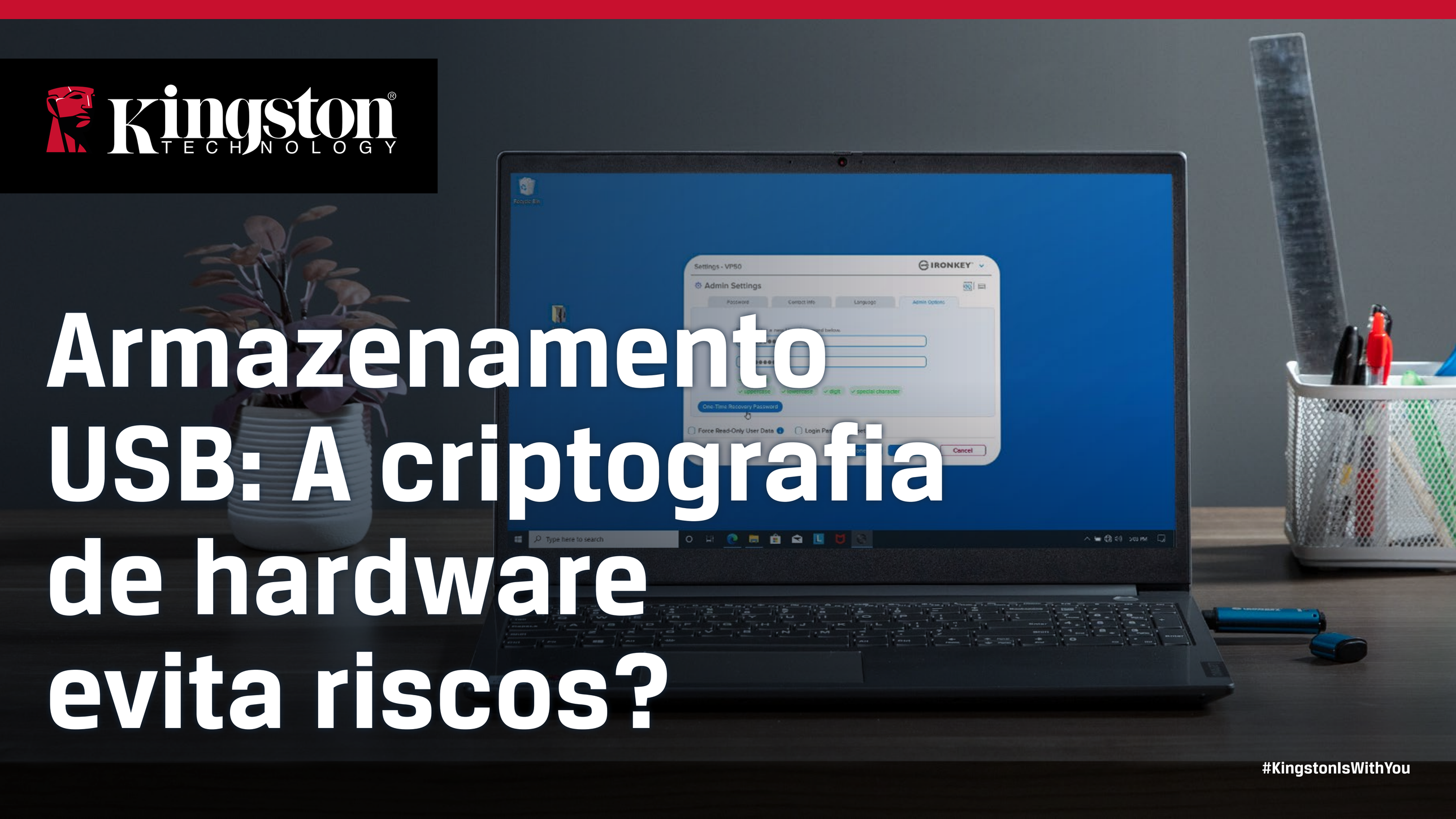
Armazenamento USB: A criptografia de hardware evita riscos?



#KingstonIsWithYou

Armazenamento USB: A criptografia de hardware evita riscos?

Prefácio e índice

A segurança cibernética é mais do que nunca uma preocupação para as empresas, mas muitas organizações estão desinformadas e despreparadas para ameaças de segurança cibernética. Nos Estados Unidos, apenas 50% das empresas possuem um plano de segurança cibernética; desses, 32% não atualizaram seus planos de segurança cibernética desde o início da pandemia do COVID-19, que viu muitas organizações migrando para modelos de trabalho remotos ou híbridos de acordo com a UpCity. E a frequência de ataques cibernéticos só está aumentando - globalmente, o número de empresas atingidas por ataques de ransomware aumentou de 37% em 2020 para 66% em 2021[1].

O comprometimento da segurança cibernética pode ter efeitos devastadores em uma empresa - além do custo monetário dos ataques cibernéticos, a perda de dados, segurança e reputação pode afetar negativamente as organizações de várias maneiras, tanto no curto quanto no longo prazo.

Um veículo comum para ameaças à segurança cibernética são os pendrives. Eles se tornaram onipresentes em muitas organizações devido à sua simplicidade - basta conectá-los a uma máquina e eles estão prontos para uso. No entanto, é exatamente essa simplicidade que deixa os pendrives tão vulneráveis a ataques: basta um drive extraviado ou roubado para que um agente mal-intencionado acesse dados potencialmente confidenciais. É aqui que a criptografia pode desempenhar um papel significativo para tornar os pendrives seguros para uso e mitigar quaisquer riscos associados para o indivíduo e a organização. Neste eBook, oferecemos respostas para as seguintes perguntas:

- Por que os USBs criptografados são tão importantes na proteção contra ataques cibernéticos?
- Onde as organizações estão se tornando vulneráveis?
- O que elas podem fazer para se proteger?

Índice	Páginas

Armazenamento USB: A criptografia de hardware evita riscos?

Colaboradores

Este eBook foi criado com uma figura líder do setor em TI e tecnologias emergentes, juntamente com nosso próprio especialista técnico.

David Clarke

David é reconhecido como um dois 10 principais influenciadores na lista dos 30 pensadores e líderes intelectuais mais influentes nas redes sociais, nas áreas de gestão de risco, compliance e reg-tech do Reino Unido pela Thompson Reuter, além de estar na lista dos 50 principais especialistas globais pela Kingston Technology.

Pasi Siukonen

Pasi é responsável por liderar uma equipe de especialistas que dão suporte aos departamentos da Kingston, como RP, Marketing, Vendas, Suporte Técnico e Atendimento ao Cliente em produtos da Kingston. Seu foco principal de produto são as linhas de produtos Flash e SSD.

A diferença entre pendrives commodity e criptografados

Embora os drives commodity (não criptografados) sejam extremamente simples de acessar e usar, a criptografia de hardware adiciona várias camadas de segurança - tanto físicas quanto digitais - que tornam o armazenamento USB muito mais seguro. A facilidade de acesso, baixo custo e portabilidade de drives commodity não criptografados significa que, embora sejam muito convenientes para o usuário, também são convenientes para agentes mal-intencionados que desejam roubar dados confidenciais, introduzir malware ou ransomware em uma rede da empresa e muito mais. Como os USBs são usados com tanta frequência, as oportunidades para ataques cibernéticos são muitas. Existem dois riscos principais associados aos drives commodity:

- **Ataques ransomware:** esses ataques baseados em USB envolvem a introdução de malware nas redes da empresa, mantendo as informações da empresa e/ou os sistemas em resgate, criptografando-os. Geralmente são causados por BadUSBs e se tornaram o tipo de malware mais proeminente.
- **Dados roubados:** basta um drive perdido, roubado ou desacompanhado de medidas de segurança apropriadas para que um agente mal-intencionado acesse facilmente os dados armazenados no drive - sejam informações confidenciais do cliente, código-fonte ou dados financeiros e de desempenho.

BadUSB – é um ataque que pode explorar a vulnerabilidade de drives USB com firmware desprotegido, que pode ser programado com software malicioso. Essas ferramentas maliciosas são incrivelmente comuns e facilmente disponíveis para criminosos cibernéticos, mas a conscientização sobre essas ferramentas permanece baixa, tornando esses ataques muito fáceis de serem executados substituindo o firmware de um drive commodity por um firmware hackeado, onde o drive USB pode se passar por um teclado e basicamente executam scripts para atacar o firewall. Como tantos ataques cibernéticos são realizados por funcionários desavisados, com ou sem intenção maliciosa, é extremamente importante que as empresas usem drives criptografados que utilizam firmware protegido e assinado digitalmente para evitar esses ataques, o que pode reduzir as chances de sucesso dos criminosos cibernéticos.

> **O custo da reconstrução da infra-estrutura, e talvez pagar o resgate e outras extorsões, é enorme em comparação com os custos dos USBs gerenciados.**
> **- David Clarke**

Por que usar USBs criptografados?

Os drives criptografados são projetados especificamente para proteger os dados contidos neles, bem como quaisquer dispositivos aos quais o drive possa estar conectado, tornando-os ferramentas valiosas no arsenal de TI de qualquer organização. À medida que as ameaças de segurança cibernética se tornaram mais avançadas, os recursos dos drives criptografados também se tornaram, permitindo que eles fiquem à frente dos criminosos cibernéticos que procuram explorar esses dispositivos. Como visto com a linha de produtos com criptografia de hardware Kingston IronKey™, recursos como criptografia AES de 256 bits no modo XTS mais forte, caixa robusta e resistente a adulterações, firmware assinado digitalmente, teclados virtuais, ao longo dos anos foram desenvolvidos e adicionados senhas de modo complexo para garantir que os usuários estejam bem e verdadeiramente protegidos contra todos os tipos de ataques.

Como os riscos cibernéticos são tão frequentemente mal compreendidos, muitas empresas optam por usar drives commodity, apesar das várias vulnerabilidades que eles trazem. Sua facilidade de acesso, baixo custo e o uso de criptografia de software desempenham um papel aqui, assim como a falta de um processo de aprovação corporativa para drives flash. Muitas vezes, não existem políticas ou processos de melhores práticas organizacionais para cumprir várias normas de TI e segurança cibernética, como a ISO27001, o RGPD, a SOC2 e as melhores práticas governamentais da WISP. Isso significa que os riscos geralmente são avaliados com base em opiniões, e não em evidências, deixando muitas organizações vulneráveis a ataques.

Embora alguns possam usar drives commodity com ferramentas de criptografia de software existentes, isso pode muitas vezes ser uma falsa economia, uma vez que muitos drives criptografados por software podem ser invadidos com ferramentas gratuitas ou pagas disponíveis na Internet para qualquer um. A criptografia de software também pode ser removida de um drive com uma simples reformatação do drive por um usuário, por conveniência, ou para usar os drives em plataformas de sistemas operacionais não suportados. Já os USBs criptografados por hardware tem sempre uma criptografia que não pode ser desativada, eles são adequados para o propósito; e são construídos para serem resistentes a adulterações, com adulterações visíveis e usam firmware assinado digitalmente para garantir a autenticidade e integridade da unidade. Limitar tentativas de senha (proteção contra ataques de força bruta) e teclados virtuais (protege contra registros de toque do teclado e da tela) são mais dois recursos de drives criptografados, como o IronKey VP50, o que significa que ele está em conformidade com as melhores práticas do setor contra agentes mal-intencionados que visam extrair senhas de usuários desavisados.

> Se a unidade IronKey detectar que o firmware foi adulterado, ela bloqueará a unidade e não inicializará, aumentando assim a segurança cibernética. - Pasi Siukonen

Quem está em risco?

Realmente, qualquer empresa que não consiga controlar seu acesso USB está em risco - e muitas vezes, elas não sabem exatamente quais são esses riscos. No entanto, existem fatores que podem tornar certas empresas alvos mais atraentes – e vulneráveis – para ataques cibernéticos.

Para empresas dos setores financeiro e de saúde, seus dados não são apenas muito mais atraentes para criminosos cibernéticos, mas também impactam as organizações e seus clientes de maneiras mais severas. No Reino Unido, um ataque cibernético em 2017 que teve como alvo o NHS causou o cancelamento de mais de 19.000 consultas e custou ao NHS 92 milhões de libras em perda de produção, bem como custos para restaurar dados e sistemas. Isso não apenas impediu que os pacientes afetados recebessem assistência médica, mas o NHS foi fortemente criticado por não responder com rapidez ou de forma substancialmente suficiente, aos avisos anteriores de ameaças cibernéticas. Embora todas as organizações devam estar atualizadas e bem informadas sobre segurança cibernética, aquelas que lidam com informações confidenciais - particularmente dados de categoria especial - devem estar duplamente vigilantes em relação aos riscos cibernéticos.

Quanto maior o valor da empresa, medido pelo volume de negócios, maior a recompensa para os agentes mal-intencionados - e, portanto, maior será o risco que enfrentam de ameaças cibernéticas. No entanto, isso não significa que empresas menores não devam se preocupar com a segurança cibernética; embora as grandes organizações possam ser alvos mais atraentes para ataques, elas geralmente também têm recursos e equipe dedicada para lidar com ameaças cibernéticas. Por outro lado, muitas PMEs não têm equipes de segurança cibernética dedicadas e abrem exceções para executivos seniores para evitar a gestão de USB, tornando-os particularmente vulneráveis com resultados devastadores. Alguns estudos mostram que as pequenas e médias empresas são, na verdade, mais visadas para os ataques cibernéticos.

O risco é ainda maior para funcionários em cargos executivos seniores; esses indivíduos são facilmente rastreáveis e geralmente têm privilégios executivos em suas organizações, o que significa que controles cibernéticos - como procedimentos de gestão de USB - não são aplicados a eles, tornando-os alvos lucrativos para criminosos cibernéticos. É aqui que os drives criptografados por hardware, sempre ativos, juntamente com o fato de se ter informação sobre segurança cibernética e seguir as melhores práticas e processos, podem ajudar bastante na redução de riscos e na proteção contra ataques.

> Muitas das violações mais recentes foram feitas por agentes mal-intencionados que se especializam em usar a ajuda interna, de forma voluntária ou involuntária.- David Clarke

Quem está em risco?

> As organizações não estão fazendo o suficiente para combater as ameaças à segurança cibernética.
> - David Clarke

A cadeia de suprimentos é outro ponto potencial de vulnerabilidade para as organizações, e os ataques à cadeia de suprimentos são muito comuns. Em 2013, a varejista norte-americana Target foi atingida por uma das maiores violações de dados da história do varejo, expondo as informações de cartão de débito e crédito de mais de 40 milhões de clientes. Embora o próprio Target estivesse muito preocupada com a segurança cibernética, tendo acabado de instalar um grande sistema de segurança cibernética 6 meses antes do ataque, os invasores se infiltraram em um dos fornecedores terceirizados do Target e obtiveram acesso à principal rede de dados do Target através deles. Ao todo, 90 ações judiciais foram movidas contra o Target, e a empresa perdeu 61 milhões de dólares em resposta à violação; embora eles possam não ter sido os responsáveis diretos pelo ataque, essa fraqueza na segurança cibernética de sua cadeia de suprimentos foi suficiente para causar danos, tanto financeiros quanto de reputação.

As soluções alternativas dos funcionários também podem ser uma fonte de vulnerabilidade. Embora essas soluções alternativas possam permitir que os funcionários sejam mais eficazes em seu trabalho diário, muitas vezes os processos básicos de segurança e as melhores práticas serão negligenciadas, como o gerenciamento de senhas. Embora a orientação do NCSC e da CISA seja bastante direta, muitas vezes é mais difícil de implementar na prática, especialmente de membros da equipe que não estão familiarizados com TI e segurança cibernética. Embora ter uma equipe dedicada de segurança cibernética certamente possa ajudar, fornecer aos funcionários as ferramentas certas - como drives criptografados por hardware - pode ajudar bastante a mitigar os riscos das soluções alternativas dos funcionários.

> Atualmente, os drives USB criptografados por hardware são fáceis de adotar e integrar às políticas de segurança cibernética existentes; desde a variedade de interfaces (gráfico, teclado, tela de toque) até amplo suporte ao sistema operacional e com capacidades que atendem às necessidades de cada organização. - Pasi Siukonen

Como as organizações podem reduzir o risco de ataques cibernéticos?

Do ponto de vista organizacional, há uma série de coisas que podem ser feitas para proteger endpoints e dados. Sem GRC (Governança, Risco, Compliance), a segurança cibernética está fadada ao fracasso - portanto, estar familiarizado e seguir os processos é extremamente importante para as empresas se protegerem. Ter um software robusto de segurança de endpoint também pode neutralizar várias ameaças cibernéticas, além de ser o mais reativo possível quando se trata de corrigir quaisquer vulnerabilidades de segurança.

> **A adoção ou não de políticas de criptografia é uma questão tão significativa ou possivelmente ainda mais significativa para a gestão de risco quanto escolher fazer backup dos seus dados... ou não.**
> **- Pasi Siukonen**

Em um nível individual, no entanto, o hardware criptografado pode reduzir drasticamente as vulnerabilidades contra ameaças de segurança cibernética. Com o aumento - e a durabilidade - do trabalho remoto e híbrido, especialmente associado ao aumento dos ataques cibernéticos no último ano, garantir que os funcionários de todos os níveis da organização manuseiem, transfiram e leiam os dados da empresa com segurança está se tornando mais importante do que nunca. USBs criptografados por hardware permitem que os usuários continuem se beneficiando da portabilidade e simplicidade dos drives flash, ao mesmo tempo em que reduzem bastante o risco associado a eles; enquanto um drive commodity extraviado ou roubado pode significar perda de dados, dinheiro, reputação e muito mais, os drives criptografados por hardware são projetados para proteger dados confidenciais de uma ampla variedade de ataques. E à medida que os criminosos cibernéticos desenvolvem novas formas de ataque, os drives criptografados continuarão evoluindo para enfrentar esses novos desafios.

Em suma, o custo de lidar com um ataque cibernético pode ser enorme. E, de fato, embora a adoção e o uso de drives criptografados em um nível organizacional possam exigir uma aprovação e configuração mais empenhadas, isso pode economizar muito dinheiro para a empresa - tanto em termos de custos de extorsão quanto em receita perdida devido a uma reputação danificada - a longo prazo. Apenas os custos legais de uma violação podem facilmente pagar o custo adicional de drives USB criptografados por hardware.

> **Por meio do compromisso de longo prazo em fornecer ótimas soluções USB criptografadas, o portfólio da Kingston permite que qualquer organização atenda às suas configurações de segurança cibernética - criptografia de hardware aplicada padrão do setor, projetos compatíveis com políticas de endpoint, recursos de gestão de dispositivos. - Pasi Siukonen**

Resumo

Na Kingston, estamos sempre observando os desenvolvimentos no espaço de segurança cibernética, garantindo que nossos drives criptografados IronKey estejam atualizados com os requisitos mais recentes e atendam às necessidades de segurança cibernética de organizações, tanto grandes como pequenas. Como a segurança cibernética continua sendo uma preocupação crescente em todo o mundo, estamos confiantes de que, com as ferramentas e o conhecimento certos à sua disposição, as organizações podem estar bem equipadas para enfrentar esses desafios de frente, protegendo a si mesmas, seus funcionários e seus clientes.

Sobre a Kingston

Com mais de 35 anos de experiência, a Kingston possui o conhecimento para identificar e resolver seus desafios de dados em movimento - fazendo com que sua força de trabalho opere com segurança sem comprometer sua organização.

#KingstonIsWithYou

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