Como Manter os Dados Protegidos em um Mundo Multicloud Híbrido

UM ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) MATERIAL TÉCNICO

PREPARADO PARA A IBM

POR PAULA MUSICH

JUNHO DE 2020

EMA™
GERENCIAMENTO DE DADOS E TI
PESQUISA | ANÁLISES DO SETOR | CONSULTORIA

Sumário

COMO MANTER OS DADOS PROTEGIDOS EM UM MUNDO MULTICLOUD HÍBRIDO

A colaboração digital e o compartilhamento de dados inerente a ela são uma realidade na empresa moderna e conectada à nuvem. A premissa tradicional de confiança dada a funcionários e contratados com credenciais apropriadas que operam dentro do perímetro rígido da empresa foi estendida às arquiteturas modernas baseadas em nuvem. As equipes que trabalham juntas para bater as metas da empresa podem compartilhar dados livremente entre aplicações híbridas privadas em nuvem híbrida, multicloud e no local (on-premises). Na maioria dos casos, esses dados são compartilhados em texto não criptografado. Pesquisas sobre dados na nuvem mostram que apenas 9,4% dos dados da nuvem são criptografados. Se esses dados forem expostos na internet ou vazarem, a organização terá pouco ou nenhum meio de recuperá-los ou apagá-los. Nesses casos, sem o uso de uma criptografia em todos os lugares, depois que os dados são roubados, não há mais o que fazer.

Todas essas atividades são baseadas no compartilhamento de dados em um ecossistema tênue de confiança que a criptografia poderia fortalecer. Infelizmente, a criptografia geralmente não é usada devido à compartimentação de tecnologias que protegem os dados nos diversos estados em que se encontram e ao aumento do atrito do usuário nas duas pontas da transação. Para piorar a situação, se o destinatário dos dados quebrar a confiança e os compartilhar com outras pessoas (seja de propósito ou por acidente), o proprietário não terá conhecimento desse fato, a menos que a parte infratora o informe. Os dados corporativos devem ser melhor e mais amplamente protegidos por meio de um conjunto holístico e altamente integrado de tecnologias. Isso ajudará os proprietários dos dados a manter o controle e rastreá-los ao longo do ciclo de vida.

O Cubo de McCumber e as Três Dimensões do Risco

Em 1991, John McCumber lançou um modelo de risco de segurança virtual, hoje conhecido como Cubo de McCumber. Esse modelo foi revolucionário na maneira como descreve os fatores de risco de segurança virtual como um cubo tridimensional. Cada uma das faces visíveis do cubo tem três aspectos diferentes de risco virtual que precisam ser gerenciados. Cada uma das interseções tridimensionais representa a união de três componentes, um de cada face. O minicubo mais à frente, destacado em vermelho, é a interseção confidencialidade/tecnologia/processamento. Isso representa a ideia de um controle de tecnologia para proteger a privacidade dos dados no processamento.

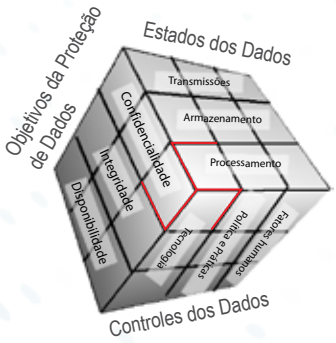

Figura 1: Cubo de McCumber

Este material discute como a aplicação adequada da criptografia em cada etapa do ciclo de vida, da transmissão, do armazenamento e do processamento dos dados criará controles mais eficazes que aumentam a proteção e a privacidade. Na era da colaboração e do compartilhamento de dados digitais, esses controles reduzem o risco de exposição, vazamento, perda e roubo de dados. Este material destaca o conceito de entrega de confidencialidade por meio de novos controles de criptografia e como os controles dos dados afetam e são afetados pelo uso da criptografia em todos os lugares ao longo do ciclo de vida dos dados.

CRIPTOGRAFIA DE DADOS NA TRANSMISSÃO

A Interseção Confidencialidade, Tecnologia e Transmissão

A aplicação adequada da criptografia pode reduzir significativamente as perdas por roubo de dados. No Cubo de McCumber, a interseção tecnologia, confidencialidade e transmissão foi tratada pelo uso do protocolo TLS (Transport Layer Security) e seu antecessor, o SSL (Secure Sockets Layer). Até o final de 2019, a proteção de dados na transmissão pela internet havia melhorado bastante, com a criptografia de quase 95% do tráfego focado no site.

Existem prós e contras no uso da criptografia baseada em transporte em todo o ambiente interno. O principal benefício para o proprietário dos dados é o nível mais alto de confidencialidade que a criptografia oferece durante a migração para fins comerciais legítimos. O principal problema para o proprietário dos dados é o nível mais alto de confidencialidade que a criptografia oferece aos black hats quando estes estão roubando os dados. O pessoal do monitoramento de segurança geralmente não vê o que está no tráfego ou precisa investir em ferramentas de proxy de gateway para interceptar o tráfego com um ataque man-in-the-middle autorizado para ver o que está acontecendo. Esse tipo de inspeção também pode aumentar a latência nas aplicações, criando outros problemas e dificultando ou encarecendo o uso da criptografia baseada em transporte.

Criar e implementar os padrões de criptografia de transporte de dados para SSL e TLS nos navegadores é logisticamente mais fácil do que a criação e a aplicação de políticas internacionais e a chave de compartilhamento. No entanto, a criptografia cria uma falsa sensação de segurança para muitos usuários da internet. Eles acreditam que os dados transportados estão seguros porque são criptografados, mas depois que passam da transmissão para o processamento ou o armazenamento, a segurança do transporte TLS se dissolve, e os dados ficam mais suscetíveis a ataques.

Também é interessante observar que, mesmo antes do boom da criptografia de transporte, o número de ataques bem-sucedidos à criptografia de transporte era baixo e o número de registros roubados dos dados em repouso era alto. O roubo de dados em trânsito é uma tarefa mais complexa que requer mais configuração técnica e pontualidade, especialmente em dados direcionados, do que para roubar dados em repouso.

CRIPTOGRAFIA DE DADOS EM REPOUSO/NO ARMAZENAMENTO

A Interseção Confidencialidade, Armazenamento e Tecnologia

Os dados em repouso são de longe o maior alvo de roubo. Embora os números variem consideravelmente dependendo da organização que os informa, os números avançados de segurança baseada em risco identificam mais de quatro bilhões de registros vazados em 2016, mais de sete bilhões em 2017, mais de cinco bilhões em 2018 e pouco menos de oito bilhões em 2019. O Thales Security 2019 Data Threat Report estimou que menos de 30% das organizações implantam criptografia em ambientes críticos, e a quantidade de dados criptografados não chega a 10%.

Historicamente, os sistemas de criptografia provaram ser caros e difíceis de instalar, configurar, operar e manter. Os usuários corporativos que interagem com os dados criticam o atrito que eles levam ao trabalho e os impactos negativos no desempenho, até ao ponto de causar solicitações com falha/perda. Assim, na briga entre usabilidade e segurança, a usabilidade ainda está ganhando.

No armazenamento, vencer esses obstáculos requer lidar com a usabilidade subjacente do sistema de criptografia, concentrando-se no gerenciamento das chaves de criptografia. A usabilidade das ferramentas de criptografia de dados para remover o atrito dos clientes de dados, sejam funcionários internos ou externos, também é importante.

CRIPTOGRAFIA DE DADOS NO PROCESSAMENTO E NO USO

A Interseção Confidencialidade, Processamento e Tecnologia

O modelo do Cubo de McCumber identifica o processamento de dados, que pode ser aplicado ao processamento automatizado em um sistema de computadores ou ao tratamento manual dos dados antes ou depois da digitalização.

Criptografia de Dados no Processamento

Proteger os dados em trânsito na aplicação é provavelmente o aspecto mais difícil do controle de risco. O primeiro ponto de controle é o provisionamento normal de acesso. Se alguém não tiver acesso à porta da frente da aplicação, acessar os dados será muito mais difícil. Além dessa barreira, o foco do controle está mais frequentemente na proteção física de servidores ou no fortalecimento dos componentes eletrônicos que compõem o sistema. Ataques aos dados em processamento exigem acesso direto ao sistema para sondagem, acesso direto aos dados em operação ou malware inserido na aplicação ou nos drivers do sistema para canalizar os dados enquanto a aplicação está em operação.

Criptografia de Dados em Uso

Dependendo de como o processamento está estruturado, é necessário adicionar controles para se defender de pessoas que estão tentando extrair os dados enquanto eles estão sendo manipulados/processados. Deve-se tomar cuidado para garantir que os dados corretos sejam direcionados à pessoa certa. Tradicionalmente, é aqui que a criptografia é mais implantada. Desde que apenas as pessoas adequadas sejam incluídas no círculo de confiança, o proprietário dos dados pode ter certeza de que eles estão seguros. No entanto, até recentemente, a limitação crucial era que, uma vez que os dados deixavam o proprietárioainda era possível alguém descriptografar as informações e encaminhá-las para outra parte sem o conhecimento do proprietário.

Defesa Contra Ataques ao Processamento e Uso

Embora o antimalware seja útil para lidar com malwares usados em ataques, bloqueios e guardas de segurança são mais empregados para manter as pessoas afastadas dos sistemas de processamento. A criptografia pode ser aplicada ao processamento e até mesmo em algumas áreas de uso para limitar a exposição dos dados durante o processamento. Existem projetos de pesquisa em andamento, como aqueles com criptografia homomórfica, que exploram como as informações de consulta relevantes podem ser extraídas dos dados criptografados sem revelar os próprios dados. Eles estão se mostrando promissores, mas provavelmente levarão anos para chegar ao mercado.

Recentemente, os recursos de criptografia evoluíram para vincular direitos persistentemente aos dados durante todo o ciclo de vida. Esse é um enorme avanço, permitindo que o proprietário dos dados adicione, altere ou revogue permissões de uso de qualquer usuário, mesmo após o compartilhamento.

REDUÇÃO DE RISCOS COM CRIPTOGRAFIA EM TODOS OS LUGARES

Proteção de Dados e Privacidade em Todos os Locais e Estados dos Dados

Em 2018, as perdas por roubo de identidade foram estimadas em US$ 1,7 bilhão apenas nos Estados Unidos. A Comissão sobre Roubo de Propriedade Intelectual dos EUA estima que os roubos de propriedade intelectual de empresas americanas pelos chineses custam até US$ 600 bilhões por ano. Para evitar esse prejuízo e garantir a real proteção ao longo do ciclo de vida dos dados, é necessária uma mudança fundamental na abordagem. Até recentemente, quando os dados eram entregues ao destino, eles saíam do controle do custodiante inicial. Confiança total era conferida à próxima pessoa na cadeia de posse dos dados. Se essa pessoa decidisse estender ainda mais o círculo de confiança, não precisaria da permissão do proprietário inicial.

Os proprietários dos dados são obrigados a compartilhar apenas as informações necessárias, geralmente tomando decisões sobre o que é necessário enquanto os aspectos dos requisitos ainda são fluidos. Isso os coloca em uma posição precária. O que foi aprovado para compartilhamento interno no passado pode, mais tarde, ser determinado como fora do escopo. No atual contexto de dados compartilhados, com ou sem criptografia, proteger a organização implementando uma política alterada e recuperar os dados agora fora do escopo requer um esforço significativo para desfazer. Na maioria dos casos, é impossível verificar se todas as cópias internas foram devolvidas ou destruídas. Mesmo sem má intenção, cópias de dados compartilhados podem ter sido capturadas em repositórios alternativos, como backups, e-mail, pastas compartilhadas e drives pessoais. O conceito de criptografia em todos os lugares resolve esse problema, mantendo os dados protegidos e privados em toda a empresa, estejam eles em repouso, em trânsito, no armazenamento ou na nuvem.

A Interseção Confidencialidade, Políticas e Processos, e Fatores Humanos

Políticas e processos são os elementos fundamentais de qualquer sistema criptográfico sólido. A política determina o que pode e o que não pode ser compartilhado e as partes que fazem parte do círculo de confiança de cada elemento de dados protegido. Infelizmente, para sistemas criptográficos tradicionais, as políticas se baseiam com mais frequência em um nível de confiança de que os humanos seguirão as políticas prescritas para garantir que os dados permaneçam onde e com quem eles pertencem. Se os fatores humanos cometerem um erro, pode ocorrer vazamento e exposição dos dados.

O algoritmo de criptografia pode ser indecifrável e as políticas muito bem redigidas, mas nada disso importa quando uma pessoa decide descumprir as regras ou comete um erro. Os dados protegidos estarão em risco. Na maioria dos casos, isso não passa de um incômodo, mas em outros pode ser devastador, causando enormes impactos financeiros e de reputação. O roubo de propriedade intelectual na American Semiconductor é um excelente exemplo dos danos que as organizações podem sofrer. O preço das ações da American Semiconductor caiu quase 50% após a descoberta do roubo.

O primeiro passo para proteger os dados de fatores humanos é reduzir o número de pessoas que podem revelar ou compartilhar dados não protegidos. O proprietário dos dados sempre pode manter o controle dos direitos aos dados, e esse controle pode ficar longe dos mecanismos de entrega ou dos ambientes de compartilhamento. Isso cria dois controles que podem impedir a liberação não intencional dos dados.

O conceito de criptografia em todos os lugares requer governança proativa dos dados durante todo o ciclo de vida deles. A proteção dos dados deve ser transformada em políticas executáveis que criem um sistema de criptografia incorporado nos dados. Se as políticas forem aplicadas aos dados antes da distribuição interna e se mantiverem nos dados enquanto eles são migrados, os proprietários poderão ter certeza de que os direitos que eles definiram nesses dados permanecerão com eles em qualquer estado em que os dados estiverem. O proprietário também deve definir por quanto tempo esses direitos serão válidos antes da necessidade de uma nova verificação do servidor de controle, mantendo assim um controle constante sobre quem pode acessar os dados compartilhados, independentemente de onde eles trafegam na empresa. A tecnologia é usada para monitorar e aplicar políticas ao longo do ciclo de vida dos dados. Isso gera uma proteção persistente que atende às demandas variáveis da empresa, desde mudanças de pessoal e parceiros de negócios até outros requisitos operacionais.

As permissões atribuídas são válidas e permanecem protegidas dentro de dados não estruturados. Quando há tentativa de acesso aos dados, uma solicitação é enviada ao sistema chave de gerenciamento no ambiente do proprietário dos dados. Se o solicitante tiver os direitos apropriados, um token temporário será enviado de volta para desbloquear as informações e permitir que os direitos sejam exercidos. Dados estruturados podem ser protegidos nos níveis do atributo ou da tabela. Os dados mantidos no local do destinatário permanecem sob o controle do proprietário o tempo todo. Se a qualquer momento o proprietário dos dados determinar que os parâmetros de acesso precisam ser alterados ou totalmente revogados, ele só precisará alterar a política, e ela será aplicada às cópias remotas dos dados.

Aplicação de política adaptativa para proteção de dados ao longo do clico de vida

Em qualquer momento em que o relacionamento de compartilhamento for encerrado ou o proprietário dos dados determinar que os direitos exigem uma alteração, ele poderá atualizar os direitos no mecanismo de políticas. Na próxima solicitação, quando os direitos forem verificados, as permissões atualizadas serão aplicadas. E isso acontecerá para todas as cópias criadas antes de serem acessadas. Se a revogação total for aplicada, as chaves serão destruídas, tornando os dados criptografados inertes. Como o destinatário não tem acesso às chaves, os dados permanecem protegidos do uso não autorizado.

PROTEÇÃO DE DADOS COM CRIPTOGRAFIA EM TODOS OS LUGARES

Uma política aplicada à tecnologia, direitos persistentes aos dados, um sistema robusto de gerenciamento de chaves e um forte conjunto de criptografia criam juntos uma base sólida para uma defesa profunda. O que torna a criptografia em todos os lugares única em conceito e aplicação é a imposição persistente de políticas, criando proteção contínua entre os datacenters e a nuvem para manter o controle dos dados qualificados, que podem ser acessados por meio de uma conexão JDBC. Para tornar o conceito de criptografia em todos lugares uma realidade funcional, os proprietários dos dados devem aproveitar um ecossistema de tecnologia, não apenas apontar soluções. Hoje, as soluções pontuais são boas no que fazem, mas não foram desenvolvidas para uma criptografia que abrange todas as partes do ecossistema. As integrações amplas não estão onde precisam estar. Assim, alcançar a proteção abrangente dos dados requer integrações estreitas com alta interoperabilidade como objetivo de projeto. Dessa forma, os dados são protegidos em cada fase da existência.

CASOS DE USO DA CRIPTOGRAFIA EM TODOS OS LUGARES

Os casos de uso mostrados aqui identificam uma combinação de componentes da IBM e de outras empresas que podem ser usados para oferecer proteção e privacidade contínuas dos dados. Embora todas as fases do conceito de criptografia em todos os lugares possam ser alcançadas por meio de soluções de outros provedores, a IBM é a única empresa que atualmente oferece um ecossistema fortemente integrado de soluções no IBM Z para fornecer proteção e privacidade contínuasdos dados qualificados. A seguir estão os componentes que fazem parte dos casos de uso:

1. IBM z15 executando o z/OS ou Linux no Z usando recursos de criptografia em todos os lugares
2. IBM Data Privacy Passports
3. Adaptadores IBM Z Fibre Channel
4. IBM DS8900F Storage
5. IBM Z Fibre Channel Endpoint Security
6. IBM Hyper Protect Virtual Servers
7. TLS ou IPSec
8. Nuvens públicas e/ou privadas da sua escolha
9. IBM Data Privacy for Diagnostics (provedores)
10. Um módulo de segurança de hardware (HSM)
11. Hardware para processamento e armazenamento de dados

Caso de Uso 1: Proteção de Dados e Privacidade na Família de Soluções IBM no Local (ON-PREMISES)

Para muitos ambientes exigentes, como varejo de alto volume, grandes bancos, processamento de cartão de crédito e outros pagamentos em grande escala, uma infraestrutura de processamento da IBM provavelmente já está implementada, e o z15 é a tecnologia de base. No z15, a criptografia em todos os lugares pode ser ativada para proteger dados e processamento qualificados dentro do sistema. A proteção e a privacidade dos dados qualificados podem ser estendidas dos ambientes IBM z15 para o restante da empresa com os controles de política apropriados do Data Privacy Passports.[1] O Passport Controller para IBM Data Privacy Passports pode ser instalado para manter e gerenciar direitos e verificações de direitos de dados qualificados de fontes de dados que podem ser acessadas por meio de uma conexão JDBC. Com a criptografia em todos os lugares protegendo os dados qualificados no local, o foco pode mudar para a proteção dos dados que precisam fluir para dentro e para fora do sistema.

1 Isenção de responsabilidade: O Data Privacy Passports tem suporte para fontes de dados que podem ser acessadas por meio de uma conexão JDBC.

Depois que as políticas são ativadas, os dados não precisam permanecer no IBM Z para serem protegidos. Os dados associados às políticas são criptografados antes de sair do armazenamento do host. Operando no ecossistema completo da IBM, adaptadores e switches IBM Fibre Channel com taxa de transferência ultra-alta podem ser usados para migrar dados muito rapidamente dentro do data center. Eles são compatíveis com outros sistemas que fazem interface com o Fibre Channel, mas se forem usados com o armazenamento IBM DS8900F, as proteções poderão ser aumentadas com a adição do IBM Fibre Channel Endpoint Security, que protege os dados em trânsito no nível do hardware. A combinação Fibre Channel e DS8900F também adiciona criptografia e autenticação de dados para os dados em trânsito.

Caso de Uso 2: Proteção de Dados e Privacidade em Data Centers Corporativos Heterogêneos

A maioria das organizações com outras plataformas de computação já implantadas não está em condições de substituir totalmente a infraestrutura atual. O Data Privacy Passports foi desenvolvido para proteger com robustez os dados críticos e sensíveis que residem em praticamente qualquer hardware conectado à rede nesses data centers. Depois que a conexão com o IBM z15 é estabelecida, a proteção dos dados qualificados pode ser aplicada em qualquer lugar do data center pela duração da existência dos dados. O z15 foi projetado para oferecer segurança com certificação FIPS 140-2 nível 4 para HSM criptográfico. Ele também foi desenvolvido para oferecer velocidade e é capaz de processar mais de 19 bilhões de transações criptografadas por dia.[2]

Caso de Uso 3: Proteção de Dados e Privacidade em Qualquer Nuvem e em Dados Compartilhados

O IBM z15 com Linux no Z oferece o IBM Hyper Protect Virtual Servers para criar uma infraestrutura de nuvem privada segura. Com o Hyper Protect Virtual Servers, os proprietários mantêm total controle das cargas de trabalho e dos dados. Nem mesmo os administradores do sistema ou da nuvem têm acesso às cargas de trabalho, a menos que permitido pelo proprietário dos dados. O Data Privacy Passports pode ser aplicado aos dados qualificados mesmo em ambientes multicloud, hiperconvergentes e altamente distribuídos, desde que a nuvem tenha acesso ao Passport Controller que aplica as políticas. Túneis TLS podem ser adicionados aos gateways da internet para aumentar a segurança do transporte, onde os endpoints de comunicação precisam ficar ocultos da visualização na internet.

Com a aplicação dos controles de dados, qualquer proprietário pode compartilhar dados com qualquer pessoa da empresa. Não importa quais são as necessidades da empresa, o acesso, a distribuição e a expiração dos dados ficam sob o controle total do gerente de políticas. Os proprietários dos dados podem ter total confiança de que, quando as necessidades mudam, a política pode mudar facilmente para se adaptar a elas. Quando a necessidade não existir mais, a proteção e a privacidade poderão permanecer intactas. Os dados qualificados em qualquer local da empresa podem se tornar inertes, destruindo as chaves locais por meio do gerenciamento de políticas usando o Data Privacy Passports.

Caso de Uso 4: minimizar os impactos da shadow IT

Shadow IT acontece quando alguém da organização decide migrar ou copiar dados para um local não autorizado. Fazer isso sem permissão cria brechas na segurança e aumenta os riscos para a empresa. O vazamento ou a exposição dos dados, mesmo acidentalmente, pode ter grandes consequências financeiras e de reputação. A implementação do Data Privacy Passports em todos os dados estruturados críticos ou sensíveis minimiza bastante o impacto da shadow IT. Mesmo se os dados forem copiados e migrados, eles ainda serão inúteis sem as permissões. Se alguém com acesso a um banco de dados controlado, mas sem permissões de acesso aos dados, migrar os dados para um local não autorizado, eles permanecerão criptografados, minimizando a exposição da empresa.

2 Isenção de responsabilidade: Essa taxa de transação se baseia em medições internas de uma configuração do z15 que consiste em duas LPARs de 8 vias e um ICF de 4 vias em execução com criptografia de conjunto de dados e criptografia CF ativada. Com base nesses resultados, as taxas de transação do z15 em tamanho real foram projetadas usando o padrão LSPR MIPS. O desempenho varia de usuário para usuário.

RESUMO: PROTEÇÃO DOS DADOS EM TODO O CICLO DE VIDA COM CRIPTOGRAFIA EM TODOS OS LUGARES

Manter a confidencialidade dos dados fornece às partes proprietárias vantagens de negócio e operacionais. Apesar disso, praticamente todas as organizações subutilizam a criptografia para proteger os dados, e muitas estão sendo vítimas de agentes mal-intencionados e indivíduos descuidados.

Dentro de uma organização, o principal problema da proteção de dados é que as ferramentas mais usadas requerem interfaces distintas e políticas separadas para proteger os dados em diferentes estados. As ferramentas e interfaces de gerenciamento operam de forma independente, com fracas integrações. A independência dificulta a coesão total e o teste e a aplicação das políticas, e muitas vezes deixa brechas na proteção.

Nos casos de colaboração, o atrito do usuário e a manutenção do controle dos dados são dois dos aspectos mais difíceis. O maior atrito do usuário afasta as pessoas das plataformas de criptografia tradicionais. A falta de flexibilidade no controle e na aplicação das políticas para os dados em campo faz com que os proprietários e custodiantes de dados relutem em implantar proteções.

Embora as tecnologias para proteger os dados em cada etapa do ciclo de vida sejam comuns, as experiências regulares de mudanças nos dados ao longo do ciclo de vida dificultam certos aspectos do gerenciamento da criptografia de dados. Independentemente dos impedimentos, as empresas devem definir requisitos de negócios para proteger todos os dados confidenciais na transmissão, no processamento e no armazenamento. As análises de custo/benefício sempre devem ser realizadas, mas uma avaliação realista quase sempre mostra que há vantagens em expandir o uso da criptografia para dados sensíveis e confidenciais.

Esteja preparado. Em alguns casos, a transição para armazenamentos de dados criptografados pode levar anos. Embora a quantidade de dados seja um fator, ela não é o mais impactante. Os requisitos mais difíceis de acomodar envolvem catalogar e definir a diversidade de tipos e locais dos dados, direitos do usuário e da aplicação e as interfaces da aplicação para interação e compartilhamento de dados. As aplicações herdadas precisam de uma atualização ou substituição para serem executados com criptografia, mas se os dados fornecerem vantagens reais de negócios e/ou operacionais e, portanto, vale a pena mantê-los, vale a pena protegê-los.

Para organizações com dados altamente sensíveis ou sistemas transacionais de alto volume, a execução do IBM z15 com o z/OS ou o Linux no Z com criptografia em todos os lugares e o Data Privacy Passports deve ser uma consideração primordial. O ecossistema do IBM z15 oferece desempenho incomparável para aplicações internas ou como base para qualquer tipo de ambiente em nuvem que está sendo construído. Sua arquitetura de segurança nativa inclui chips aceleradores criptográficos integrados, serviços e chips de módulo de segurança de hardware embutidos, serviços de criação de chaves de criptografia e gerenciamento do ciclo de vida, interfaces multi-Gbps criptografadas e armazenamento de alta velocidade compatível com criptografia. A plataforma oferece confidencialidade persistente de dados, gerenciamento de políticas e aplicação compatíveis com qualquer requisito de criptografia. Atualmente, não existe um sistema de produção em massa mais abrangente e eficiente.

Independentemente das soluções escolhidas, a implementação de uma estratégia de criptografia em todos os lugares reduz significativamente os custos de uma violação de privacidade e de compliance. Se o proprietário dos dados puder fornecer provas razoáveis de que algum dado vazou, foi roubado ou comprometido, a notificação, a investigação forense, a restituição da vítima e as multas serão significativamente reduzidas e, às vezes, eliminadas. O impacto negativo na imagem da marca também pode ser significativamente reduzido/eliminado. A redução desses fatores ajuda a diminuir o reconhecimento dos lucros.

Para saber mais sobre como sua organização pode se beneficiar da abordagem da IBM para um ecossistema abrangente de criptografia de dados usando o IBM z15 com criptografia em todos os lugares e o Data Privacy Passports, visite: https://www.ibm.com/br-pt/it-infrastructure/z/capabilities/enterprise-security.

Sobre a Enterprise Management Associates, Inc.

Fundada em 1996, Enterprise Management Associates® (EMA) é uma empresa líder em análise de mercado que fornece uma visão profunda de todo o espectro de tecnologias de gerenciamento de dados e TI. Os analistas da EMA aproveitam uma combinação única de experiência prática, as melhores práticas do setor e conhecimento profundo das soluções de provedores atuais e planejadas para ajudar os clientes a alcançar os objetivos deles. Saiba mais sobre os serviços de pesquisa, análise e consultoria da EMA para usuários corporativos de linha de negócios, profissionais de TI e provedores de TI em www.enterprisemanagement.com ou blog.enterprisemanagement.com. Siga a EMA no Twitter, Facebook ou LinkedIn.

Sede da empresa:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Telefone: +1 303.543.9500
www.enterprisemanagement.com

3933,03022020-06032020.revision9