Entendendo o modelo de responsabilidades compartilhadas em serviços na nuvem

O mundo da tecnologia em datacenters locais era prático quando os serviços na nuvem não estavam disponíveis. Originalmente, o gerenciamento de serviços de tecnologia de ponta a ponta, seja de infraestrutura ou software, ficava a cargo da empresa que os executava em seus próprios estabelecimentos físicos ou alugados de fornecedores terceirizados. Alguns serviços eram terceirizados ou prestados por meio de de contratos gerenciados e incluíam funções como coleta de fitas de backup e armazenamento externo. Caso contrário, a maioria dos serviços e áreas de risco eram geridos internamente.

Só recentemente o modelo como serviço se tornou mais presente. O advento de serviços fora das premissas acelerou significativamente, e esse rápido aumento criou uma falsa suposição de que responsabilidade, responsabilização e risco ainda não são um modelo de responsabilidades compartilhadas. Este é o centro do problema: As organizações ficam em situações difíceis sem entender adequadamente seus acordos e responsabilidades quando os serviços são selecionados e entregues aos provedores de serviços na nuvem (CSPs).

Benefícios significativos dos processos na nuvem

Todas as organizações, sejam pequenas, médias ou grandes, estão se transformando rapidamente adaptando-se aos processos na nuvem. O termo "nuvem" é amplo, mas pode ser definido como o portfólio de serviços de TI que são entregues sob demanda ou como um serviço. A transformação para processos na nuvem que foi originalmente prevista para os próximos cinco anos foi acelerada para apenas três anos. transição para processos na nuvem beneficia uma organização de várias maneiras, incluindo escalabilidade mais fácil, maior resiliência, continuidade e economia de custos. Várias organizações evoluíram rapidamente sua infraestrutura digital usando soluções baseadas na nuvem e adotando estratégias que priorizam a nuvem. Isso resultou no aumento da conectividade simples e segura de qualquer lugar por meio de arquiteturas multinuvem híbridas e maior agilidade para atender às necessidades de negócios em rápida evolução. Como resultado, as operações na nuvem atingiram um nível inesperado de maturidade e utilidade.

JAI SISODIA | CISA, CCP, ITIL V3

É o gerente global de saúde digital, TI, auditoria cibernética e de privacidade em uma organização global de dispositivos médicos e assistência médica. Ele é responsável por liderar e executar auditorias globais e atividades de consultoria em várias áreas, incluindo plataformas na nuvem, fábricas e sistemas de controle industrial, sistemas de planejamento de recursos empresariais, avaliações de privacidade, risco de terceiros, cibersegurança de dispositivos médicos e integração de auditoria financeira. Sisodia já trabalhou como consultor de assurance e consultoria para uma das principais empresas de consultoria Big Four.

MOHAMMED KHAN | CISA, CRISC, CDPSE, CIPM, SIX SIGMA CERTIFIED GREEN BELT

É o chefe global de auditoria de saúde digital, TI, cibernética e privacidade em uma organização global de dispositivos médicos e assistência médica. Ele gerencia uma equipe global responsável pelo gerenciamento de riscos corporativos em toda a organização e conduz auditorias, avaliações e compromissos de consultoria. Ele liderou auditorias e avaliações globais multinacionais em várias áreas, incluindo sistemas de planejamento de recursos empresariais, data centers globais, plataformas na nuvem, revisões de fabricação e terceirização de terceiros, reengenharia e melhoria de processos, avaliações globais de privacidade e US Food and Drug Administration (FDA) orientações específicas para a cibersegurança de dispositivos médicos. Anteriormente, trabalhou como consultor assurance para as principais empresas de consultoria e organizações multinacionais. Khan frequentemente fala em conferências nos EUA e internacionais sobre tópicos relacionados à privacidade de dados, cibersegurança e consultoria de risco. Ele é revisor de artigos do *ISACA® Journal* e contribui ativamente para o *ISACA Journal* e blogs. Ele também atua no Comitê de Saúde Digital da ISACA, recomendando liderança e orientação de pensamento líderes do setor. Ele recebeu o Prêmio Global ISACA® John W. Lainhart IV em reconhecimento de suas principais contribuições para o desenvolvimento e aprimoramento do corpo comum de conhecimento usado pela ISACA e seus membros.

Escalabilidade

As soluções na nuvem são vantajosas para lidar com mudanças dinâmicas na demanda e escala de serviços digitais que podem levar a grandes mudanças nos padrões de uso de dados. Um exemplo é uma rede de entrega de conteúdo (CDN), que é um grupo de servidores distribuídos geograficamente que aceleram a entrega de conteúdo da Web, aproximando-o de onde os usuários estão localizados.[1] Os CDNs são componentes críticos de qualquer infraestrutura de nuvem e melhoram significativamente a confiabilidade, tempos de resposta e taxas de conversão mais altas. Eles também foram altamente benéficos durante a pandemia do COVID-19, quando muitas empresas de repente tiveram que operar remotamente.

Resiliência e Continuidade

A resiliência é necessária para lidar com qualquer evento potencialmente desastroso, como desastres naturais (por exemplo, inundações, furacões, terremotos) e ataques terroristas, e a pandemia forneceu ampla evidência de que é fundamental ter resiliência nos processos de uma organização para reagir e recuperar rapidamente das perturbações do mercado.

Os serviços na nuvem oferecem controles em várias camadas da infraestrutura de rede para garantir segurança e continuidade. Essas soluções de segurança contêm protocolos que protegem transações e informações confidenciais. Além disso, os CSPs empregam equipes de segurança dedicadas cujo trabalho em tempo integral é garantir que os agentes mal-intencionados sejam expostos. Esse pessoal de segurança tem a experiência de proteger os ativos de vários clientes, o que torna a nuvem ainda mais confiável.

Custo-benefício

Os benefícios dos serviços na nuvem incluem a criação de pegadas de carbono menores, a transferência do risco de gerenciamento de recursos para os provedores de serviços, a redução dos gastos de capital e a simplificação dos processos de computação:

> *O custo inicial da nuvem também é menor do que as soluções internas. Para empresas que precisam de produtos de primeira linha, mas não têm fundos extensivos imediatamente disponíveis, as soluções na nuvem oferecem uma flexibilidade fantástica.*[2]

Modelos de implantação na nuvem

Os CSPs oferecem vários tipos de ambientes de nuvem com base nos requisitos de seus clientes, que podem ser amplamente categorizados em propriedade, nível de acesso e escala. Esses modelos de implantação

de nuvem são nuvem pública, nuvem privada, nuvem híbrida e nuvem comunitária.

Nuvem pública

O modelo de implantação de nuvem pública é um serviço de computação que é oferecido por terceiros a seus clientes através da Internet em um modelo de pagamento por uso. Isso permite que os clientes aproveitem a escalabilidade e a flexibilidade que a nuvem oferece sem arcar com os custos associados à compra, gerenciamento e manutenção da infraestrutura subjacente.

A nuvem pública, devido à sua arquitetura multitenant, tem limitações. Por exemplo, ele não fornece controle da infraestrutura subjacente, como hipervisores, equipamentos de rede ou outros serviços. Isso pode ser um fator de alto risco para algumas organizações que trabalham em setores sensíveis, como defesa, bancos ou tecnologia. Outras limitações importantes da nuvem pública incluem:

- Os CSPs públicos oferecem uma abordagem de one size fits all, que pode não funcionar para algumas organizações.
- Os serviços fornecidos no modelo de nuvem pública podem não estar em conformidade com determinados regulamentos governamentais. Isso é

> "A pandemia forneceu amplas evidências de que é fundamental ter resiliência nos processos de uma organização para reagir e se recuperar rapidamente das interrupções do mercado."

especialmente relevante para o setor financeiro.

- Uma falha de segurança na infraestrutura da nuvem pode tornar todo o ambiente e todos os seus clientes vulneráveis a um ataque.

Nuvem privada

A nuvem privada é um ambiente de computação na nuvem dedicado a uma empresa ou organização. Ele oferece todos os benefícios de uma nuvem pública com controle adicional e um nível mais alto de segurança e privacidade. Os serviços e infraestrutura em uma nuvem privada são sempre mantidos em uma rede privada. A própria nuvem pode estar localizada no data center da organização ou hospedada por um provedor de serviços terceirizado. No entanto, há outras considerações ao escolher o modelo de implantação na nuvem:

- A nuvem privada oferece recursos de computação dedicados, que custam mais do que a nuvem pública, onde o custo é distribuído entre vários locatários.
- A nuvem privada requer suporte e manutenção contínuos da infraestrutura de nuvem.

Esse tipo de nuvem é adequado para organizações que precisam de maior controle de seus dados ou operações, como agências governamentais, instituições financeiras ou organizações de saúde.

Nuvem híbrida

Uma nuvem híbrida combina a nuvem privada e a pública. Essa abordagem é selecionada por organizações maiores com necessidades críticas de negócios, como requisitos regulatórios, aplicativos herdados que não podem ser movidos para a nuvem pública, requisitos de segurança ou baixa latência. O modelo de nuvem híbrida permite que a organização se beneficie da flexibilidade da nuvem pública e da segurança da nuvem privada.

> "O modelo de responsabilidade compartilhada é uma estrutura que define as responsabilidades de segurança entre o CSP e seus clientes."

Nuvem comunitária

No modelo de computação na nuvem comunitária, a infraestrutura na nuvem é compartilhada entre diferentes organizações de uma comunidade específica, como bancos, empresas comerciais ou fabricantes de dispositivos médicos. Esse modelo fica em algum lugar entre as nuvens públicas e privadas e é adequado para organizações sujeitas a requisitos regulatórios semelhantes, trabalhando em projetos conjuntos ou compartilhando recursos comerciais.

Tipo de serviço

Os CSPs fornecem seus serviços principalmente com base em três modelos de serviço padrão: Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). Esses modelos oferecem um grau variado de abstração e, como tal, são retratados como diferentes camadas em uma pilha: infraestrutura, plataforma e serviços de aplicativos.

Infraestrutura como um serviço

IaaS, também conhecido como Hardware como Serviço (HaaS), fornece recursos de computação de propriedade do provedor de serviços para clientes sob demanda pela Internet. Provedor de serviços gerencia e mantém a infraestrutura, que oferece vários benefícios, incluindo permitir que uma organização evite os custos associados à compra e gerenciamento de infraestrutura física e ao dimensionamento de recursos para cima e para baixo com base na demanda.

Plataforma como serviço

Os provedores de PaaS oferecem recursos de computação de software e hardware, o que permite que os desenvolvedores criem, testem e executem aplicativos sem precisar manter uma infraestrutura física ou software. Ele fornece um ambiente de tempo de execução que oferece vários benefícios:

- O tempo de codificação é drasticamente reduzido porque o CSP oferece componentes de aplicativos como recursos de segurança e diretórios.
- O modelo pay-per-use o torna uma opção econômica para organizações que não têm recursos para comprar o software.
- Os clientes podem se concentrar em suas competências essenciais sem a necessidade de manter e gerenciar os recursos subjacentes.

Software como serviço

SaaS é um modelo de entrega de serviços através do qual o aplicativo completo é entregue aos clientes via Internet. Os clientes de SaaS não precisam comprar, gerenciar ou manter hardware ou software complexo. Os principais benefícios do SaaS incluem:

- Benefícios de custo significativos, pois os aplicativos SaaS geralmente são hospedados em um ambiente multilocatário, onde os custos associados a licenças de hardware e software são distribuídos
- Capacidade de escalar recursos para cima e para baixo, com base na demanda, sem preocupação com gerenciamento ou custos de hardware ou software

Modelo de responsabilidade compartilhada

QUER SABER MAIS?

- Leia *Gerenciando impactos de segurança em um ambiente multinuvem. www.isaca.org/multicloud-security-impacts*
- Saiba mais, discuta e colabore sobre informações e cibersegurança nos fóruns online da ISACA. *https://engage.isaca.org/onlineforums*

O modelo de responsabilidade compartilhada é uma estrutura que define as responsabilidades de segurança entre o CSP e seus clientes (**figura 1**). Ele evoluiu como um conceito novo e interessante para organizações que planejam migrar para a nuvem ou já migraram. Responsabilidade do cliente depende dos tipos de serviços que ele opta por usar.[3] No geral, um CSP é responsável por gerenciar a segurança e o cliente é responsável por proteger seus ativos na nuvem.

A complexidade adicional surge devido a diferenças entre os tipos de serviços na nuvem e entre provedores de serviços do mesmo tipo. Áreas de controle, como conformidade regulatória, são de responsabilidade de ambas as partes.

Na IaaS, a responsabilidade do provedor de serviços inclui áreas físicas como instalações, data centers e componentes de rede. A responsabilidade do CSP também se estende aos sistemas operacionais host que executam os aplicativos e o código.

O cliente pode ser responsável por:

- Configurar com segurança as cargas de trabalho do servidor em nuvem
- Indentificar e corrigir vulnerabilidades conhecidas
- Implementar de regras de segmentação
- Aplicar de controles preventivos, de detecção e corretivos de tempo de execução

No modelo PaaS, os provedores de serviços também gerenciam o sistema operacional convidado para que os clientes possam se concentrar no desenvolvimento de aplicativos, garantindo que os controles de segurança de aplicativos e dados estejam em vigor.

Os modelos SaaS colocam a responsabilidade máxima no provedor de serviços, como gerenciamento físico, infraestrutura e controle em nível de aplicativo. No entanto, o cliente ainda possui os dados e os processos relacionados ao acesso.

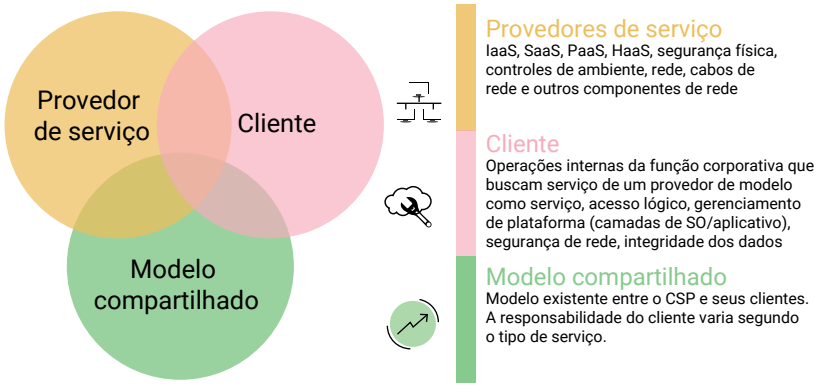
A **Figura 2** fornece um resumo dos controles pertencentes a um CSP típico versus seus clientes em cada modelo.

Principais desafios na adoção da nuvem

Os controles complementares da entidade do usuário (CUECs), também conhecidos como considerações de controle do usuário (UCCs), estão incluídos no sistema de um fornecedor, que o cliente deve implementar para garantir que os objetivos de controle do fornecedor sejam alcançados.[4] As organizações que movem seus recursos para a nuvem geralmente devem assumir que toda a responsabilidade relativa à gestão e segurança desses recursos foi transferida para o CSP. No entanto, este não é o caso. Na Demystifying the

FIGURA 1

Responsabilidades compartilhadas entre cliente e provedores de serviços



Cloud: Shared Responsibility Security Model, apenas 18% dos entrevistados mencionaram que entendem completamente sua responsabilidade em relação ao uso da nuvem para todos os tipos de serviço.[5] Isso é motivo de preocupação.

Exemplos de CUECs em um relatório de controle de organização de serviços que os clientes devem estar cientes incluem:

- **Acesso lógico**—Os direitos de acesso a aplicativos devem ser monitorados periodicamente quanto à adequação e para verificar se os deveres estão adequadamente segregados.
- **Gestão de mudanças**—O cliente deve identificar como as mudanças são configuradas e gerenciadas e revisar as requisições de mudança para ver se estão completas em relação ao processo de gerenciamento de mudanças estabelecido
- **Gerenciamento de interface**—As interfaces devem ser monitoradas para confirmar que todos os dados são aceitos e processados e que os resultados esperados são recebidos.
- **Implementação de plano de continuidade de negócios**—O cliente deve verificar se o plano de continuidade de negócios está em vigor e garantir que ele esteja de acordo com a estratégia de recuperação de negócios.

"As organizações que movem seus recursos para a nuvem geralmente assumem que toda a responsabilidade referente ao gerenciamento e segurança desses recursos foi transferida para o CSP."

FIGURA 2

Resumo dos controles de propriedade do CSP e seus clientes

Área de controle	IaaS	PaaS	SaaS
Controles físicos—O acesso físico aos data centers é restrito ao pessoal autorizado e os mecanismos estão em vigor para minimizar o efeito de um mau funcionamento ou desastre físico nas instalações do data center	CSP	CSP	CSP
Controles ambientais—Controles vinculados a monitores de incêndio, ar condicionado ou outras atividades do data center para apoiar a redução do risco de desastres	CSP	CSP	CSP
Integridade e confidencialidade dos dados—Controles para fornecer garantia razoável de que o manuseio de dados entre o cliente e o provedor de serviços de hospedagem é seguro	Cliente	Cliente	Cliente
Gerenciamento de identidade e acesso	**Cliente**	**Compartilhado**	**Compartilhado**
Políticas de acesso—Restrição de acesso lógico para verificar o acesso não autorizado	Cliente	Cliente	Cliente
Gerenciamento de identidade— Acesso de controle seguro a serviços e recursos para usuários	Cliente	CSP	CSP
Acesso e autenticação— controles de autenticação multifator (MFA) em todas as camadas de acesso ao ambiente	Cliente	CSP	CSP
Processos da camada de aplicativo	**Cliente**	**Compartilhado**	**CSP**
Segurança do aplicativo—Controles como proteção ou gerenciamento de patches usados para verificar a segurança adequada	Cliente	CSP	CSP
Lógica e código específicos do aplicativo—Controles em todo o ciclo de vida de desenvolvimento do aplicativo	Cliente	Cliente	CSP
Gerenciamento de rede	**Compartilhado**	**CSP**	**CSP**
Segurança e configuração de rede—Controles sobre a proteção contra problemas de segurança de rede, incluindo negação de serviço distribuído (DDoS), ataques man-in-the-middle (MitM), falsificação de protocolo de Internet (IP), varredura de porta ou detecção de pacotes	Cliente	CSP	CSP
Rede—Cabos de rede e outros componentes de rede	CSP	CSP	CSP
Monitoramento de rede—Controles sobre o uso da rede, varredura de portas, uso de aplicativos ou tentativas de intrusão não autorizada	CSP	CSP	CSP

Conclusão

Uma vez que o cliente entenda suas responsabilidades relacionadas à segurança de acordo com o modelo de responsabilidade compartilhada de seu CSP, ele deve determinar os controles aplicáveis em seu caso de uso. A responsabilidade do cliente varia com base em muitos fatores, incluindo serviços na nuvem e o modelo escolhido, a integração desses serviços em seu ambiente de TI e as leis e regulamentos aplicáveis à sua organização e carga de trabalho.[6]

Notas de rodapé

1 Akamai, "Content Delivery Networks—What Is a CDN?" *https://www.akamai.com/our-thinking/cdn/what-is-a-cdn*

2 Turco, K.; "Four Ways Cloud Computing Can Save Your Company Money" Technology Advice, 24 de junho de 2021, *https://technologyadvice.com/blog/information-technology/4-ways-cloud-computing-can-save-money/*

3 Simorjay, F.; E. Tierling; *Shared Responsibility for Cloud Computing*, Microsoft, EUA, outubro de 2019, *https://azure.microsoft.com/mediahandler/files/resourcefiles/shared-responsibility-for-cloud-computing/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf*

4 Hill, L.-M.; "Importance of Complementary User Entity Controls for Vendor Relationships," Venminder, 12 de outubro de 2021, *https://www.venminder.com/blog/importance-complementary-user-entity-controls-vendor-relationships*

5 Oracle e KPMG, *Demystifying the Cloud Shared Responsibility Security Model,* 2020, *https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf*

6 Amazon, "Shared Responsibility Model," *https://aws.amazon.com/compliance/shared-responsibility-model/*