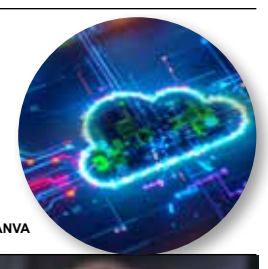
Empresas & Negócios

Matéria de capa



juststock_CANVA

TECNOLOGIA

MITOS E VERDADES SOBRE SEGURANÇA NA NUVEM

A segurança na nuvem é um assunto que pode parecer ambíguo, pode despertar tanto entusiasmo quanto receio no mundo dos negócios. Ao passo que as empresas movimentam suas operações para a nuvem, questões relacionadas à proteção de dados, privacidade e conformidade se tornam ainda mais críticas.

Roberto Martins (*)

No entanto, o debate sobre a segurança na nuvem é frequentemente ofuscado por vários mitos que precisam ser explicados. E por essa razão trago aqui alguns desses mitos e as verdades que os acompanham.

Mito 1: "Nuvens Não São Seguras" – Uma das ideias mais difundidas é que as Nuvens são altamente inseguras, sobretudo porque os dados estão armazenados fora das instalações da empresa. No entanto, essa visão simplificada ignora a complexidade e robustez das medidas de segurança implementadas pelos principais fornecedores do Cloud.

E a verdade é que os principais fornecedores de Cloud como AWS, Google Cloud e Microsoft Azure investem bilhões anualmente para sua segurança. Eles têm pessoal treinado, tecnologias de ponta e práticas rigorosas para proteger dados.

Além disso, a segurança em nuvem segue o modelo de responsabilidade compartilhada, onde o provedor garante a segurança da infraestrutura enquanto o cliente é responsável pela segurança de suas aplicações e dados. Em muitos casos, as práticas de segurança na nuvem superam aquelas encontradas em ambientes "on-premise".

Mito 2: "A Nuvem Não é Adequada para Dados Sensíveis" – Outro mito comum é a ideia de que dados altamente sensíveis, como informações financeiras ou de saúde, não devem ser armazenados na nuvem devido ao risco de vazamento ou roubo. E a verdade em relação a isso passa pela seguinte lógica:

Com as devidas precauções e configurações, a nuvem pode ser um dos ambientes mais seguros para dados sensíveis. As soluções de criptografia avançada, tanto para dados em repouso quanto em trânsito, garantem que informações críticas permaneçam inacessíveis a terceiros.

Além disso, muitos provedores de nuvem estão em conformidade com normas de segurança rigorosas, como GDPR, HIPAA e PCI-DSS, que regulamentam o tratamento destes mesmos. Tendo tudo isso dito em mente; Quais são os serviços necessários? E as políticas estabelecidas?

ALLVISIONN_CANVA

Mito 3 – "Provedores de Nuvem Têm Acesso aos Meus Dados" – A crença de que os provedores de nuvem têm acesso irrestrito aos dados de seus clientes é outra preocupação recorrente alimentando o medo da espionagem corporativa ou governamental. A verdade é que provedores de nuvem respeitáveis têm políticas rigorosas em relação à privacidade dos dados de seus clientes.

Em muitos casos, a criptografia de ponta a ponta é implementada, o que significa que apenas o cliente tem as chaves para decifrar seus dados. Além disso, contratos e acordos de serviço (SLAs) geralmente incluem cláusulas específicas que protegem os direitos dos clientes sobre seus dados, restringindo o acesso do provedor. É fundamental que as empresas entendam e escolham os serviços e configurações que garantam essa privacidade.

Mito 4 – "Migrar para a Nuvem é Suficiente para Garantir a Segurança" – Há uma falsa sensação de segurança entre algumas empresas que acreditam que, ao migrar para a nuvem, toda a responsabilidade pela segurança é transferida para o provedor. O fato é que a segurança em nuvem é uma responsabilidade compartilhada.

Enquanto os provedores garantem a segurança da infraestrutura, as empresas devem gerenciar corretamente o acesso aos dados, configurar firewalls, monitorar atividades suspeitas e implementar políticas de segurança interna. A negligência em qualquer uma dessas áreas pode expor dados críticos a riscos, independentemente da robustez do provedor de nuvem.

Mito 5 – "Ambientes MultiCloud Aumentam a Vulnerabilidade" – Com a crescente adoção de estratégias multicloud, onde empresas utilizam serviços de vários provedores, surge o mito de que isso aumenta a complexidade e, consequentemente, a vulnerabilidade a ataques. Embora a multicloud possa trazer desafios adicionais de gerenciamento, ela também oferece a oportunidade de melhorar a segurança.

Ao diversificar os provedores, as empresas podem mitigar o risco de falhas de segurança em um único ponto e aproveitar o melhor de cada serviço oferecido. No entanto, é essencial ter uma estratégia clara de gerenciamento de segurança que unifique a proteção de dados e a conformidade entre diferentes plataformas.

Mito 6: "Uma Brecha de Segurança na Nuvem Afetará Todas as Empresas que Utilizam o Serviço" – Existe uma crença de que, se uma brecha de segurança ocorrer em um provedor de nuvem, todas as empresas que utilizam seus serviços serão automaticamente afetadas. Para além da crença, a realidade é que as arquiteturas de nuvem modernas são projetadas com segmentação rigorosa e isolamento entre os diferentes clientes. Isso significa que, mesmo que uma vulnerabilidade afete um cliente, é improvável que ela comprometa outros usuários na mesma plataforma.

Os provedores de nuvem utilizam técnicas como "multi-tenancy" seguro e isolamento de rede para garantir que as operações de uma empresa não interfiram nas de outra. Portanto, a segurança de cada empresa depende muito de suas próprias configurações e práticas, além das medidas de segurança do provedor.

LaymanZoom_CANVA

Mito 7 –"A nuvem elimina a necessidade de backup local" – Enquanto alguns acreditam que não há mais nenhuma necessidade de ter backups locais, uma vez que os dados estão na nuvem, como o provedor de serviços de nuvem faz tudo. Os provedores de nuvem oferecem redundância e recuperação de desastres, ainda assim é de bom tom, e recomendado manter backups locais ou em nuvens secundárias.

Esta estratégia é referida como uma estratégia de backup 3-2-1; três cópias de dados em dois tipos diferentes de mídia, um dos quais deve estar fora do local. Ter uma cópia local ou uma cópia em outra nuvem separada pode proteger contra incidentes inesperados, como falhas de serviço, exclusão acidental de dados ou até mesmo questões legais que podem exigir acesso rápido e independente às informações.

A segurança na nuvem é um campo dinâmico e em constante mudança. Embora existam riscos associados ao uso da nuvem, a maioria desses medos são baseados em mitos ou informações obsoletas Ao entender o que realmente está por trás desses mitos, as empresas podem tomar decisões mais informadas e aproveitar plenamente as vantagens oferecidas pela nuvem sem comprometer a segurança de seus dados.

A chave para o sucesso está na seleção do provedor certo, implementando práticas de segurança robustas combinadas com as melhores práticas do mercado.

(*) - É especialista em Computação em Nuvem e CEO da Avantiv (https://avantiv.com/).