Seis maneiras de como a cloud computing dá suporte aos seus recursos de segurança

A adoção da cloud computing leva organizações a decidir entre a economia, escalabilidade e conveniência de usar um ambiente de nuvem ou o conforto de manter seus dados e aplicações hospedados de forma segura em seus próprios servidores. Mas o on-premise é mesmo mais seguro que a cloud computing? Muitos especialistas afirmam que não. Os seis fatores a seguir mostram por que você pode ter confiança em mudar para a cloud computing.

1 A segurança é dispendiosa

A segurança custa dinheiro. Pergunte-se: quanto minha empresa pode pagar por ela? A implantação de métodos de segurança necessários para seu data center on-premise é muito cara, especialmente para empresas de pequeno e médio porte. Não é prático tentar alcançar o nível de segurança aproximado ao oferecido por hiperescaladores.

2 A segurança exige recursos de pessoal significativos

Do mesmo modo, a segurança também exige mais recursos de pessoal. Os provedores de nuvem em larga escala possuem equipes de segurança trabalhando em tempo integral e um centro de operações de segurança completo para monitorar a infraestrutura de TI e hardware físico sem pausas. Por exemplo, o Microsoft Azure é protegido por uma equipe de mais de 3.500 especialistas em cibersegurança. A maioria das organizações não tem a capacidade de pessoal para fornecer o mesmo nível de segurança de hiperescaladores.

3 Provedores de nuvem estão inseridos no ramo da segurança

A segurança é importante para você, mas não é o seu ramo. Ela é uma das suas muitas preocupações, mas é a maior prioridade de provedores de nuvem. Para manter os negócios e continuar competitivos, os provedores de nuvem precisam entregar o maior nível de segurança para os clientes. Por exemplo, o Google oferece "infraestrutura de segurança por padrão" com proteção e criptografia embutidas como padrão.[1]

O Microsoft Azure identifica ameaças "ao analisar muitas fontes, incluindo 18 bilhões de web pages do Bing, 400 bilhões de emails, 1 bilhão de atualizações de dispositivos do Windows e 450 bilhões de autentificações mensais usando machine learning, análises comportamentais e inteligência baseada em aplicação como parte do Intelligent Security Graph da Microsoft."[2]

Os provedores de nuvem também precisam atender aos mais altos padrões, com certificações independentes e reconhecidas internacionalmente e auditorias do pessoal da segurança, processos e tecnologias por meio de vários programas rigorosos. Por exemplo, a Amazon Web Services (AWS) alcança validações de terceiros regularmente por milhares de requisitos de conformidade. A maioria das organizações não tem o tempo, recursos ou orçamento necessários para alcançar esse nível de garantia de segurança.[3]

1 *"Trust and security.", Google, acessado em 29 de abril de 2022.*

2 *"Strengthen your security posture with Azure.", Azure, acessado em 29 de abril de 2022.*

3 *"AWS cloud security." Amazon, acessado em 29 de abril de 2022.*

4 Ferramentas de segurança avançadas

Os provedores de nuvem implantam uma variedade de ferramentas avançadas de segurança para proteger as aplicações e dados do cliente. A AWS oferece identidade de alta granularidade e controles de acesso, monitoramento constante, detecção de ameaças, proteção de rede e aplicações, múltiplas camadas de criptografia, resposta e recuperação de incidentes automatizadas e muito mais. Os hiperescaladores oferecem acesso a centenas de soluções de segurança adicionais disponíveis nas lojas de parceiros. É praticamente impossível reproduzir o trabalho dessa grande variedade de ferramentas de segurança na sua própria rede e data center. O custo, contratação de pessoal, tempo e esforço exigidos exigem um comprometimento muito grande para uma empresa não especializada em segurança.

5 Segmentação de rede

Uma vantagem da segurança inerente ao ambiente de nuvem é a segmentação das estações de trabalho do usuário. Um método comum de ataque cibernético é ter como alvos usuários específicos no sistema por meio de email e sites. Nesses casos, a entrada no sistema acontece pelas estações de trabalho do usuário. No entanto, em um ambiente de nuvem, essas estações têm conectividade suficiente apenas para permitir que os usuários desempenhem suas tarefas. Elas não possuem acesso direto à rede empresarial. Então, mesmo que uma delas seja comprometida, o invasor não consegue acesso a empresa e suas aplicações e dados.

6 Segurança física

A segurança física ainda é um fator crítico. Pessoas com acesso físico direto ao hardware podem representar um sério risco em potencial à segurança. No entanto, se os dados e aplicações estiverem em um ambiente de nuvem, funcionários descontentes ou que possam causar danos acidentais presencialmente não têm mais acesso fácil a esses recursos. É muito mais difícil para eles localizarem dados em um ambiente de nuvem.

Além disso, os hiperescaladores têm recursos para prevenir roubo físico de dados, incluindo guardas de segurança, servidores trancados à chave e outros controles de segurança física de ponta que a maioria das organizações não tem.

Leia mais

Leia o artigo "Empowering developers through cloud services" para mais informações sobre como o Red Hat® Cloud Services pode ajudar você na sua jornada para aplicações nativas em nuvem.

Sobre a Red Hat

A Red Hat ajuda os clientes a definir padrões entre diferentes ambientes, desenvolver aplicações nativas em nuvem, integrar, automatizar, proteger e gerenciar ambientes complexos com serviços de consultoria, treinamento e suporte premiados.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

br.redhat.com
#F31540_0522

Copyright © 2022 Red Hat, Inc. Red Hat e o logotipo da Red Hat são marcas comerciais ou registradas da Red Hat, Inc. e suas subsidiárias nos Estados Unidos e em outros países.