AS TRÊS PRINCIPAIS CONSIDERAÇÕES DE SEGURANÇA PARA A NUVEM

Um centro de dados é um ambiente fixo em que os aplicativos são executados em servidores dedicados que podem ser acessados somente por usuários autorizados. Por outro lado, um ambiente em nuvem é dinâmico e automatizado, em que conjuntos de recursos de computação estão disponíveis para oferecer suporte a cargas de trabalho do aplicativo que podem ser acessados de qualquer lugar, a qualquer momento, de qualquer dispositivo. Para o profissional com experiência em segurança da informação, parece que vários dos princípios que tornam a computação em nuvem atraente são contrários às melhores práticas da segurança de rede. A seguir estão as três principais considerações para proteger os centros de dados tradicionais e os baseados em nuvem, bem como os requisitos-chave para a segurança da nuvem.

A computação em nuvem não diminui os riscos de segurança de rede existentes

Os riscos de segurança que hoje ameaçam um centro de dados e a rede mudam quando os aplicativos se mudam para a nuvem, seja em uma migração completa ou em um cenário híbrido no qual alguns aplicativos se mudam para a nuvem enquanto outros permanecem no local. Na verdade, de várias formas, os riscos de segurança enfrentados quando se muda para a nuvem se tornam mais significativos.

Por exemplo, vários aplicativos do centro de dados usam uma vasta gama de portas, tornando medidas de segurança tradicionais ineficazes quando esses aplicativos se mudam para a nuvem. Criminosos cibernéticos estão criando sofisticados ataques agnósticos para portas que usam múltiplos vetores para comprometer seu alvo, ocultando às claras os aplicativos comuns para concluir sua missão.

A segurança deseja separação e segmentação – A nuvem depende de recursos compartilhados

Durante décadas, as melhores práticas de segurança da informação ditaram que aplicativos e dados essenciais fossem separados em segmentos seguros na rede. Normalmente, isso é chamado de Confiança Zero: nunca confie, sempre verifique.

Em uma rede física dentro do centro de dados empresarial, a Confiança Zero é relativamente simples de implantar por meio do uso de firewalls e VLANs (ou seja, LANs virtuais), gerenciados por políticas com base em aplicativo e na identidade do usuário.

INFORMAÇÕES E INSIGHTS

Em um ambiente de computação em nuvem, a comunicação direta entre máquinas virtuais dentro de um servidor ocorre de forma constante, em alguns casos, em níveis variados de confiança. Isso torna a segmentação uma tarefa difícil, especialmente quando se leva em conta que os aplicativos em nuvem se baseiam na noção de recursos compartilhados. Níveis mistos de confiança, quando combinados com uma falta de visibilidade do tráfego dentro do host por ofertas de segurança baseadas na porta virtualizada, provavelmente introduzirão uma postura de segurança enfraquecida.

As configurações de segurança são orientadas por processo | Os ambientes de computação em nuvem são dinâmicos

Cargas de trabalho virtuais podem ser criadas ou modificadas em minutos. Assim, as equipes de computação em nuvem operam em um ambiente altamente dinâmico, com cargas de trabalho sendo incluídas, removidas e alteradas de forma constante.

Por outro lado, a configuração de segurança para essa carga de trabalho pode levar horas, dias ou semanas. Os atrasos na segurança não são projetados para criar bloqueios. Em vez disso, eles são o resultado de um processo projetado para manter uma forte postura de segurança. As mudanças na política precisam ser aprovadas, os firewalls adequados precisam ser identificados e as atualizações de política relevantes determinadas.

A menos que esse desequilíbrio seja entendido e tratado como parte da migração para nuvem, o resultado será uma discrepância entre a política de segurança e a implantação da carga de trabalho na nuvem. O resultado é uma postura de segurança enfraquecida que pode colocar dados importantes e a propriedade intelectual em perigo e pode também causar violações de conformidade, além de políticas e regulamentos de governança.

Principais requisitos para segurança na nuvem

- **Segurança** consistente em fatores de forma física e virtualizada. Os mesmos níveis de controle de aplicativo, manipulação de aplicativos invasivos e configurados incorretamente e prevenção de ameaças são necessários para proteger o ambiente de computação em nuvem e a rede física.
- **Aplicativos** de negócios do segmento usando princípios de Confiança Zero. Para maximizar completamente o uso de recursos de computação, agora é prática relativamente comum combinar níveis de confiança de carga de trabalho do aplicativo no mesmo recurso de computação. O objetivo é controlar o tráfego entre cargas de trabalho ao mesmo tempo em que se impede a movimentação lateral de ameaças.
- **Gerenciar** centralmente as implantações de segurança e simplificar as atualizações de política. A segurança da rede física ainda é implantada na maioria das organizações, de modo que é crítico ter a capacidade de gerenciar implantações de hardware e de fator de forma virtualizado a partir de um local centralizado usando a mesma infraestrutura e interface de gerenciamento. A solução selecionada deve ser capaz de abranger ambientes físicos e virtuais por meio de um gerenciamento de política e uma estrutura de execução consistentes e deve incluir recursos que automatizam as atualizações da política de segurança.

Para saber mais sobre como proteger os centros de dados tradicionais e os baseados em nuvem com firewalls de última geração, leia o **artigo técnico**.