Media Contact:
Ken Kadet, VP, Public Relations
952-937-1154 | ken.kadet@entrust.com

Empresas priorizam a proteção de dados do cliente, mas continuam deixando-os expostos, revela o estudo global de tendências de criptografia de 2021 da Entrust

Realizado pelo Ponemon Institute, o 16º estudo anual destaca que metade das organizações finalmente alcançaram uma estratégia de criptografia consistente e outras tendências importantes em criptografia e cibersegurança

São Paulo, 14 de abril de 2021 - As empresas enxergam a proteção das informações pessoais do cliente como a principal razão para criptografar dados mas, ainda assim, relatam que a efetiva criptografia dos dados do cliente é muito menor. Esta e outras descobertas ganharam destaque no Estudo Global de Tendências de Criptografia 2021 da Entrust, o 16º estudo anual realizado pelo Ponemon Institute, que relata os desafios de segurança cibernética que as organizações enfrentam hoje e como e porque as organizações implementam a criptografia.

Ameaças e prioridades identificadas

Pelo segundo ano consecutivo, os profissionais de TI classificam a proteção das informações do cliente como o principal motivo para a implantação de tecnologias de criptografia. A grande desconexão relatada é que as informações do cliente estão em quinto lugar na lista de informações que as empresas realmente criptografam, indicando um grande abismo entre as prioridades de uma organização e as realidades da implementação da criptografia. Ao observar o que as empresas entrevistadas realmente criptografam, registros financeiros (55%), dados relacionados a pagamentos (55%), dados de funcionários /RH (48%) e propriedade intelectual (48%) superaram as informações pessoais do cliente (42%).

“As violações de informações pessoais atingem o núcleo da relação entre as empresas e seus clientes. A criptografia é a base da proteção de dados e, quando as organizações não priorizam a proteção das informações pessoais dos clientes, aumentam o risco de a empresa perder negócios e reputação”, disse John Grimm, vice-presidente de estratégia da Entrust.

Compliance - que até recentemente era classificada como a principal razão para criptografar - tem uma grande influência, porém decrescente, no uso da criptografia, continuando uma tendência observada no Estudo Global de Tendências de Criptografia 2020. A proteção das informações do cliente (54%), a proteção contra ameaças específicas identificadas (50%) e a proteção da propriedade intelectual (49%) são classificadas acima do *Compliance*, agora com 45%.

A complexidade do gerenciamento da criptografia e chaves em 2021

O estudo também destaca tendências encorajadoras. Pela primeira vez, metade (50%) das organizações agora relata ter uma estratégia geral de criptografia aplicada de forma consistente, enquanto 37% relatam ter uma estratégia de criptografia limitada.

Mas esse marco revela novas lacunas, especialmente em ambientes com várias nuvens. As ferramentas de criptografia são abundantes, com relatórios de organizações usando uma média de oito produtos diferentes executando criptografia. Os entrevistados classificam o desempenho, o gerenciamento de chaves de criptografia, a aplicação de políticas e o suporte para implantação em nuvem e local (*on premise*) são os recursos mais valiosos das soluções de criptografia. Na verdade, 45% dos entrevistados classificaram o gerenciamento de chaves unificado entre várias nuvens e ambientes corporativos como muito importante ou importante. Essa descoberta é consistente com as chaves de criptografia para serviços em nuvem - incluindo Bring-Your-Own-Key (BYOK) - sendo o mais desafiador de gerenciar de todos os tipos de chave, de acordo com o estudo.

Não apenas o gerenciamento de chaves está cada vez mais complexo, mas apenas saber onde os dados da organização se encontram, entre ambientes locais, virtuais, em nuvem ou híbridos, tem se tornado um problema constante. Assim, 65% das organizações relatam que descobrir onde residem os dados confidenciais continua sendo, de longe, o principal desafio no planejamento e execução de uma estratégia de criptografia metódica.

O crescente papel dos módulos de segurança de hardware (HSMs, na sigla em inglês)

A geração e o gerenciamento de chaves de criptografia podem ser administrados de forma mais eficaz com o uso de módulos de segurança de hardware (HSMs). A adoção deles está crescendo, com dois terços (66%) dos entrevistados nomeando os HSMs como sendo fundamentais para as estratégias de criptografia ou gerenciamento de chaves, com crescimento projetado para 77% nos próximos 12 meses. O estudo também mostra que, além de aplicativos tradicionais como TLS/SSL, criptografia de aplicativos e PKI, os HSMs estão sendo cada vez mais usados para casos de uso mais modernos, como serviços de criptografia/assinatura de containers, criptografia em nuvem pública, gerenciamento de segredos e gerenciamento de acesso privilegiado.

À medida que as organizações continuam suas transformações digitais, os HSMs passam a desempenhar um papel cada vez mais significativo em ambientes de nuvem. O estudo descobriu que os serviços de criptografia ou assinatura para containers (40%) são o terceiro caso de uso mais popular para HSMs, atrás da criptografia de aplicativos (47%) e TLS/SSL (44%). A criptografia de nuvem pública, incluindo BYOK, é o quarto caso de uso de HSM mais popular (34%). Destaca-se ainda o uso de HSMs com soluções de gerenciamento de segredos, que subiu para o 7º lugar na lista dos principais casos de uso de HSMs e segue em ascensão, com um crescimento estimado de 5% nos próximos 12 meses.

Blockchain, algoritmos quânticos e adoção de novas tecnologias de criptografia

A visão sobre futuras tecnologias de criptografia, como computação multipartidária e criptografia homomórfica, é que elas estão há pelo menos cinco anos de distância do uso em larga escala, de acordo com os entrevistados. Da mesma forma, embora os algoritmos quânticos não devam ser uma realidade por cerca de oito anos, esta previsão de cronograma foi acelerada em meio ano em relação ao relatório de 2020.

Blockchain é a tecnologia de criptografia mais próxima do uso convencional. Atualmente é usada principalmente como base para criptomoedas, mas espera-se que em menos de três anos a adoção do blockchain e casos de uso sejam ampliados para incluir:

- Criptomoedas/carteiras digitais (59%)
- Transações/gestão de ativos (52%)
- Identidade (45%)
- Cadeia de suprimentos (37%)
- Contratos inteligentes (35%)

“Observando os resultados do Estudo Global de Tendências de Criptografia 2021 da Entrust, no contexto dos últimos 16 anos, fica claro que a segurança cibernética e a proteção de dados nunca foram tão complexas, em um momento em que os riscos nunca foram tão altos”, disse o Dr. Larry Ponemon, chairman e fundador do *Ponemon Institute*. “É encorajador que a proteção de dados do consumidor seja uma prioridade tão alta para as organizações, mas há claramente trabalho a ser feito para transformar essa prioridade em realidade em termos de quais dados são realmente criptografados e em quais pontos do ciclo de vida deles. Também é evidente que organizações de todos os tipos e tamanhos estão procurando adotar a criptografia para uma variedade de novos e inovadores casos de uso, que sem dúvida continuarão a impulsionar a inovação na indústria.”

“A TI tem a tarefa de implantar, rastrear e gerenciar a criptografia e a política de segurança em ambientes locais, em nuvem, com várias nuvens e híbridos, para uma gama crescente de casos de uso entre ameaças cada vez maiores. A criptografia é essencial para proteger os dados da empresa e do cliente, mas o gerenciamento da criptografia e a proteção das chaves secretas associadas são pontos cada vez mais problemáticos à medida que as organizações contratam vários serviços em nuvem para funções críticas”, acrescentou Grimm. “O uso crescente de HSMs para criptografia e gerenciamento de chaves mostra que a TI está começando a enfrentar esses desafios. As organizações se beneficiarão de um ecossistema crescente de soluções integradas para gerenciamento de políticas de segurança em nuvem, gerenciamento de segredos, e proteção de containers e desenvolvimento de aplicativos para ajudá-los a darem vida à criptografia, com máximo controle”.

Principais tendências globais:

- Dos países pesquisados, os EUA são os principais usuários de criptografia (70%, o que está 20% acima da média global) e de HSMs (72%, 23% acima da média global).
- O Reino Unido possui a maior taxa de criptografa das informações do cliente (59% contra a média global de 42%).
- A Suécia é o país que mais usa a criptografia com dispositivos IoT (47% amplamente implantados contra uma média global de 33%).

- Apesar da média global de 54%, Espanha, Japão e Hong Kong classificam a proteção de informações do cliente como o principal motivador para criptografar com taxas de 77%, 74% e 72%, respectivamente.
- Os entrevistados na Coreia estão planejando um grande aumento no uso de HSMs com criptografia de aplicativos nos próximos 12 meses - crescendo de 40% para 61%.

Principais tendências no Brasil:

- O uso de Criptografia e HSM (módulo de segurança de hardware) está defasado na maioria das regiões/países. No entanto, o uso de criptografia em serviços de nuvem pública no Brasil ultrapassa a maioria das regiões. Já o uso de HSM é forte com criptografia de big data, TLS/SSL, processamento de transação de pagamentos e emissão de credenciais e criptografia/assinatura de contêiner.
- A influência sobre a estratégia de criptografia é mais distribuída entre cargos do que em qualquer outra região/país (39% relatam que nenhuma função tem responsabilidade).
- O gerenciamento de chaves é o recurso de solução de criptografia mais importante (86% vs 68% na média global), seguido de perto pelo suporte para implantação em nuvem e local (79% vs 62% de média global).
- Os registros financeiros são de longe o tipo de dados mais criptografado (81% vs 55% da média global).
- A falta de pessoal qualificado é de longe a maior causa de dor no gerenciamento de chaves (71% vs 57% da média global).

Informação adicional

O Estudo Global de Tendências de Criptografia 2021 da Entrust em português está disponível em Estudo Global de Tendências de Criptografia 2021 da Entrust

Sobre a Entrust Corporation

A Entrust mantém o mundo se movendo com segurança, possibilitando identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo compras, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colaboradores e uma rede de parceiros e clientes globais em mais de 150 países, não é de se admirar que as organizações mais confiáveis do mundo confiem em nós. Para mais informações, visite www.entrust.com.