Residência de dados

Perspectivas da política da AWS

Julho de 2018

aws

[Perspectivas de política]

Avisos

Este documento é disponibilizado apenas para fins informativos. Ele relaciona as atuais ofertas de produtos e práticas da AWS a contar da data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento e de qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido "como está", sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais, condições ou seguros da AWS, suas afiliadas, fornecedores ou licenciadores. As responsabilidades e obrigações da AWS para com seus clientes são controladas por contratos da AWS, e este documento não modifica nem faz parte de qualquer contrato entre a AWS e seus clientes.

Contents

Introdução

Tendo em vista a complexidade do ambiente de computação atual, as organizações do setor público continuam tendo preocupações legítimas quanto à segurança de seus dados. Por esse motivo, alguns governos concluíram que a residência de dados obrigatória, ou seja, a exigência de que o conteúdo de todos os clientes processado e armazenado em um sistema de TI seja mantido dentro das fronteiras específicas de um país, oferece uma camada extra de segurança. A residência de dados reflete um conjunto de problemas associados principalmente com riscos de segurança percebidos (e, em alguns casos, reais) em torno do acesso a dados por parte de terceiros, inclusive por agências estrangeiras de execução da lei. Os clientes do setor público desejam a garantia de que seus dados estão protegidos contra acesso não desejado não somente de invasores nefastos, mas também de outros governos.

Uma postura rigorosa com relação à residência de dados restringe o uso de provedores de serviços em nuvem (CSPs) multinacionais e em larga escala, geralmente chamados de CSPs de "hiperescala". Preocupações gerais com a segurança cibernética, assim como a preocupação de determinados países com a possibilidade de extrapolação da vigilância governamental, contribuíram para um foco contínuo sobre a manutenção de dados dentro das fronteiras do país. Entretanto, essa restrição é contraproducente no que diz respeito ao objetivo de proteger com eficiência os dados do setor público. Tal como é analisado a seguir, os CSPs de hiperescala, que podem estar localizados fora do país, oferecem a toda a sua base de clientes a possibilidade de obter altos níveis de proteção de dados por meio da proteção de sua plataforma e de ferramentas prontas para seus clientes. Além de fazer isso, eles ao mesmo tempo preservam a soberania regulamentar do Estado-nação.

Os serviços de nuvem em hiperescala representam uma ruptura tecnológica transformacional em virtude do alto grau de eficiência, agilidade e inovação na segurança de nível internacional que eles oferecem para apoiar seus clientes. Os CSPs de hiperescala projetam, operam e mantêm produtos e serviços para atender a clientes de vários setores (comercial, público, regulamentado) e lidar com alguns dos riscos de segurança e vulnerabilidades mais prevalecentes. Os clientes contam com os produtos e serviços oferecidos pelos CSPs para incorporar práticas de segurança dinâmicas e responsivas contra ameaças em tempo real, e isso melhora drasticamente a postura de segurança de todos os clientes. Os CSPs, por sua vez, têm todos os devidos incentivos para manter uma segurança cibernética de nível internacional porque podem enfrentar consequências significativas a longo prazo, como impactos associados ao comprometimento de sistemas, perda de confiança dos clientes e danos à marca. Em outras palavras, para ser bem-sucedido, o CSP tem a obrigação de oferecer o que há de melhor em segurança. A segurança deve estar totalmente integrada ao projeto, ao desenvolvimento e às operações dos serviços em nuvem em hiperescala.

Este documento aborda o seguinte:

- Riscos de segurança reais e percebidos que são expressos pelos governos quando requerem residência de dados dentro do país.
- Impacto comercial, econômico e sobre o setor público de políticas de residência de dados dentro do país com foco em dados governamentais
- Fatores que os governos devem avaliar antes de impor exigências que podem restringir involuntariamente as metas de transformação digital do setor público e aumentar o risco à segurança cibernética.

Por que a residência de dados não oferece melhor segurança

A propriedade e o posicionamento geográfico dos dados tornaram-se um tópico fundamental para as iniciativas de segurança cibernética e política de nuvem ao redor do mundo. Tradicionalmente, ter posse e controle sobre dados empresariais confidenciais significava armazenar as informações localmente ou em instalações fisicamente acessíveis de propriedade de um prestador de serviço dentro do país. Ter propriedade total sobre a "pilha", das instalações físicas ao software dos servidores, era motivo para que as pessoas confiassem que seus dados tinham o máximo possível de proteção. Esse raciocínio ainda prevalece em vários governos.

Como a tecnologia evoluiu, três realidades fundamentais romperam com o modelo tradicional de "controle total sobre a pilha":

1. **A maioria das ameaças é explorada remotamente.** A localização física dos dados tem pouco ou nenhum impacto sobre as ameaças propagadas na Internet. Os sistemas conectados à Internet expõem uma organização a um amplo espaço de ameaças, todas elas propagadas de qualquer local. Por exemplo, o recente ransomware Petya afetou os serviços de saúde, debilitando suas operações e a capacidade de oferecer cuidados aos pacientes. Isso ocorreu em virtude de um malware propagado pela Internet que afetou seus datacenters locais. Apesar do enorme empenho para proteger sistemas interconectados por meio de firewalls e de outros dispositivos anti-invasão, a experiência demonstra que essa segurança de perímetro constitui uma parte ínfima da proteção de um sistema. Independentemente da localização física, quando os sistemas de TI estão conectados de alguma forma à Internet (ou a outras redes de vários participantes), mesmo que indiretamente, estão expostos a um risco considerável e suscetíveis a uma ampla variedade de ameaças de acesso lógico.

Independentemente da localização física, quando os sistemas de TI estão conectados de alguma forma à Internet (ou a outras redes de vários participantes), mesmo que indiretamente, estão expostos a um risco considerável.

2. **Os processos manuais apresentam risco de erro humano.** As falhas humanas de processo desempenham uma função na falha de causa raiz (quando não na causa de modo geral) da maior parte da segurança cibernética. Um exemplo comum é a falha na correção de sistemas vulneráveis com a publicação de atualizações de software vários meses antes de uma ameaça. O processo de atualização manual de sistemas com as correções mais recentes é difícil e sua realização regular é impraticável sem automação.

3. **As ameaças internas são um risco significativo prevalecente.** A vasta maioria dos principais casos de comprometimento de dados ocorreu em virtude de erros não intencionais ou de comportamentos mal-intencionados por parte de indivíduos que usaram contas autorizadas com direito de acesso aos dados. Nos últimos anos, as violações de alta visibilidade foram atribuídas principalmente a práticas inadequadas de higiene cibernética. Alguns dos cenários de ameaça a contas autorizadas mais comuns são:

    - Descuido: credenciais perdidas ou mal administradas que dão espaço para um invasor agir dentro de um sistema como usuário válido.
    - Engenharia social: invasões por phishing e ataques de engenharia social que levam enganosamente usuários ou administradores a revelar credenciais aos invasores.
    - Má intenção: a ameaça interna mais comum – agentes maldosos dentro da organização com intenções nefastas.

A localização física dos dados não tem nenhuma ligação com as realidades relacionadas acima.

Nas condições atuais, o gerenciamento de risco é uma tarefa ainda mais descomunal quando levamos em conta a tecnologia móvel e as inter-relações entre entidades externas e internas. Qualquer sistema conectado à Internet, direta ou indiretamente, apresenta um vetor de ataque convincente, seja qual for a localização física da infraestrutura ou do sistema. Como a tecnologia continua avançando e mudando as vulnerabilidades e os vetores de ameaça dos clientes, os governos devem reavaliar como estão modelando suas estratégias e a tolerância ao risco. Exemplos do mundo real mostraram que armazenar dados em seus próprios servidores, em seu próprio datacenter, em seu próprio país, não é de forma alguma uma base adequada para proteger seus dados.

Por exemplo, houve uma violação altamente ostensiva de uma agência do governo dos EUA que afetou mais de 20 milhões de funcionários federais em um ambiente local em virtude de credenciais de usuários comprometidas. Essas credenciais foram comprometidas e usadas pela rede em vários locais, ignorando todas as proteções oferecidas pelo ambiente local. A violação da agência do governo dos EUA é um bom exemplo das ameaças que surgem na Internet sem limites geográficos.

Esse problema se aplica a mais do que apenas sistemas voltados para a Internet. Os sistemas que não têm uma conexão direta com a Internet fornecem acesso aos usuários por conexões de rede privada virtual (VPN) de laptops, computadores domésticos ou dispositivos móveis. As violações não exigem acesso físico a um servidor, mas, em vez disso, exploram a falta de controles de segurança lógicos eficientemente implementados. Isso demonstra que os requisitos de residência de dados têm pouca relevância na proteção de informações das ameaças atuais mais prevalecentes. Assim, os requisitos de localidade geográfica têm pouca relevância para proteger as informações das ameaças atuais. Em vez disso, os melhores mecanismos para proteger, detectar, responder e recuperar é usar a segurança transformacional que um CSP de hiperescala oferece por meio da modernização e automação. CSPs de hiperescala, como a AWS, investem em e refletem as melhores práticas de segurança técnica e operacional, pois elas são essenciais para suas operações e ofertas. Os clientes se beneficiam de utilizar as ofertas de infraestrutura e nuvem de um CSP, como a AWS.

Tanto a Gartner[1] quanto a IDC[2], duas importantes organizações de pesquisa em TI, concluíram que a postura de segurança dos principais CSPs é igual ou melhor que a dos melhores datacenters corporativos e que a segurança não deve mais ser considerada o principal inibidor primário para a adoção de serviços em nuvem pública. Na verdade, as empresas realmente se beneficiam da segurança nativa na nuvem.

1 http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

2 Pete Lindstrom, "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment" (Avaliar o risco: sim, a nuvem pode ser mais segura que seu ambiente local), International Data Corporation (julho de 2015).

Por que a nuvem não impacta o risco de acesso compulsório

Para alguns governos, os requisitos de residência de dados têm o objetivo de atenuar os riscos relacionados ao acesso de outra entidade aos seus dados. Essa seção visa abordar o risco percebido da capacidade de uma entidade de "obrigar o acesso" aos dados de uma entidade soberana quando esses dados estiverem armazenados em um ambiente CSP de hiperescala. O conceito de divulgação obrigatória ou acesso obrigatório se refere aos direitos de acesso aos dados pelos governos ou seus agentes usando meios legais. O resultado desses tipos de direitos de acesso pode significar que as empresas estão sujeitas às leis e regulamentos em vigor nos níveis nacional, provincial e setorial em qualquer país, e podem ser compelidas a conceder acesso ou entregar dados sob essas leis ou regulamentos. A preocupação percebida é que a divulgação obrigatória possa potencialmente deixar o proprietário dos dados sem a capacidade de impedir o acesso aos seus dados por uma entidade que pretenda invocar a lei aplicável. No entanto, o acesso legal de uma nação soberana aos dados não é um problema específico da nuvem.

Possuir o sistema físico, seja diretamente ou por meio de um contrato terceirizado, não reduz o risco do acesso obrigatório, pois já existem outros mecanismos legais em vigor que dão aos governos de uma jurisdição os meios para solicitar acesso a dados armazenados em outra jurisdição. Por exemplo, Tratados Legais de Assistência Mútua (MLATs)[3] e Cartas rogatórias[4] já estavam em vigor para governar as solicitações de dados de uma nação soberana muito antes do surgimento da tecnologia de nuvem.

Em comparação com um ambiente local tradicional, a execução da lei geralmente deve enfrentar mais barreiras ao tentar obrigar um CSP a divulgar dados de outro cliente. A execução da lei não pode pesquisar ou apreender dados armazenados nos servidores de um CSP sem obedecer às estruturas legais que dão suporte a um conjunto restrito de objetivos da execução da lei. Além disso, os CSPs podem contestar solicitações que sejam abrangentes demais, excedam a autoridade do solicitante ou não estejam em total conformidade com a lei vigente.

Mais importante, os CSPs, como a AWS, estão totalmente comprometidos em fornecer aos clientes afetados notificações de solicitações de dados, permitindo que o cliente se envolva com as autoridades e/ou tome outras medidas apropriadas para impedir a divulgação indevida dos seus dados. É importante reconhecer que esse desafio complexo não é exclusivo do governo dos EUA ou das empresas sediadas nos EUA, pois qualquer empresa multinacional está sujeita às leis e regulamentos em vigor nos níveis nacional, provincial e setorial em qualquer país, independentemente da localização dos dados.

3 Os Tratados Legais de Assistência Mútua (MLATs) geralmente permitem a troca de evidências e informações em questões criminais e afins. https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

4 Cartas rogatórias são solicitações de tribunais de um país aos tribunais de outro país em que se pede a aplicação de uma lei que, se realizada sem a sanção do tribunal estrangeiro, poderia constituir uma violação da soberania desse país. As cartas rogatórias podem ser usadas para efetuar uma intimação ou obter evidência, se permitido pelas leis do país estrangeiro. https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html

Como limitar o acesso compulsório

Desde o século 20, muitos países usaram mecanismos legais para permitir o acesso a informações armazenadas no exterior em resposta a solicitações legais apropriadas de informações relacionadas a processos e investigações criminais. Por exemplo, uma empresa que esteja fazendo negócios no País X pode estar sujeita a uma solicitação legal de informações, mesmo que o conteúdo esteja armazenado no País Y sob estruturas legais bilaterais e multilaterais estabelecidas. Na maioria dos casos, o mecanismo legal reconhecido é um Tratado Legal de Assistência Mútua (MLAT).

Além dos acordos bilaterais MLATs (Tratado Legal de Assistência Mútua) entre os países, há também os principais MLATs regionais, como o MLAT interamericano, o MLAT entre União Europeia e Estados Unidos e o MLAT da ASEAN (Associação de Nações do Sudeste Asiático). Na ausência de um MLAT, os países podem obter Cartas rogatórias para buscar assistência de governos estrangeiros. As leis de cada jurisdição terão critérios que devem ser atendidos para que o órgão de execução da lei apropriado faça uma solicitação válida. Por exemplo, a agência governamental em busca de acesso talvez precise obter uma ordem judicial ou um mandado mostrando que há um motivo válido para solicitar acesso ao conteúdo. Embora sejam mecanismos legítimos, esses instrumentos legais não tinham como objetivo conceder acesso à execução da lei aos dados em um mundo digital.

> As leis que regem o acesso a dados armazenados no exterior por agências de execução da lei em suporte à investigação de crimes graves, como terrorismo, não foram escritas com a tecnologia moderna em mente. Isso resultou em casos em que empresas de tecnologia que cumpriam um mandado judicial sob as leis de um país também enfrentavam o risco de violar as leis de outro país que proibiam a divulgação. A lei CLOUD fornece uma nova estrutura para contestar solicitações de execução da lei quando houver acordos executivos vigentes entre os EUA e outro país, e também confirma, sob os princípios da cortesia entre nações, o direito de provedores de serviço a se oporem à divulgação de qualquer dado, caso isso entre em conflito com as leis de outro país, mesmo na ausência de um acordo executivo. Ela também permite que provedores de serviços em nuvem divulguem informações para governos que emitirem pedidos ou mandados de busca de informações baseados em fatos suficientes que demonstrem a causa provável de que um crime grave tenha ocorrido e que as informações solicitadas estejam diretamente relacionadas a esse crime.

Em um esforço para alinhar leis assíncronas com a tecnologia moderna, os EUA aprovaram a lei de esclarecimento do uso legal de dados no exterior (CLOUD) em março de 2018. A lei CLOUD fornece um terceiro mecanismo legal de abrangência internacional para adquirir dados armazenados no exterior por solicitações diretas emitidas ao provedor de serviço.[5] A lei CLOUD define procedimentos para os EUA fecharem Acordos executivos com outros países. Esses Acordos executivos buscam remover restrições legais à capacidade de certas nações estrangeiras buscarem dados diretamente de provedores dos EUA, desde que os EUA determinem que as leis do país estrangeiro protegem adequadamente a privacidade e as liberdades civis. De acordo com a lei CLOUD, os provedores de serviços em nuvem (CSPs) têm o direito de se opor a divulgar informações, caso isso entre em conflito com as leis de outro país. O MLAT, as Cartas rogatórias e os Acordos executivos sob a lei CLOUD fornecem mecanismos legais internacionais recíprocos para que a execução da lei acesse dados armazenados no exterior.

5 A lei CLOUD se aplica às empresas dos EUA e estrangeiras que operam nos Estados Unidos fornecendo "serviços de comunicação eletrônica" e/ou "serviços de computação remota", como negócios que oferecem serviços de e-mail, sistema de mensagens eletrônicas ou armazenamento na nuvem para o público.

As Leis nacionais de um país geralmente se aplicam a todas as empresas em operação naquele país, independentemente de onde a empresa está incorporada ou se as informações estão armazenadas na nuvem, em um datacenter local ou em registros físicos. Conforme as nações continuam se digitalizando e avançando em direção a sociedades modernas baseadas em informações, regimes legais de acesso compulsório em apoio a investigações de crimes graves que impactam a segurança nacional, como o terrorismo, também estão evoluindo. A promulgação da lei CLOUD é outra estrutura que visa fortalecer o devido processo legal para solicitação de execução da lei nesse contexto moderno.

Restringir os CSPs a uma única jurisdição não isola melhor os dados em relação ao acesso governamental

Uma análise jurídica independente entre os primeiros governos que adotaram a nuvem avaliou as leis específicas do país que regulamentam o acesso das entidades de aplicação da lei a dados baseados na nuvem armazenados no exterior. Esse estudo avaliou dez jurisdições internacionais – Alemanha, Austrália, Canadá, Dinamarca, Espanha, EUA, França, Irlanda, Japão e Reino Unido – e constatou que restringir os CSPs a uma única jurisdição não isola melhor os dados em relação ao acesso governamental.

A realidade é que esse acesso compulsório ocorre em um número muito limitado de casos, e geralmente somente quando há uma necessidade extrema de informações (isto é, para prevenir eventos relacionados a terrorismo). Para atenuar até mesmo esse baixo risco, as organizações podem realizar auditorias e desenvolver suas próprias proteções com os serviços em nuvem disponíveis. Na AWS, atenuações como criptografia de dados em repouso e em trânsito, distribuição e sanitização de dados e destruição de mídias e estratégias de tokenização podem ser empregadas para uma fração da carga de recursos comparada a uma solução no local.

A AWS é cautelosa em relação à proteção do conteúdo dos clientes, independentemente de onde venha uma solicitação de conteúdo ou de quem seja o cliente. A AWS não revelará o conteúdo do cliente, a menos que seja obrigada a fazer isso com uma ordem vinculativa e legalmente válida, como uma intimação ou uma ordem judicial. A AWS examina atentamente cada solicitação para validar a sua precisão e verificar se está em conformidade com a lei vigente. A AWS contestará solicitações que sejam abrangentes demais, excedam a autoridade do solicitante ou não estejam em total conformidade com a lei vigente. A menos que seja proibido por lei, a AWS também tentará redirecionar a solicitação diretamente para o cliente, dando a ele uma oportunidade de tomar uma atitude contra a solicitação. Informações adicionais podem ser encontradas em nosso relatório de transparência mais recente e em nossas Diretrizes da Amazon para execução da lei.[6]

6 http://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

Por que o risco de acesso não autorizado é menor na nuvem

Para alguns governos, os requisitos de residência de dados têm o objetivo de atenuar os riscos relacionados ao acesso de outra entidade aos seus dados. Esta seção visa abordar o aumento percebido no risco de acesso não autorizado ao usar um CSP de hiperescala. O acesso não autorizado é a ameaça mais comum feita por adversários tentando obter acesso aos dados do cliente usando diversos meios. O acesso não autorizado pode incluir preocupações com acesso de terceiros, incluindo a possibilidade de ameaças internas ou agentes maliciosos externos.

Os requisitos de residência de dados falham ao tratar dos caminhos comuns que os invasores usam para obter acesso. A exploração desses vetores quase sempre resulta de uma falha nas disciplinas básicas de higiene cibernética, como gerenciamento de inventário do sistema, gerenciamento de configuração, criptografia de dados e gerenciamento de acesso privilegiado.

Como atenuar o acesso não autorizado

Evitar o acesso não autorizado exige a prática de higiene de segurança adequada e a implementação de habilidades robustas de prevenção e investigação. Por exemplo, os sistemas devem ser projetados para limitar o "raio de detonação" de qualquer invasão, para que um nó comprometido tenha impacto mínimo em qualquer outro nó da empresa. CSPs de hiperescala como a AWS fornecem um ambiente completo de ferramentas de segurança para permitir que os clientes mantenham suas comunicações criptografadas e implementem proteções contra violações para amenizar o risco de acesso não autorizado. A AWS não tem visibilidade nem conhecimento do conteúdo da conta dos clientes, inclusive sobre se o conteúdo inclui ou não informações pessoais. Os clientes da AWS podem usar diversas técnicas, como criptografia,[7] tokenização, decomposição de dados e simulação cibernética para tornar o conteúdo ininteligível para a AWS ou outras partes que tentem acessar seu conteúdo.

- Criptografia – a criptografia adequada dos dados pode torná-los ilegíveis. Isso significa que armazenar dados criptografados na nuvem, independentemente do local, pode fornecer proteção apropriada contra a grande maioria das ameaças de exfiltração. É importante que as chaves de criptografia dos dados sejam cuidadosamente gerenciadas a fim de manter proteções reforçadas contra qualquer tentativa de interceptação. A AWS oferece serviços que podem fornecer esses recursos em nível empresarial com o AWS CloudHSM or AWS Key Management Service (KMS).[8] O grau de controle sobre o método de criptografia e o armazenamento e gerenciamento das chaves de criptografia usadas com os dados fica a critério dos clientes.[9]

---

7 A AWS permite que os clientes usem seus próprios mecanismos de criptografia em quase todos os serviços da AWS, incluindo o Amazon S3, o Amazon EBS, o Amazon DynamoDB e o Amazon EC2. Os túneis IPSec para a VPC também são criptografados. O Amazon S3 também oferece criptografia no servidor como opção para os clientes. Os clientes também podem usar tecnologias de criptografia de terceiros.

8 O serviço AWS CloudHSM (módulo de segurança de hardware) permite que você proteja as chaves de criptografia com módulos HSM projetados e validados de acordo com padrões governamentais (FIPS 140-2 nível 3) para o gerenciamento seguro de chaves, incluindo proteções robustas contra adulterações. O AWS KMS, validado pelo FIPS 140-2 nível 2, fornece um serviço semelhante, porém com melhor escalabilidade e integração mais profunda com uma ampla variedade de serviços da AWS, de forma que as proteções são fornecidas automaticamente com simples alterações na configuração do serviço. Usando um desses serviços, é possível gerar, armazenar e gerenciar com segurança as chaves criptográficas usadas na criptografia de dados de modo que elas sejam acessadas apenas por você. Para obter detalhes, consulte https://aws.amazon.com/pt/cloudhsm/ e https://aws.amazon.com/pt/kms/.

9 Os detalhes das opções de criptografia da AWS podem ser obtidos pelos seguintes links: (1) Proteção de dados em repouso com criptografia, (2) Proteção de dados usando criptografia no Amazon S3, (3) Detalhes da criptografia do AWS Key Management Service e (4) Visão geral dos processos de segurança da AWS.

- Tokenização – processo que permite que você defina uma sequência de dados para representar uma informação confidencial (por exemplo, um token que representa o número de cartão de crédito de um cliente). Um token não possui significado isoladamente e não pode ser mapeado de volta para o dado que representa sem o sistema de tokenização. É possível criar cofres de tokens nas VPCs para armazenar informações confidenciais em formato criptografado e compartilhar esses tokens com serviços aprovados para transmitir dados ofuscados. Além disso, a AWS tem diversos parceiros especializados em fornecer serviços de tokenização integrados com bancos de dados populares e outros serviços de armazenamento.
- Decomposição de dados – processo que reduz os conjuntos de dados em elementos irreconhecíveis que por si sós não têm nenhum significado.[10] Esses elementos, ou fragmentos, são armazenados de forma distribuída para que qualquer comprometimento em um nó produza apenas um fragmento de dado insignificante. Uma vantagem específica dessa técnica é que ela requer que um agente ameaçador comprometa todos os nós, obtenha todos os fragmentos e conheça o algoritmo (ou esquema de fragmentação) para reunir os dados de forma coerente.
- Defesa de simulação cibernética – as soluções e arquiteturas de simulação cibernética podem ser elementos importantes no esforço de mitigar os adversários mais avançados. As soluções de simulação podem usar iscas e armadilhas para dar ao invasor a impressão de que ele se infiltrou no sistema, ao passo que, na realidade, ele é desviado para um ambiente altamente controlado. Para mitigar futuras ameaças, são coletadas informações sobre o invasor e o ataque é neutralizado.

Uma preocupação relacionada ao acesso não autorizado é o acesso por parte de terceiros ao conteúdo do cliente e a adequação das medidas de controle de acesso para impedir o acesso não autorizado pelo corpo de funcionários do CSP. O acesso por parte de terceiros aos sistemas da AWS é concedido com base no princípio de privilégio mínimo, aprovado por uma pessoa autorizada antes de ser provisionado e supervisionado por um funcionário da AWS. Os deveres e as áreas de responsabilidade (por exemplo, a solicitação e aprovação do acesso, a solicitação e aprovação do gerenciamento de alterações etc.) devem ser distribuídos entre pessoas distintas para reduzir as chances de uma modificação não autorizada ou não intencional, ou de uso indevido dos sistemas da AWS. Os funcionários da AWS que precisam acessar o plano de gerenciamento são obrigados a usar primeiro a autenticação multifator, que é distinta de suas credenciais corporativas da Amazon, para obter acesso a determinados hosts administrativos. Esses hosts administrativos são sistemas especificamente concebidos, criados, configurados e reforçados para proteger o plano de gerenciamento. Todo esse acesso é registrado e auditado. Quando um funcionário não tem mais a necessidade comercial de acessar o plano de gerenciamento, os privilégios e o acesso a esses hosts e sistemas relevantes são revogados. A AWS implementou uma política de bloqueio de sessão que é aplicada sistematicamente. O bloqueio de sessão é mantido até que os procedimentos de identificação e autenticação sejam realizados.

A AWS também monitora o gerenciamento remoto não autorizado e rapidamente desconecta ou desativa qualquer acesso remoto não autorizado que seja detectado. Todas as tentativas de acesso administrativo remoto são registradas em logs e esses logs são analisados, não apenas por pessoas em busca de atividades suspeitas, mas também pelos sistemas automatizados de machine learning criados pela equipe de segurança da AWS para detectar padrões de acesso incomuns que possam indicar tentativas não autorizadas de acessar os dados. Se alguma atividade suspeita é detectada, os procedimentos de resposta a incidentes são iniciados. Além disso, a AWS estabeleceu políticas e procedimentos formais para

10 Existe uma série de pesquisas sobre técnicas de decomposição de dados. Um dos relatórios analisados neste documento chama-se Proteção de dados por meio da fragmentação em vários sistemas de armazenamento distribuídos diferentes - uma pesquisa, Kapusta e Memmi, 20 de junho de 2017.

delinear padrões de acesso lógico aos hosts e à infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. A menos que seja proibido por lei, a AWS exige que funcionários passem por uma verificação detalhada de antecedentes, proporcional ao seu cargo e nível de acesso a dados.

Por fim, os clientes com instâncias virtuais são controlados somente pelo cliente, que tem acesso à raiz ou controle administrativo completo sobre aplicativos, serviços e contas. Os funcionários da AWS não podem fazer login em instâncias do cliente.

Nuvem de hiperescala: Uma abordagem transformacional da segurança

Os principais CSPs de hiperescala, como a AWS, oferecem aos clientes a oportunidade de montar uma segurança adaptável e altamente resiliente para suas cargas de trabalho. Restringir as operações de acordo com imposições internas dos países inibiria as inovações de serviços e prejudicaria a capacidade de bloquear ameaças, como aquelas que atingem a disponibilidade. Uma outra consequência prejudicial das limitações geográficas internas dos países é que os agentes ameaçadores podem conseguir maior precisão de direcionamento ao saber que os dados residem dentro de áreas específicas. Os CSPs de hiperescala têm ofertas disponíveis e arquiteturas de suporte para oferecer recursos de defesa em profundidade[11] e defesa em amplitude.[12] Isso ocorre porque os mecanismos de segurança são intrínsecos ao projeto e à operação das ofertas do CSP de hiperescala.

> Um efeito não intencional da imposição de residência dos dados em um país é que os agentes ameaçadores podem obter maior precisão ao alvejar sistemas sabendo que os dados residem em locais específicos.

Os seis itens a seguir refletem os principais atributos de segurança que integram um CSP de hiperescala como a AWS:

1. A integração profunda entre segurança e conformidade (raramente alcançada nos sistemas tradicionais) significa que a segurança se beneficia diretamente da conformidade, pois os controles de segurança são continuamente monitorados e atualizados.
2. As economias de escala aplicam-se não apenas à tecnologia, mas também ao corpo de funcionários e processos de segurança, resultando em um retorno de investimento sem precedentes em comparação com os sistemas tradicionais.
3. O CSP é responsável pela maior parte da "área de superfície" de segurança, executando com a objetividade e qualidade profissional capaz de superar quase qualquer cliente. Como resultado, os clientes podem direcionar a atenção de seus profissionais e recursos de segurança para uma seção muito menor do desafio, como a segurança de aplicativos.
4. A nuvem oferece grandes benefícios de segurança, como visibilidade, homogeneidade e automação nunca vistas no sistemas tradicionais. Isso inclui recursos de registro em log e auditoria significativamente profundos que podem, por exemplo, gravar chamadas de API que registram as ações realizadas por um CSP que podem afetar a conta do cliente.

---

11 Defesa em profundidade é a prática de implementação de várias camadas de controles de segurança para oferecer autonomia e redundância. Se uma camada de controles falha, a camada subsequente está disponível para mitigar incursões adicionais contra um ativo.

12 Defesa em amplitude é uma abordagem que usa atividades multidisciplinares para fornecer diversos mecanismos de proteção em cada camada de defesa identificada. Em geral, isso significa mais automação e maior variação de controles de segurança em cada camada.

5. Os CSPs operam como um tipo de “contêiner do sistema” que fornece um conhecimento muito maior sobre o comportamento e o funcionamento do sistema, incluindo as operações de segurança, oferecendo aos clientes uma nova camada de “defesa em profundidade”.

6. Com acesso fácil e barato a quantidades massivas de capacidade de armazenamento e processamento, os clientes da AWS "usam a nuvem para proteger a nuvem", ou seja, eles executam análises de big data em dados de segurança e dados de log, o que fornece mais conhecimento sobre sua postura de segurança e permite remediar os problemas rapidamente.

Com a velocidade da inovação e a escala aumentada, a segurança em nuvem tende a melhorar. Por exemplo, somente no último ano, a AWS adicionou potentes recursos de segurança, como o Amazon GuardDuty[13], uma oferta de detecção gerenciada de ameaças que monitora continuamente comportamentos maliciosos ou não autorizados; o Amazon Macie[14], uma oferta que usa machine learning para proteger dados confidenciais, e o AWS CloudHSM 2.0[15], uma oferta totalmente gerenciada que usa um hardware validado pelo FIPS 140-2 nível 3[16] implantado automaticamente em um cluster de várias zonas de disponibilidade com alta disponibilidade e redundante, permitindo aos clientes gerar, gerenciar e usar com facilidade suas próprias chaves de criptografia na Nuvem AWS, sem oferecer à AWS qualquer acesso às chaves mestras ou às principais operações de criptografia.

A criptografia deve ser considerada um serviço essencial, pois pode agir como um meio para proteger dados, caso outros recursos falhem. Ela adiciona mais uma camada de segurança e garante a confidencialidade e a integridade dos dados em trânsito e em repouso. A combinação do AWS Key Management Service (KMS) e do AWS CloudHSM é a peça central de uma rigorosa solução de criptografia.[17] CSPs de hiperescala, como a AWS, oferecem criptografia onipresente, o que pode estar fora de alcance para operações no local. Por exemplo, o AWS Key Management Service (KMS), com validação FIPS 140-2 nível 2, oferece a opção Traga suas próprias chaves (BYOK), permitindo que os clientes usem seus próprios materiais de chaves gerados e armazenados localmente com os serviços da AWS. Os clientes podem atender a requisitos de segurança e conformidade específicos em relação a cargas de trabalho altamente confidenciais com esse recurso, já que podem reter e gerenciar o material de chaves fora da AWS.

13 https://aws.amazon.com/pt/guardduty/

14 https://aws.amazon.com/pt/macie/

15 https://aws.amazon.com/pt/cloudhsm/

16 O FIPS 140-2, Requisitos de segurança para módulos de criptografia, abrange 11 áreas relacionadas ao modelo e à implementação de um módulo de criptografia.

17 https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf

Responsabilidade do CSP: Segurança nativa na nuvem

A infraestrutura da AWS é personalizada para a nuvem, com todos os elementos projetados para uma boa intercomunicação e para apresentar a menor superfície de ataque possível. Além disso, os controles físicos de segurança presentes em nossos datacenters foram projetados para serem alguns dos mais rigorosos do mundo. A arquitetura da AWS foi avaliada e validada em relação a dezenas de estruturas de conformidade internacional.[18] Usamos avaliadores e auditores externos e independentes para avaliar e atestar nossa adesão a esses regimes, e concedemos acesso aos clientes aos relatórios de resultados e às evidências de apoio. Para atender a uma variedade tão ampla de requisitos de segurança, a AWS cria seus datacenters e arquitetura para escalar e avançar com o ritmo da inovação. Essa abordagem fez com que a AWS ganhasse a confiança de governos, organizações militares, bancos globais, instituições de saúde e outras organizações de alta confidencialidade.

Na AWS, nosso ambiente exclusivo foi um incentivo para a construção de muitas de nossas próprias ferramentas de segurança. Essas ferramentas automatizam uma ampla gama de tarefas de rotina, permitindo que nossos especialistas em segurança se concentrem em aspectos críticos da proteção ao ambiente. Nossas ferramentas resultam em requisitos de segurança que são integrados e aos quais aderimos por todo o ciclo de vida do desenvolvimento do sistema. Preocupações comuns com a segurança são remediadas nas fases iniciais do desenvolvimento do sistema, permitindo que nossos especialistas em segurança se concentrem na atenuação de ameaças avançadas e complexas no nível da produção.

Nossas equipes de segurança monitoram a infraestrutura todos os dias, durante o dia inteiro e estão bem conectadas a todos os principais fornecedores e grupos de defensores da segurança para identificar possíveis ameaças imediatamente. Isso é feito em escala massiva, o que é algo que diferencia a organização de segurança da AWS. Ao usar algoritmos complexos para verificar milhões de contas ativas de clientes executando praticamente todos os tipos possíveis de carga de trabalho, podemos ver os problemas que podem ocorrer somente uma vez em um bilhão de operações várias vezes ao dia. Quando remediamos o problema, isso é feito para a plataforma inteira. Esse tipo de visibilidade e resposta simplesmente não é alcançável para a grande maioria das organizações que executam datacenters no local. O valor que vem da perícia focada e da escala massiva explica por que a Gartner e a IDC determinaram que cargas de trabalho de infraestrutura como um serviço (IaaS) em nuvens públicas sofrerão menos incidentes de segurança do que aquelas em datacenters tradicionais. A pesquisa da Gartner estima uma redução de pelo menos 60% nos incidentes de segurança.[19]

Responsabilidade do cliente: Abordagem de arquitetura segura

As capacidades de segurança que são nativas dos servidores em nuvem em hiperescala, como a AWS, permitem que os clientes criem arquiteturas exclusivas para atenuar os riscos de acesso. Instalações locais e similares não têm a homogeneidade, economias de escala, visibilidade e automação que podem trazer grandes avanços na segurança. Esses avanços são necessários para construir sistemas altamente seguros que possam combater as ameaças em desenvolvimento vistas externa e internamente. As instalações no local lutam para empregar esses novos conceitos operacionais devido aos requisitos de recursos para refatoração de rede e aquisição de novos sistemas, bem como para o trabalho humano necessário devido à falta de infraestrutura definida de software. Os CSPs de hiperescala criam um nível de agilidade e adaptabilidade em em sua infraestrutura para implementar organicamente esses avanços na segurança. Isso significa que os clientes podem usar os novos

18 Consulte https://aws.amazon.com/pt/compliance

19 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

avanços mais rapidamente, já que eles estão integrados de forma nativa às ofertas de CSP, permitindo que os clientes criem sistemas usando arquiteturas exclusivas, como microssegmentação, modelos polimórficos[20] e redes multiníveis de fraude.

Por exemplo, analisando mais detalhadamente o modelo baseado em microssegmentação na AWS, um cliente pode usar uma ampla gama de tecnologia, incluindo Amazon Virtual Private Cloud (Amazon VPC), AWS Identity and Access Management (IAM), grupos de segurança, listas de controle de acesso à rede, vários serviços de criptografia e registro em log, além do AWS Certificate Manager para formar a base da construção de uma rede do Modelo de Confiança Zero[21] (ZTM). A princípio, o ZTM pode oferecer uma vantagem distinta para a atenuação de ameaças e o monitoramento do desempenho. As organizações têm uma necessidade evidente de implementar um ZTM ou um modelo de segmentação de segurança semelhante para combater as ameaças atuais, mas é extremamente difícil e caro construir esse tipo de arquitetura em ambientes corporativos tradicionais. Mudar para um provedor em nuvem pública oferece às organizações a oportunidade de implementar o ZTM e conceitos similares sem a carga significativa de gastos e recursos associada à atualização/criação da rede física.

Funções para proteção de dados

Existem cinco conceitos importantes relacionados à propriedade e gerenciamento de dados no modelo de responsabilidade compartilhada:

1. Os clientes continuam a ser donos dos seus dados.
2. Os clientes escolhem as localizações geográficas em que desejam armazenar seus dados; elas só são alteradas por decisão do cliente.
3. Os clientes podem fazer o download ou excluir seus dados sempre que quiserem.
4. Os clientes podem excluir seus dados de maneira "criptografada" excluindo as chaves de criptografia mestras necessárias para descriptografar as chaves de dados, que são, por sua vez, necessárias para descriptografar os dados.
5. Os clientes devem considerar a confidencialidade dos seus dados e decidir se e como criptografar os dados enquanto estiverem em trânsito e em repouso.

As medidas de proteção de dados são mais eficientes se aplicadas após definir as funções do gerenciamento de dados para determinar as funções e as responsabilidades apropriadas da parte interessada. A maioria dos esquemas de proteção de dados diferencia entre as obrigações do controlador de dados (também chamado de "usuário") e as do processador de dados com base naquelas funções distintas. Por exemplo, sob a Regulação geral da proteção de dados da União Europeia, o controlador de dados é responsável por implementar medidas técnicas e organizacionais apropriadas para proteger os dados pessoais contra destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizados. Quando o processamento é realizado por um processador de dados em nome do controlador de dados, o controlador de dados também é responsável por escolher um processador que ofereça medidas técnicas e organizacionais suficientes para

---

20 Em termos simples, o modelo polimórfico permite a criação de alvos móveis, dificultando para os adversários a execução de ataques bem-sucedidos.

21 O conceito foi originalmente cunhado pela Forrester Research. Ele propõe que nenhuma entidade na rede é confiável. O objetivo é impor o acesso seguro a todos os recursos, sejam internos ou externos. Isso significa que uma organização deve entender e classificar seus dados, e mapear como esses dados, principalmente os dados confidenciais, fluem entre armazenamento, processamento, trânsito e consumidores. Assim, quando os dados forem entendidos, uma organização poderá implementar os mecanismos de ZTM que impõem e automatizam o privilégio mínimo absoluto, a criptografia de ponta a ponta e a inspeção completa do tráfego.

reger o processamento a ser realizado. Essas distinções ajudam a delinear responsabilidades entre provedores terceirizados e seus clientes.

Como um provedor de infraestrutura de autoatendimento totalmente sob o controle dos clientes, inclusive a respeito de como e se os dados são processados, a AWS oferece os serviços de infraestrutura para clientes que desejam fazer upload e processar conteúdo na AWS. A AWS não tem visibilidade sobre ou conhecimento de quais clientes estão fazendo upload na rede, inclusive se o conteúdo inclui ou não dados pessoais. Os clientes da AWS também são encorajados a usar a criptografia a fim de deixar o conteúdo ininteligível para a AWS e qualquer terceiro buscando acesso aos dados.

Os serviços da AWS independem de conteúdo, pois oferecem o mesmo alto nível de segurança para todos os clientes, independentemente do tipo ou da região geográfica do conteúdo processado ou armazenado. Em outras palavras, a AWS adota o mesmo alto nível de segurança em todas as nossas ofertas. Isso significa que adotamos o mais alto nível de classificação de dados percorridos e armazenados em nossa nuvem comercial e aplicamos esses mesmos níveis de proteção a todas as nossas ofertas e para todos os nossos clientes. Essas ofertas são então colocadas em fila para certificação em relação ao alto nível de segurança e conformidade, o que se traduz em benefícios para os clientes pelos níveis elevados de proteção dos seus dados processados e armazenados na nuvem. A Nuvem da AWS foi certificada em várias indústrias regulamentadas (saúde, financeira, etc.), e obteve credenciamento nacional (FedRAMP dos Estados Unidos, C5 da Alemanha, IRAP da Austrália, e credenciamentos globais, como ISO 27001,[22] ISO 27018,[23] Payment Card Industry Data Security Standard (PCI DSS) (Padrão de segurança de dados da indústria de cartões de pagamento),[24] e Service Organization Controls (SOC) (Controles de organização de serviço)[25], que testam e validam a segurança de nossos sistemas com relação aos padrões mais rigorosos.

Fluxo livre de dados não pessoais proposto como as regiões de fato da UE e do transpacífico

A Comissão Europeia publicou recentemente um projeto de regulamento sobre o livre fluxo de dados ***proibindo regras nacionais de localização de dados em Estados-membros da UE*** e reconhecendo o princípio da livre movimentação de dados não pessoais dentro da UE. Essa proposta estabelece o fluxo de dados transnacional como o padrão de facto, colocando o ônus sobre os Estados-membros para fornecer justificativa de segurança pública para a imposição de requisitos de localização de dados. Embora esteja nos estágios iniciais da deliberação, essa proposta reconhece as vantagens econômicas e de segurança dos fluxos de dados transnacionais, que superam as considerações para impor as políticas de residência de dados. Além disso, no início de 2018, o **Acordo de Parceria Transnacional Abrangente e Progressivo**, estabelecido entre 11 países, também apoia ***fluxos de dados transnacionais*** e não exige que as empresas estabeleçam instalações de computação no país como condição para realizar negócios naquele país.

22 A ISO 27001/27002 é um padrão de segurança global amplamente adotado que estabelece os requisitos e as práticas recomendadas para uma abordagem sistemática de gerenciamento de informações da empresa e do cliente, com base em avaliações periódicas de riscos apropriadas e cenários de ameaça em constante mudança.

23 ISO 27018 é um código de práticas concentrado na proteção de dados pessoais na nuvem. Ela baseia-se no padrão de segurança da informação ISO 27002 e disponibiliza diretrizes sobre a implementação dos controles desse padrão aplicáveis às Informações Pessoalmente Identificáveis (PII) da nuvem pública. E também fornece um conjunto de diretrizes associadas e controles adicionais destinados a abordar os requisitos de proteção de PII da nuvem pública, que não foram contemplados no conjunto de controles da ISO 27002 atual.

24 A Payment Card Industry Data Security Standard (também conhecida como PCI DSS) é uma norma de segurança de informações proprietárias administrada pelo PCI Security Standards Council (https://www.pcisecuritystandards.org/), que foi fundado pelas empresas American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. A PCI DSS é aplicável a todas as entidades que armazenam, processam ou transmitem dados de portadores de cartões (CHD) e/ou dados de autenticação confidenciais (SAD), incluindo comerciantes, processadores, compradores, emissores e provedores de serviços.

25 Os relatórios de controle de empresas de serviços (SOC 1, 2, 3) destinam-se a atender a uma ampla variedade de requisitos de auditoria financeira dos Estados Unidos e de órgãos internacionais de auditoria. A auditoria para esse relatório é realizada de acordo com as Normas internacionais para contratos de garantia nº 3402 (ISAE 3402) e o AICPA (American Institute of Certified Public Accountants): AT 801 (antigo SSAE 16).

Como alinhar política de segurança, transformação digital e crescimento econômico

As políticas precisam evoluir para atender às constantes mudanças tecnológicas e ao mundo que elas ajudam a criar. Caso contrário, os governos continuarão defasados em atualizar suas operações, servir seus cidadãos e adotar soluções mais modernas e seguras. Esta seção descreve como a AWS aborda os objetivos de segurança que estão por trás das imposições de residência de dados a fim de diminuir as preocupações dos criadores de políticas. Ela também explora os desafios econômicos e de modernização de TI associados às considerações sobre políticas e residência de dados, visando avançar a adoção segura da nuvem no setor público.

Desafios do setor público e comercial com a residência de dados

Os governos devem analisar o quanto suas políticas nacionais promovem ou impedem as oportunidades de crescimento econômico e desenvolvimento da força de trabalho que são impulsionadas pelos serviços em nuvem de hiperescala. A implementação de imposições de residência de dados pode ter impactos negativos significativos, como:

- **Efeitos adversos nos esforços de expansão comercial multinacional de empresas locais** – quando uma empresa cresce e se expande para além de suas operações regionais, é vital que ela tenha acesso a recursos de alcance global. A restrição do acesso a serviços de CSPs de hiperescala limita seriamente o nível de experiência de usuário que uma empresa pode fornecer à sua base de clientes globais.
- **Opções de redundância geográfica limitadas em relação às regiões globais do CSP** – para governos e empresas, garantir a redundância em caso de falhas operacionais devido a um desastre ou outras circunstâncias é vital para sua estabilidade. Manter as operações aglomeradas em apenas um país expõe a organização a um nível de risco que pode superar em muito as preocupações com o acesso aos dados.
- **Estruturas caras necessárias para acomodar requisitos rigorosos** – ambientes de "nuvem" de locador único ou criadas por comunidades exigem um nível de custo para a sustentação operacional que pode, na realidade, impedir a aquisição dos recursos adicionais necessários para alcançar uma defesa em profundidade.

A tecnologia de nuvem é o fator que torna possível o avanço nos setores comercial e público, e na medida em que os governos podem promover ou se opor ao princípio dos fluxos de dados entre fronteiras, isso terá um impacto na força de suas economias locais, bem como em sua competitividade no mercado global.

Impacto comercial

A promoção do fluxo de dados livre entre fronteiras tem um impacto líquido positivo significativo na economia global. Estudos recentes feitos por várias organizações de pesquisa enfatizam esse impacto e vão ainda mais longe, destacando o custo de criação de barreiras para os fluxos de dados. Um relatório do McKinsey Global Institute, de fevereiro de 2016, estimou que os fluxos de dados entre fronteiras contribuíram com aproximadamente US$ 2,8 trilhões para a economia global em 2014[26] pela facilitação do fluxo de produtos, serviços e outros recursos. Os relatórios estimam que este número

26 http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

pode alcançar US$ 11 trilhões até 2025. Os governos que impõem que os dados estejam residentes no local e limitam os fluxos econômicos entre fronteiras pagam um alto preço. O Centro Europeu de Economia Política Internacional (ECIPE), um instituto de pesquisa de políticas independente, publicou um estudo sobre o impacto econômico da imposição de residência de dados que discrimina fornecedores estrangeiros em sete jurisdições: Brasil, China, Coreia do Sul, Índia, Indonésia, União Europeia e Vietnã.[27] A pesquisa concluiu que a imposição de restrições unilaterais aos fluxos de dados entre fronteiras e ao acesso a mercados estrangeiros tem um impacto negativo no crescimento e na recuperação econômica, pois limita o acesso a preços competitivos, aumento de empregos em vários setores de serviços e mercadorias e oportunidades de investimento. O estudo observou que a imposição de residência de dados tem um impacto não apenas no fluxo de dados, mas também em um conjunto mais amplo de oportunidades de expansão comercial que dependem de fluxos de dados entre as fronteiras.

Um estudo semelhante feito pelo Banco Mundial pesquisou seis países em desenvolvimento e os 28 Estados-membros da União Europeia, e concluiu que as imposições de residência de dados podem reduzir o PIB em até 1,7%, os investimentos em até 4,2% e as exportações em 1,7%.[28] Este impacto é sentido com mais intensidade pelas empresas menores e as startups. Por meio da nuvem, por exemplo, indivíduos e pequenas e médias empresas (PMEs) podem acessar recursos de TI por um custo e escala antes ao alcance apenas de entidades com um nível de capitalização muito superior. As PMEs são os principais motores da criação de novos empregos. A computação em nuvem diminui as barreiras à criação de negócios e ao acesso ao mercado, possibilitando a criação de mais startups e, consequentemente, mais empregos. Entretanto, de acordo com a Comissão Europeia, empresas de tecnologia como os CSPs podem se deparar com custos significativos para se adaptar às variadas leis nacionais, o que faz com que os custos da venda online excedam os benefícios. Mais recentemente, em maio de 2017, a Fundação de Tecnologia da Informação e Inovação, um instituto de pesquisa neutro, chegou independentemente a constatações semelhantes.[29]

27 Centro Europeu para Economia Política Internacional (ECIPE): "The Costs of Data Localization: A Friendly Fire on Economic Recovery", http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.8208626.1580578791.1473954628.

28 http://documents.worldbank.org/curated/en/961621467994698644/pdf/102724-WDR-WDR2016Overview-ENGLISH-WebResBox-394840B-OUO-9.pdf

29 Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Fundação de Tecnologia da Informação e Inovação (maio de 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243762501.1722557619.1508762047-1611916082.1508762047.

Uma conclusão importante e constante nesses estudos é que proibir o fluxo de dados entre fronteiras, com a imposição de residência de dados, pode afetar o crescimento econômico local e regional e a competitividade no mercado global, e nesse caso o maior impacto incidirá sobre as PMEs. Um sistema seguro na UE não é nem mais nem menos seguro do que um sistema de arquitetura semelhante na América Latina. Os governos não conseguem compreender que a proteção de dados nem sempre depende do lugar em que as informações estão armazenadas, mas das medidas que são usadas para protegê-los. A localização física geralmente não tem relevância, pois os datacenters estão quase sempre conectados a redes amplamente acessíveis e, por isso, a proteção real depende dos métodos e processos técnicos, operacionais e gerenciais implementados pelos CSPs e pelos clientes.[30]

Custos para operar exclusivamente em datacenters dentro do país

Um estudo de 2015, realizado por uma empresa de segurança da informação, avaliou que o modelo de datacenter em âmbito nacional é bem mais caro em comparação com o aproveitamento dos CSPs globais. Esse estudo constatou que o custo dos serviços em nuvem pode aumentar substancialmente devido à localização física dos dados, dependendo da disponibilidade de serviços alternativos. Esse estudo constatou que:

- Se o Brasil tivesse decretado a localização dos dados como parte de sua "Declaração de Direitos da Internet" em 2014, as empresas teriam de pagar em média 54% a mais para usar serviços em nuvem (de todas as categorias) de provedores de nuvem locais em comparação com o menor preço em nível mundial.
- Se a União Europeia decretasse a localização dos dados, as empresas ainda assim teriam de pagar até 36% a mais para usar serviços semelhantes fornecidos por CSPs de hiperescala. Na ocasião em que esse estudo foi realizado, alguns dos datacenters de mais baixo custo estavam localizados na União Europeia.[31]

Impacto sobre o setor público

Os países que impõem barreiras ao fluxo de dados podem impedir que os cidadãos beneficiem-se de serviços inovadores que melhoram a qualidade de vida e o fornecimento de serviços governamentais. Por exemplo, os aplicativos de inteligência artificial e machine learning (IA/ML) requerem uma infraestrutura personalizada para um funcionamento ideal.[32] E, embora os CSPs globais continuem ampliando o espaço de seus datacenters, não faz sentido presumir que os datacenters se estabelecerão em todos os países. Por isso, como cada vez mais se tem usado a IA/ML para melhorar os serviços, como os prognósticos de saúde e as previsões climáticas para prontidão emergencial, os cidadãos dos países com exigências rigorosas de residência de dados ficarão defasados em relação ao acesso a avanços tecnológicos nos serviços que lhes são direcionados.

30 Ibid p. 4. Conclusões semelhantes são extraídas independentemente neste documento.

31 http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.51021357.566718019.1510350061-1611916082.1508762047

32 Por exemplo, sistemas com capacidade de GPU de propósito geral e matrizes de portas programáveis em campo (FPGA).

Existem também custos socioeconômicos em cascata na restrição ao fluxo de dados, especificamente para a competitividade comercial e o desenvolvimento da força de trabalho. À medida que a tecnologia de nuvem tornar-se onipresente e mais fortemente vinculada ao avanço econômico, o comércio digital (e a diminuição das barreiras contra ele) terá maior prioridade junto aos governos. Os países que permitem o livre fluxo de dados estarão em vantagem com relação ao acesso à tecnologia de ponta, o que, por sua vez, terá um impacto sobre a modernização dos serviços comerciais e do setor público, melhorará a produtividade dos trabalhadores e acelerará o crescimento do emprego local e das habilidades em todos os setores. Os países que restringem o fluxo de dados e o comércio digital perceberão, com o passar do tempo, uma desvantagem competitiva. Por exemplo, os inúmeros benefícios associados com a IoT, que possibilitam o desenvolvimento da agricultura, da fabricação ou de cidades "inteligentes", não podem ser realizados com políticas restritivas que impõem obstáculos às análises de big data, à machine learning ou a outros recursos oferecidos pelo movimento de dados livre e ao mesmo tempo seguro.

A demanda por habilidades de computação em nuvem em áreas importantes como segurança de aplicativos, desenvolvimento de aplicativos empresariais na nuvem, migração de nuvem empresarial e big data tem sido alta e frequente. O Departamento de Estatísticas do Trabalho dos Estados Unidos relata que a demanda prevista de empregos em segurança da informação deve crescer 37% entre o período de 2012-2022. Para atender à nova demanda de emprego, os governos terão de investir para fornecer aos indivíduos oportunidades educacionais e de capacitação para aquisição de habilidades tecnológicas.

Os obstáculos ao acesso aos sofisticados serviços de TI fornecidos pelos CSPs de hiperescala também provocarão uma defasagem permanente no desenvolvimento e na manutenção de uma força de trabalho altamente qualificada e tecnicamente experiente. Isso porque a aptidão da força de trabalho está correlacionada com a sofisticação tecnológica da organização, o que, por sua vez, baseia-se na capacidade da organização de acessar tecnologias de ponta. O uso eficaz da tecnologia moderna requer uma força de trabalho com habilidades para usar essa tecnologia. Em vista da amplitude e do ritmo da inovação nos serviços em nuvem, existe uma defasagem reconhecida e cada vez mais ampla nessas habilidades. Os governos, em particular, estão defasados na corrida por especialistas que são essenciais para a modernização de aplicativos e, ao mesmo tempo, para a proteção de informações e sistemas do setor público contra adversários altamente sofisticados e violações que aumentam em frequência e impacto.

Considerações sobre como estabelecer políticas de residência de dados

Como analisado acima, é possível aproveitar os benefícios de custo e segurança de CSPs de hiperescala como a AWS e, ao mesmo tempo, manter a soberania regulamentar do Estado-nação sobre os dados. As medidas de segurança implantadas em todos os serviços da AWS, e verificadas por meio de auditorias de terceiros, oferecem um alto nível de garantia no sentido de impedir e combater eventos de risco de acesso ilícito a dados.

Incentivamos os governos a considerar as políticas a seguir para concretizar os objetivos de segurança associados com a residência de dados.

1. Desenvolver políticas e requisitos que permitam o uso de instalações de processamento de dados fora do país, desde que os dados sejam processados e armazenados em um ambiente de nuvem de hiperescala moderno e altamente seguro. Os clientes também podem escolher locais com leis de proteção de dados que sejam consistentes com suas próprias leis e onde os acordos de transferência de dados já estejam presentes.

2. Alinhar as políticas nacionais e os requisitos regulatórios com o princípio de livre movimentação de dados entre fronteiras para equilibrar eficazmente as metas de segurança, econômicas e de modernização de TI.

3. Avaliar modelos de transferência de dados, como a Privacy Shield entre UE e EUA, e cláusulas contratuais padronizadas, como as Cláusulas Modelo da UE, que foram aprovadas pelas autoridades de proteção de dados da UE e podem ser usadas em acordos entre os provedores de serviços e seus clientes a fim de garantir que os dados pessoais que saem da Área Econômica Europeia sejam transferidos em conformidade com a Regulamentação Geral de Proteção de Dados (GDPR).[33] Esses tipos de acordos de transferência de dados fornecem garantias de que os CSPs protegem os dados pessoais de maneira responsável, além de oferecer um meio pré-aprovado para proteger e dar suporte ao fluxo de dados internacional de forma segura e compatível.

A Regulamentação Geral de Proteção de Dados da UE, em vigor desde maio de 2018, destina-se a conciliar as leis de proteção de dados por toda a União Europeia (UE), aplicando uma única lei de proteção de dados que é obrigatória para todos os estados-membros. A GDPR não impõe leis de residência de dados dentro da UE, mas apoia estruturas legais na forma de modelos de transferência de dados e cláusulas contratuais padronizadas (isto é, Cláusulas Modelo da UE) para encorajar o fluxo de dados entre as regiões.

O artigo 45 da GDPR estabelece o princípio de que as transferências de dados pessoais para um terceiro país, ou organização internacional, podem ocorrer se o terceiro país, território ou os setores especificados dentro deste país, ou organização internacional em questão, garantir um nível de proteção adequado. Para alcançar esse objetivo, os governos podem:

- Alterar sua lei atual de proteção de dados e iniciar discussões sobre adequação com outros países. Por exemplo, a Nova Zelândia está a caminho de alcançar uma decisão sobre a adequação pela Comissão Europeia.
- Estabelecer estruturas bilaterais como a Privacy Shield entre UE e EUA.

4. Garantir que os CSPs e os contratados de terceiros demonstrem controles de segurança robustos com relação ao acesso não autorizado de terceiros aos dados, sistemas e ativos por meio de credenciamentos reconhecidos internacionalmente (por exemplo, ISO 27001, ISO 27018, SOC, PCI DSS etc.).

5. Classificar os dados e definir as funções e responsabilidades de tratamento de dados a fim de determinar as obrigações com relação à proteção de dados apropriadas para cada parte. Os governos devem considerar o uso do ISO 27018 como base para definir as funções de controlador e processador de dados. Os governos podem trabalhar com CSPs para compreender e aplicar de forma adequada as responsabilidades de proteção de dados do controlador em oposição às do processador, para cada um dos modelos de serviço na nuvem.

6. Garantir que o cliente compreenda e implemente os serviços de segurança na criptografia de dados. A AWS foi precursora dos serviços de criptografia que fornecem aos clientes a capacidade de controlar totalmente suas chaves de criptografia. A AWS fornece aos clientes a opção de criptografar dados usando chaves próprias, que podem ser armazenadas fora da AWS ou com segurança dentro das opções de armazenamento. Isso permite que eles controlem as chaves e o acesso aos dados e atendam a rígidas obrigações de compatibilidade e segurança.

33 O Adendo de Processamento de Dados da GDPR para a AWS, que inclui as Cláusulas Modelo da UE, agora faz parte dos nossos Termos de serviços online. Isso significa que todos os clientes globais da AWS podem aplicar os termos do AWS GDPR DPA sempre que utilizarem os serviços da AWS para processar dados pessoais sob a GDPR. Mais informações sobre a abordagem da AWS sobre a conformidade com a GDPR estão disponíveis aqui: https://aws.amazon.com/pt/compliance/gdpr-center/.

7. Envolver-se em iniciativas bilaterais e multilaterais de atualização do processo MLAT para equilibrar as exigências governamentais em obter rapidamente as evidências necessárias em investigações e acusações com os direitos individuais à privacidade em relação ao conteúdo eletrônico de sua propriedade. Apoiamos uma legislação que atualize os termos de privacidade e o acesso das autoridades legais às comunicações eletrônicas – tanto em âmbito nacional quanto internacional. Incentivamos os governos a analisar e atualizar suas leis nacionais visando abordar as funções, as responsabilidades e os mecanismos que controlam o acesso legítimo aos dados de forma consistente com os princípios do processo MLAT.

Conclusão

Embora os governos possam ter uma percepção de maior segurança quando impõem exigências de residência para dados processados e armazenados em instalações de TI locais porque elas oferecem proximidade e controle físicos, uma avaliação mais profunda demonstra que restringir os serviços de TI à jurisdição local não oferece melhor segurança de modo geral aos dados. Do ponto de vista da relação risco-benefício, os CSPs de hiperescala, como a AWS, podem ajudar a gerenciar melhor os riscos de segurança cibernética e ainda minimizar os riscos do acesso aos dados por um governo estrangeiro. Os governos também precisam levar em consideração os compromissos significativos associados às imposições de residência de dados. Os governos que aplicarem imposições restritivas de residência de dados não só perderão o acesso a alguns dos ambientes de computação mais seguros do mundo, mas para além da segurança, serão forçados a lidar com uma defasagem perpétua no acesso à tecnologia de ponta de baixo custo, que é necessária para sua própria transformação digital. Encorajamos os governos a reavaliarem os objetivos de segurança realmente alcançados por meio de restrições na localização dos dados em comparação com as perdas significativas de economia, modernização de TI e oportunidades de segurança. Os recursos de segurança dos CSPs de hiperescala abordam não apenas as principais preocupações, mas fornecem segurança em um nível superior às instalações tradicionais locais ou contratadas localmente. As soluções que incluem políticas, como os acordos de transferência de dados e a utilização de credenciamentos de segurança internacionais de boa reputação, podem servir como meios satisfatórios para alcançar os objetivos de residência de dados e, ao mesmo tempo, promover as metas de transformação digital do setor público.