CRIPTOGRAFIA DE SOFTWARE E CONFORMIDADE REGULATÓRIA: SOLUÇÃO MAIS BARATA COM MAIORES RISCOS DE SEGURANÇA

EXIGÊNCIAS DE CONFORMIDADE E REGULATÓRIAS

A segurança de dados costumava ser relegada apenas aos departamentos de TI, mas devido às contínuas violações de dados de clientes, os governos do mundo todo impuseram mais e mais exigências sobre os negócios para criptografar e proteger todos os dados que sejam pessoalmente identificáveis.

Da HIPAA na área de saúde, GDPR na EMEA e CCPA na Califórnia, a criptografia de classes de dados protegidas está sendo exigida através das regulamentações. As organizações de compliance se multiplicaram exponencialmente nos últimos 3 anos ou mais, conforme essas regulamentações e suas multas e riscos de prêmios legais dispararam.

Com tais mudanças, os departamentos de TI tiveram dificuldade para manter a segurança e os custos crescentes. Durante toda a pandemia do COVID, orçamentos foram gastos em investimentos adicionais em firewall e hardware, às custas de um foco na criptografia de dados.

De fato, a criptografia de software utilizando Microsoft BitLocker® ou software de gestão de endpoint de empresas como Symantec, McAfee e outras estão em crescimento. Alguns negócios e consumidores também utilizam USB padrão com "vault" de software como fornecidos por algumas empresas.

CRIPTOGRAFIA E DADOS EM TRÂNSITO

Funcionários e consumidores têm a necessidade de levar seus dados consigo. Eles têm opções tal como utilizar:

1. Serviços de nuvem: O que é ótimo, já que podem ser acessados de qualquer dispositivo conectado à internet. Entretanto a flexibilidade tem um preço. O armazenamento de dados em nuvem remove o controle dos dados do usuário ou da empresa e possui um risco potencial já que temos visto servidores de nuvem serem deixados desbloqueados ou abertos.
2. USB padrão: Enquanto carregar um USB parece mais seguro, o risco de exposição de dados por causa da perda do drive pode ser significativo. Por exemplo, há muitas histórias de USBs perdidos que foram encontrados com informações secretas ou lavanderias com gavetas cheias de USBs perdidos.
3. USBs com hardware criptografado: Esses USBs possuem arquiteturas personalizadas que incorporam um controlador de criptografia integrado e controle de acesso. Os dados são criptografados utilizando a mais forte criptografia AES-256 bit no modo XTS em geral, junto a outras proteções possíveis para mitigar ataques com base em firmware e físicos. Esses drives são fabricados por empresas que se especializam em dispositivos de segurança e mesmo que sejam mais caro do que os drives USB padrão, oferecem uma melhor segurança de dados. Drives FIPS 197 ou FIPS 140-2 Nível 3 podem adicionar maiores níveis de proteção e paz de espírito.
4. Drives USB padrão com criptografia de software: Por uma questão de segurança como exigido pela regulamentação, a criptografia de software com BitLocker ou outras ferramentas podem ser utilizadas. São opções decentes já que são relativamente baratas e oferecem a mesma criptografia AES-256 XTS.

Não é surpresa descobrir que na maioria dos casos, negócios e indústrias tendem a escolher a opção 4, utilizando drives USB padrão com criptografia de software, principalmente porque a criptografia de software como a BitLocker ou outros serviços de cofre de dados são "gratuitos".

A CRIPTOGRAFIA DE SOFTWARE NÃO ESTÁ EM CONFORMIDADE COM AS REGULAMENTAÇÕES

Para um profissional de segurança nos negócios, a criptografia de software pode oferecer as mesmas possibilidades de criptografia do que drives USB com hardware criptografado mais caros. Mas esse é o caminho? Os orçamentos são apertados, portanto os negócios estão se movendo para a criptografia de software por razões de conformidade, desconhecendo o lado obscuro da criptografia com base em software.

Qual é o problema com o drive USB de software criptografado? Os dados estáticos e em trânsito não estão criptografados pela AES-256 XTS? Em geral, sim. O problema é: A criptografia de software é considerada uma "criptografia removível".

Espera – Removível? Isso significa que um drive USB com software criptografado pode ter sua criptografia desabilitada por um usuário?

A resposta é – Sim. Usuários podem remover o recurso de criptografia de software de seus drives USB. Por que fariam isso? Você pergunta. Porque eles podem e porque eles querem apenas acessar os arquivos sem utilizar uma senha ou simplesmente esquecem a senha mas precisam utilizar o drive USB.

COMO REMOVER A CRIPTOGRAFIA DE SOFTWARE DE UM DRIVE USB CRIPTOGRAFADO

Para um usuário que não quer lidar com senhas de entrada complexas ou outras para acessar seus dados, o processo é simples:

1. Conecte o drive com software criptografado em um computador
2. Formate o drive
3. Depois que o drive estiver formatado, toda a criptografia é removida
4. Copie arquivos com informações secretas ou confidenciais para o drive para fácil acesso

Isso é fácil para usuários fazerem utilizando um computador que não seja restrito – os departamentos de TI restringiram o uso de comandos de formatação em computadores da empresa, mas isto pode ser feito em qualquer computador que não seja da empresa.

Por questões de conformidade – a facilidade de remover a criptografia de dados significa que o drive fornecido pela empresa agora não está criptografado, ainda que os dados que foram criptografados no drive sejam considerados perdidos para sempre uma vez que a criptografia é removida através do método acima (chaves de criptografia estão vinculadas aos dados). Qualquer dado copiado no dispositivo quando a criptografia é removida é considerado desprotegido e potencialmente fora de conformidade, o que pode representar um risco de violação de regulamentos da HIPAA, GDPR, CCPA e muitas outras.

AS CONSEQUÊNCIAS DE PERDAS DE DRIVES NÃO CRIPTOGRAFADOS

Se um drive USB designado por uma empresa é perdido e encontrado, mesmo se a empresa não souber inicialmente, mas tomar conhecimento depois através de redes sociais, exigências de conformidade especiais entram em vigor para a empresa e possivelmente exigirão que ela:

1. Conduza uma investigação forense para identificar quais dados foram perdidos
2. Determine se uma violação jurídica ocorreu, em consulta com o Jurídico
3. Determine se os clientes foram notificados

É aqui que uma simples perda de um drive USB pode se tornar muito custosa. Com taxas jurídicas de centenas de dólares por hora, este processo de conformidade pode resultar em milhões de dólares em gastos, adicionalmente a potenciais multas, processos de clientes ou de outro tipo, e o constrangimento pela exposição de dados.

Quando a criptografia por software é considerada para sua implementação de baixo custo, esses riscos e suas grandes consequências financeiras não são considerados.

Há um outro perigo em permitir o uso de drives USB não criptografados em uma empresa. Isso é chamado normalmente de "BadUSB". O BadUSB é uma classe de malware que foi utilizada por agentes maldosos para violar o firewall de uma empresa e introduzir malwares nas defesas cibernéticas de uma empresa através de dispositivos de armazenamento USB.

BadUSB

Quando um drive USB é conectado em um computador, o controlador de chipset do computador começa um aperto de mão com o controlador do drive USB via firmware. Essa troca ocorre antes que o sistema operacional, como Microsoft/ macOS/Linux, esteja ciente de que um drive USB foi conectado. Todo drive USB possui um firmware que funciona quando o drive é conectado em uma porta USB.

Agentes maldosos aprenderam que podem introduzir malwares através deste mecanismo de aperto de mão ao substituir o firmware que funciona no drive USB por outro, um firmware malicioso que injeta um malware no sistema do computador alvo conforme se comunica com o drive USB. Um drive USB padrão não tem segurança no seu firmware interno que é executado por seu controlador, portanto o BadUSB nasceu quando bons drives USB foram armados para penetrar em firewalls e violar defesas cibernéticas.

Muitas empresas tentam banir o uso de drives USB em seus sistemas, ou ir ainda mais longe fechando as portas USB com massa epóxi. Entretanto, elas constataram que os funcionários precisam carregar dados consigo em drives USB. Por exemplo, executivos querem levar dados com eles para o trabalho ou fornecer para conselheiros Jurídicos ou Financeiros externos que não estão na nuvem da empresa; contratados da empresa que precisam de dados para trabalhar mas têm acesso restrito a base de dados da empresa; analistas financeiros que estão correndo para fechar os relatórios mensais e precisam trabalhar nas planilhas em casa.

Como as análises anteriores mostram, há um risco significativo ao utilizar este drives USB padrão + solução de criptografia por software. À primeira vista, o que parece mais barato se torna potencialmente muito perigoso e muito mais caro. Apenas o custo de 2 ou 3 horas de consultoria com um advogado sobre uma potencial violação de dados acaba com qualquer economia ao utilizar uma solução mais barata.

DRIVES USB COM HARDWARE CRIPTOGRAFADO SÃO A MELHOR OPÇÃO PARA CONFORMIDADE REGULATÓRIA

O que faz com que os drives USB com hardware criptografado sejam a melhor escolha para essas aplicações regulatórias:

1. Drives USB com hardware criptografado possuem uma criptografia que está sempre LIGADA: Não existe uma forma do usuário desligar a criptografia, reconfigurar as regras de senha (tamanho mínimo, complexidade) e desabilitar as tentativas de senha automáticas. Diferente da criptografia por software, que não previne repetidos tentativas de senha utilizando ataques de dicionário de software, as versões de hardware limitam as tentativas de senha e bloqueiam os dados quando senhas erradas são inseridas 10 vezes, ou até menos. Isso é muito seguro na era dos supercomputadores.
2. Drives com hardware criptografado utilizam controladores de criptografia premium e incorporam muitos recursos de segurança: Embora não divulguemos sempre todas as contramedidas de segurança, há uma contramedida para se proteger do BadUSB. Na fábrica, quando o firmware é carregado nos drives com hardware criptografado apenas, o firmware é digitalmente assinado e carregado. Isso significa que, quando esses USBs criptografados são conectados, o controlador de criptografia primeiramente verifica a integridade do firmware através da assinatura digital e carrega apenas se ele passar pela verificação. Qualquer tentativa de substituir o firmware congelará o drive e ele não funcionará mais - e sem ameaças.
3. Os drives USB com hardware criptografado podem ter IDs de produto (PIDs) personalizadas definidas para uma empresa específica: Esses drives premium podem ter um identificador digital programado dentro deles para que, se um drive for conectado no firewall interno ou externo da empresa, o drive possa ser identificado como um drive elaborado para a empresa. Por exemplo, se um funcionário perde o drive da empresa e compra o mesmo modelo no varejo, o drive recém comprado não validará na rede da empresa. Esta personalização adiciona outra camada de segurança ao uso de drives USB.
4. Drives com hardware criptografado economizam dinheiro muito rapidamente: Apenas a redução e eliminação dos riscos fazem com que o ciclo de recompensa seja bem curto.

A Kingston é a maior fabricante de drives USB criptografados do mundo e oferece famílias de drive com vários recursos e pontos de preço. Contate diretamente a Kingston para discutir como podemos te ajudar a se manter em conformidade com as soluções USB criptografas para executivos, funcionários, contratados e mais.