales asociados a los dispositivos de productos básicos:

- **Ataques de ransomware:** estos ataques basados en USB implican la introducción de malware en las redes de la empresa, la retención de información de la empresa y/o el rescate de sistemas mediante su encriptado. Estos son a menudo causados por BadUSBs y se han convertido en el tipo más prominente de malware.
- **Datos robados:** todo lo que se necesita es un dispositivo perdido, robado o desatendido sin las medidas de seguridad adecuadas para que un actor malicioso pueda acceder fácilmente a los datos almacenados en el dispositivo, ya sea información del cliente, código fuente o datos financieros y de rendimiento confidenciales.

BadUSB – es un ataque que puede explotar la vulnerabilidad de los dispositivos USB con firmware desprotegido, que luego se puede programar con software malicioso. Estas herramientas maliciosas son increíblemente comunes y están fácilmente disponibles para los ciber-delincuentes, pero la concienciación sobre estas herramientas sigue siendo escasa, lo que hace que estos ataques sean demasiado fáciles de llevar a cabo sustituyendo el firmware de un dispositivo básico por un firmware pirateado en el que el dispositivo USB puede hacerse pasar por un teclado y, básicamente, ejecutar scripts para atacar el firewall. Dado que muchos ciberataques se llevan a cabo a través de personal interno desprevenido, con o sin intención maliciosa, es increíblemente importante que las empresas utilicen dispositivos encriptados que empleen firmware protegido y firmado digitalmente para evitar estos ataques, ya que pueden reducir las posibilidades de éxito de los ciber-delincuentes.

> **El costo de reconstruir la infraestructura, y tal vez pagar el rescate y otras extorsiones, es enorme en comparación con los costos de los USB administrados.**
> **- David Clarke**

¿Por qué usar USB encriptados?

Los dispositivos encriptados están diseñados específicamente para proteger los datos contenidos en su interior, así como los dispositivos a los que pueda estar conectado el dispositivo, lo que los convierte en valiosas herramientas del arsenal informático de cualquier organización. A medida que las amenazas de ciberseguridad se han vuelto más avanzadas, también lo han hecho las características de los dispositivos encriptados, lo que les permite mantenerse por delante de los ciber-delincuentes que buscan explotar estos dispositivos. Como se ha visto con la línea de productos encriptados por hardware de Kingston IronKey™, se han desarrollado y añadido a lo largo de los años características como el encriptado AES de 256 bits en el modo XTS más potente, una carcasa robusta y resistente a las manipulaciones, firmware firmado digitalmente, teclados virtuales, modos complejos o de frase de contraseña y mucho más, para garantizar que los usuarios estén bien protegidos contra todo tipo de ataques.

Debido a que los riesgos cibernéticos son a menudo poco conocidos, muchas empresas optan por utilizar dispositivos básicos, a pesar de las diversas vulnerabilidades que conllevan. Su facilidad de disponibilidad, bajo costo y el uso de encriptado por Software juegan un papel aquí, al igual que la falta de un proceso de aprobación corporativa para los dispositivos flash. Con demasiada frecuencia, no existen políticas o procesos de mejores prácticas organizativas para cumplir con diversas normas de TI y ciberseguridad, como ISO27001, GDPR, SOC2 y las mejores prácticas gubernamentales de WISP. Esto significa que los riesgos a menudo se evalúan en función de la opinión, en lugar de la evidencia, lo que deja a muchas organizaciones vulnerables a los ataques.

Mientras que algunos pueden utilizar dispositivos básicos con herramientas de encriptación de software existentes, esto puede ser a menudo un falso ahorro, ya que muchos dispositivos encriptados por software pueden ser hackeados con herramientas gratuitas o de pago disponibles en Internet para cualquiera. El encriptado por software también se puede ser quitado de un dispositivo con un reformateo simple del dispositivo por un usuario, para mayor comodidad o para usar los dispositivos en plataformas de SO no compatibles. Mientras que los USB encriptados por hardware tienen una encriptación siempre activa que no se puede desactivar, son aptos para su finalidad; y están construidos para ser resistentes a la manipulación, con evidencia de manipulación, y utilizan un firmware firmado digitalmente para garantizar la autenticidad e integridad del dispositivo. La limitación de los intentos de contraseña (protección contra ataques de fuerza bruta) y los teclados virtuales (protegen contra el registro de teclas y el registro de pantalla) son otras dos características de los dispositivos encriptados como IronKey VP50, lo que significa que cumplen con las mejores prácticas de la industria contra los actores maliciosos que pretenden extraer las contraseñas de los usuarios desprevenidos.

> Si el dispositivo IronKey detecta que el firmware ha sido manipulado, bloqueará el dispositivo y no arrancará, mejorando así la ciberseguridad.
> - Pasi Siukonen

¿Quién está en riesgo?

Realmente, cualquier empresa que no sea capaz de controlar el acceso a su USB está en riesgo, y a menudo no es consciente de cuáles son exactamente esos riesgos. Sin embargo, hay factores que pueden hacer que ciertas empresas sean más atractivas y vulnerables a los ciberataques.

Para las empresas de los sectores de la salud y las finanzas, sus datos no sólo son mucho más atractivos para los ciber-delincuentes, sino que también afectan a las organizaciones y a sus clientes de forma más severa. En el Reino Unido, un ciberataque de 2017 dirigido al NHS causó la cancelación de más de 19.000 citas y costó al NHS 92 millones de libras esterlinas en pérdida de producción, así como los costos de restauración de datos y sistemas. Esto no solo impidió que los pacientes afectados recibieran atención médica, sino que el NHS fue muy criticado por no responder de manera rápida o lo suficientemente sustancial a las advertencias anteriores de ciber-amenazas. Si bien todas las organizaciones deben estar actualizadas y bien informadas sobre la ciberseguridad, las que se ocupan de la información confidencial, en particular los datos de categorías especiales, deben estar doblemente atentas a los riesgos cibernéticos.

A mayor valor de la empresa, medido por la facturación, mayor es la recompensa para los actores maliciosos, por lo tanto, mayor es el riesgo que enfrentan de las amenazas cibernéticas. Sin embargo, eso no significa que las organizaciones más pequeñas no deban preocuparse por la ciberseguridad; si bien las empresas pueden ser objetivos más atractivos para los ataques, a menudo también tienen los recursos y el personal dedicado para abordar las amenazas cibernéticas. Por otro lado, muchas PYMES no tienen equipos de ciberseguridad dedicados y/o hacen excepciones con los altos ejecutivos para evitar la administración del USB, lo que las hace especialmente vulnerables con consecuencias devastadoras. Algunos estudios muestran que las pequeñas y medianas empresas son en realidad el blanco de los ciberataques.

El riesgo es aún mayor para los empleados que ocupan puestos ejecutivos de alto nivel; estas personas son fácilmente rastreables y a menudo gozan de privilegios ejecutivos en sus organizaciones, lo que significa que los controles cibernéticos -como los procedimientos de gestión de USB- no se aplican a ellos, convirtiéndolos en objetivos lucrativos para los ciber-delincuentes. Aquí es donde los dispositivos encriptados por hardware siempre activos, junto con estar bien informado sobre la ciberseguridad y seguir las mejores prácticas y procesos, pueden ayudar mucho a reducir el riesgo y a protegerse contra los ataques.

> Muchas de las infracciones más recientes han sido cometidas por actores maliciosos especializados en utilizar la ayuda interna, ya sea de forma voluntaria o sin saberlo. - David Clarke

¿Quién está en riesgo?

> **Las organizaciones no están haciendo lo suficiente para contrarrestar las amenazas de ciberseguridad.**
> **- David Clarke**

La cadena de suministro es otro punto potencial de vulnerabilidad para las organizaciones, y los ataques a la cadena de suministro son demasiado comunes. En 2013, el minorista estadounidense Target sufrió una de las mayores violaciones de datos de la historia del comercio minorista, exponiendo la información de las tarjetas de débito y crédito de más de 40 millones de clientes. Aunque Target estaba muy preocupado por la ciberseguridad, después de haber instalado un extenso sistema de ciberseguridad 6 meses antes del ataque, los atacantes se habían infiltrado en uno de los proveedores externos de Target y habían obtenido acceso a la red de datos principal de Target a través de ellos. En total, se presentaron 90 demandas contra Target, y la compañía perdió 61 millones de dólares en respuesta a la violación; si bien es posible que no hayan sido directamente responsables del ataque, esta debilidad en la ciberseguridad de su cadena de suministro fue suficiente para causar daños, tanto financieros como de reputación.

Las soluciones alternativas para los empleados también pueden ser una fuente de vulnerabilidad. Si bien estas soluciones pueden permitir a los empleados ser más eficaces en su trabajo diario, con demasiada frecuencia se pasarán por alto los procesos básicos de seguridad y las mejores prácticas, como la gestión de contraseñas. Aunque la orientación de NCSC y CISA es bastante sencilla, a menudo es más difícil de implementar en la práctica, especialmente de los miembros del equipo que no están familiarizados con TI y ciberseguridad. Si bien contar con un equipo de ciberseguridad dedicado puede ayudar, proporcionar a los empleados con las herramientas adecuadas, como dispositivos encriptados por hardware, puede ayudar mucho a mitigar los riesgos en cuanto a las soluciones alternativas de los empleados.

> **Los dispositivos USB encriptados por hardware hoy en día son fáciles de adoptar e integrar en las políticas de ciberseguridad existentes; desde su variedad de interfaces (gráficas, teclado, pantalla táctil) hasta el amplio soporte del sistema operativo, y con capacidades que satisfacen las necesidades de cada organización. - Pasi Siukonen**

¿Cómo pueden las organizaciones reducir el riesgo de ciberataques?

Desde el punto de vista de la organización, hay una serie de cosas que se pueden hacer para asegurar los puntos finales y proteger los datos. Sin GRC (Gobierno, Riesgo, Cumplimiento), la ciberseguridad está condenada al fracaso, por lo que estar familiarizado con los procesos y seguirlos es increíblemente importante para que las empresas se protejan. Disponer de un sólido software de seguridad endpoint también puede neutralizar una serie de ciber-amenazas, además de ser lo más receptivo posible a la hora de aplicar parches a cualquier vulnerabilidad de seguridad.

> **Adoptar o no políticas de encriptación aplicadas es una cuestión tan importante, o posiblemente más, para la gestión de riesgos como la de optar por hacer copias de seguridad de los datos... o no. - Pasi Siukonen**

Sin embargo, a nivel individual, el hardware encriptado puede reducir drásticamente las vulnerabilidades contra las amenazas de ciberseguridad. Con el aumento - y persistencia - del trabajo remoto e híbrido, sumado especialmente al incremento de los ciberataques en el último año, garantizar que los empleados de todos los niveles de la organización manejen, transfieran y lean los datos de la empresa de forma segura es más importante que nunca. Los USB encriptados por hardware permiten a los usuarios seguir beneficiándose de la portabilidad y la simplicidad de los dispositivos flash, al tiempo que reducen en gran medida el riesgo asociado con ellos; mientras que un dispositivo de producto extraviado o robado puede significar pérdida de datos, dinero, reputación y más, los dispositivos encriptados por hardware están diseñados para proteger los datos confidenciales de una amplia gama de ataques. Y a medida que los ciber-delincuentes desarrollen nuevas formas de ataque, los dispositivos encriptados continuarán evolucionando para enfrentar estos nuevos desafíos.

En general, el costo de lidiar con un ciberataque puede ser enorme. Y, de hecho, si bien la adopción y el uso de dispositivos encriptados a nivel organizacional pueden requerir de una aprobación y configuración más involucradas, le pueden ahorrar a la empresa mucho dinero a largo plazo, tanto en términos de costos de extorsión como de pérdida de ingresos debido a una reputación dañada. Solo los costos legales de una violación pueden pagar fácilmente el costo adicional de los dispositivos USB encriptados por hardware.

> **Gracias a su compromiso a largo plazo de proporcionar excelentes soluciones USB encriptadas, la cartera de Kingston le permite a cualquier organización cumplir con sus configuraciones de ciberseguridad-encriptación de hardware aplicada de acuerdo con los estándares de la industria, diseños que cumplen con las políticas endpoint y capacidades para la administración de dispositivos. - Pasi Siukonen**

Resumen

En Kingston, siempre estamos mirando los desarrollos en el área de ciberseguridad, asegurando que nuestras dispositivos encriptados IronKey estén al día con los últimos requisitos y satisfaciendo las necesidades de ciberseguridad de las organizaciones, tanto grandes como pequeñas. A medida que la ciberseguridad continúa siendo una preocupación creciente a nivel mundial, estamos seguros de que con las herramientas y el conocimiento adecuados a su disposición, las organizaciones pueden estar bien equipadas para enfrentar estos desafíos de frente, al tiempo que se protegen a sí mismas, a sus empleados y a sus clientes.

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

Acerca de Kingston

Con más de 35 años de experiencia, Kingston tiene los conocimientos necesarios para identificar y resolver sus desafíos en materia de datos móviles, lo que facilita que su personal desempeñe su trabajo de forma segura sin poner en peligro su organización.

#KingstonIsWithYou