Seis maneiras de falhar com a sua cloud empresarial

OVHcloud

vmware®

O cloud computing tem-se imposto cada vez mais no mundo informático tradicional. Com uma transformação digital visível em todos os setores, as empresas recorrem a estratégias multicloud para melhor se adaptarem às novas exigências do mercado. Para as empresas, um elemento essencial desta abordagem é a cloud privada, que é considerada intrinsecamente mais segura do que a cloud pública.

Apesar de uma cloud privada empresarial oferecer um maior controlo sobre o ambiente físico e capacidades de personalização inigualáveis, criar a sua cloud privada tem os seus riscos...

Violações de segurança

As violações de dados, informações de identificação comprometidas, sistemas de autenticação corrompidos, interfaces e API pirateadas: 2018 ficou marcado por violações massivas da segurança. As informações semanais sobre novos ciberataques e violações de segurança não ajudam a atenuar as desconfianças associadas ao cloud computing.

Isto leva muitas empresas a pensar que os seus dados ficam mais seguros internamente, nos seus próprios ambientes cloud. Na realidade, os ambientes alojados são tão seguros quanto os que são acolhidos on-premises, ou até mais seguros. São concebidos e geridos por especialistas em segurança que compreendem os desafios da segurança na cloud e sabem como enfrentá-los.

Ataques DDoS

Os ataques distribuídos de negação de serviço (DDoS) continuam a ser uma importante preocupação para todas as empresas digitais. Ao longo dos anos, os responsáveis pelos ataques tornaram-se cada vez mais sofisticados nos seus métodos, e com as novas tecnologias, como a Internet dos Objetos (IoT), surgem novas ameaças.

Um ataque DDoS sobrecarrega um servidor web e, caso seja bem-sucedido, torna o website inacessível durante horas ou dias, podendo provocar uma perda em termos de receitas, assim como de confiança dos clientes. Uma boa proteção contra os ataques DDoS já não é uma simples funcionalidade prática para as empresas: é um elemento imprescindível para qualquer sistema de segurança. No entanto, a proteção das infraestruturas no local nunca poderá estar à altura da capacidade dos sistemas líderes do setor para limitar os ataques DDoS.

---

[1] *IDC Infobrief, Junho de 2019.*

"Enquanto fornecedor de serviços cloud, recebemos e mitigamos mais de 2000 ataques DDoS por dia. Por predefinição, o nosso sistema anti-DDoS protege todos os clientes. A razão é muito simples: um ataque DDoS, se não for mitigado, pode causar danos colaterais. Isto significa que afetará o alvo que está a ser atacado, assim como todos os servidores vizinhos do rack. O VAC (uma combinação de tecnologias desenvolvidas pela OVHcloud para atenuar os ataques DDoS) só é ativado quando um ataque é detetado. No entanto, para os clientes com necessidades específicas em matéria de segurança, a OVHcloud propõe uma filtragem constante do tráfego, ou seja, uma ativação permanente do VAC".

Jakub Słociński, Network Innovation Manager na OVHcloud.

Segurança física e redundância

A maioria das empresas não dispõe das mesmas funcionalidades de segurança física que os datacenters de terceiros, o que pode pôr em perigo os seus dados valiosos. Um datacenter fiável será como uma fortaleza, com estritas medidas de acesso e protegido por uma vedação de arame farpado. Os sistemas de videovigilância e deteção de movimentos devem funcionar continuamente, tal como os sistemas de deteção e de extinção de incêndios.

Atualmente, a acessibilidade permanente, a alta disponibilidade e a resiliência são elementos essenciais para muitos serviços informáticos. Atingir o mesmo nível de redundância para uma cloud privada alojada internamente seria uma tarefa ambiciosa. A dupla alimentação elétrica, os geradores de energia, os dispositivos UPS e as ligações de rede redundantes acarretam custos de manutenção elevados e requerem um elevado nível de competência por parte das equipas internas.

Problemas de conformidade

As normas PCI DSS incluem mais de 250 controlos e funções de segurança para garantir o processamento seguro dos dados dos cartões de pagamento. Uma cloud privada oferece um maior controlo em termos de segurança, mas não facilita os processos de conformidade regulamentar.

A manutenção da conformidade deve estar sempre na linha da frente do planeamento, em especial quando estão envolvidos vários tipos de dados regulamentados, como os dados sobre cartões de pagamento, a informação comercial sensível e os dados dos clientes. Trata-se de um processo demorado e oneroso, que requer muitas vezes a intervenção de um especialista informático com bons conhecimentos destas regulamentações. Além disso, a equipa informática deverá monitorizar continuamente os sistemas, desenvolver procedimentos claros em caso de incidente de segurança e utilizar a encriptação dos dados para garantir que os requisitos de conformidade são constantemente respeitados.

Problemas de desempenho

Os problemas de desempenho são bem conhecidos nos ambientes virtualizados dinâmicos, nos quais é difícil prever a forma como as alterações a nível da infraestrutura afetarão o desempenho das aplicações, uma vez que até uma simples atualização de software pode desequilibrar um ecossistema fechado. Para garantir que tira o melhor partido da sua infraestrutura, é essencial implementar um processo contínuo para validar o desempenho da cloud. Para qualquer nova implementação e alteração relevantes, deverá realizar testes de desempenho realistas, de preferência automatizados, que permitam detetar os problemas numa fase inicial. A implementação de um processo deste tipo protege a sua empresa contra custos desnecessários e permite-lhe manter um estreito controlo sobre a relação preço/desempenho.

Compra desnecessária de recursos

Quer esteja a construir a sua cloud privada com OpenStack ou VMware, o desafio será sempre o mesmo: como alcançar flexibilidade e escalabilidade na gestão de uma infraestrutura interna?