Construção de confiança em um céu nebuloso

Os serviços na nuvem são atualmente um componente habitual das operações de TI, sendo utilizados por mais de 90% das organizações em todo o mundo. Muitos estão trabalhando segundo uma filosofia de "nuvem em primeiro lugar", optando por distribuir um serviço interno somente quando não há disponível uma variante adequada para nuvem. Consequentemente, as arquiteturas de TI estão mudando rapidamente para um modelo híbrido de nuvem privada/pública. Nossos entrevistados esperam que 80% de seus orçamentos de TI sejam baseados na nuvem dentro de um prazo médio de 15 meses.

A Intel Security consultou mais de 2.000 profissionais de TI em setembro de 2016 para produzir este exame anual do estado da adoção da nuvem, representando uma ampla variedade de setores, países e tamanhos de organização. Diante da escassez continuada de pessoal qualificado em segurança, consideramos uma prioridade o impacto dessa escassez na adoção da nuvem no relatório deste ano. Outros objetivos foram compreender a adoção de diferentes modelos de utilização da nuvem, identificar as principais preocupações relacionadas a serviços em nuvens públicas e privadas e investigar a evolução do impacto da TI oculta.

Os participantes da pesquisa foram técnicos seniores responsáveis pela tomada de decisões em organizações pequenas (500 a 1.000 funcionários), médias (1.000 a 5.000 funcionários) e grandes (mais de 5.000 funcionários) na Alemanha, Austrália, Brasil, Canadá, Cingapura, Costa do Golfo (Arábia Saudita e Emirados Árabes Unidos), Estados Unidos, França, Japão, México e Reino Unido.

93%

das organizações **utilizam serviços de nuvem** de alguma forma.

49%

dos entrevistados **atrasaram sua adoção da nuvem** por falta de qualificações em cibersegurança.

62%

das organizações disseram que **armazenam informações pessoais de clientes** em nuvens públicas.

Principais descobertas

- Os serviços de nuvem são amplamente utilizados, de alguma forma, com 93% das organizações utilizando ofertas de software, infraestrutura ou plataforma como serviço.
- O número médio de serviços de nuvem em uso em uma organização caiu de 43 em 2015 para 29 em 2016, indicando uma possível consolidação de soluções ou provedores de nuvem. As arquiteturas de nuvem também mudaram significativamente, de predominantemente privadas em 2015 para uma adoção crescente da nuvem pública, resultando em uma infraestrutura público-privada híbrida em 2016.
- Quase a metade (49%) dos profissionais consultados afirmaram ter desacelerado sua adoção da nuvem devido a uma falta de qualificações em segurança cibernética, sendo essa escassez mais pronunciada no Japão, no México e nos países da Costa do Golfo.
- A confiança e a percepção dos serviços na nuvem pública continuam melhorando a cada ano. A maioria das organizações considera os serviços na nuvem mais seguros que nuvens privadas e com mais chances de proporcionar menores custos de propriedade e melhor visibilidade dos dados. As organizações que confiam em nuvens públicas já superam, em uma proporção de dois para um, as que delas desconfiam.

intel Security

Resumo executivo

52%

dos entrevistados rastrearam uma **infecção de malware até um aplicativo SaaS**.

40%

dos serviços de nuvem são **instalados sem o envolvimento do departamento de TI**.

65%

dos profissionais de TI acham que **a nuvem oculta está interferindo** em sua capacidade de manter a nuvem segura.

Dois anos

Prazo no qual os entrevistados esperam ter um **data center completamente definido por software**.

- Esse aumento de confiança e percepção, bem como a maior compreensão dos riscos pela diretoria sênior, está incentivando mais organizações a armazenar dados sigilosos na nuvem pública. As informações pessoais dos clientes são o tipo de dados mais provável a ser armazenado em nuvens públicas, sendo lá mantido por 62% dos entrevistados.
- Os aplicativos de nuvem continuam sendo um vetor para ataques cibernéticos e mais da metade (52%) dos entrevistados indicaram ter rastreado conclusivamente uma infecção de malware até um aplicativo SaaS.
- A TI oculta é uma preocupação crescente para o departamento de TI. Em decorrência da adoção mais lenta pelo departamento de TI ou da aceitação generalizada das nuvens, quase 40% dos serviços de nuvem são instalados sem o envolvimento do departamento de TI. Como resultado, 65% dos profissionais de TI acham que esse fenômeno está interferindo em sua capacidade de manter a nuvem segura.
- A virtualização de arquiteturas de data centers privados está avançando. Em média, 52% dos servidores de data center de uma organização são virtualizados e a maioria das organizações espera concluir em dois anos a conversão para um data center exclusivamente definido por software.

Conclusões e recomendações

As empresas estão confiando aos serviços de nuvem uma ampla variedade de dados e aplicativos, muitos dos quais confidenciais ou fundamentais para os negócios. Os dados vão para onde são mais necessários, mais eficazes e mais eficientes, e a segurança precisa estar presente com antecedência, para detectar ameaças rapidamente, proteger a organização e corrigir tentativas de comprometimento dos dados. A economia de custos e recursos obtida com os serviços de nuvem é verdadeira e a ampla variedade de ofertas permite escolher a mais adequada à organização. Os fornecedores de segurança estão oferecendo ferramentas para lidar com questões fundamentais de segurança, como proteção dos dados em trânsito, gerenciamento dos acessos dos usuários e configuração de políticas consistentes entre múltiplos serviços.

A movimentação de dados confidenciais para a nuvem pública pode atrair cibercriminosos. Os atacantes procurarão os alvos mais fáceis, independentemente de onde estes se encontrem. Soluções de segurança integradas ou unificadas são uma defesa forte contra essas ameaças, ao proporcionar às operações de segurança visibilidade sobre todos os serviços que a organização utiliza e sobre quais conjuntos de dados podem passar por eles.

Credenciais de usuários, especialmente de administradores, serão a forma de ataque mais provável. As organizações devem se certificar de utilizar as melhores práticas de autenticação, como senhas diferentes, autenticação de múltiplos fatores e até mesmo biometria, quando disponível.

Apesar da percepção predominante de que a TI oculta está colocando a organização em risco, tecnologias de segurança, como prevenção de perda de dados (DLP), criptografia e agentes de segurança de acesso à nuvem (CASBs), continuam subutilizados. Integrar essas ferramentas ao sistema de segurança existente aumenta a visibilidade, permite a descoberta de serviços ocultos e proporciona opções para proteção automática de dados confidenciais estacionários e em movimento em qualquer tipo de ambiente.

Embora seja possível terceirizar o trabalho para várias partes, não é possível terceirizar o risco. As organizações precisam evoluir rumo a uma abordagem de mitigação e gerenciamento do risco para conseguir a segurança da informação. Considere a adoção de uma estratégia de "nuvem em primeiro lugar" para incentivar a adoção de serviços de nuvem, reduzindo os custos e aumentando a flexibilidade, e colocar as operações de segurança em uma posição proativa em vez de reativa.

Para ler o relatório completo, **faça o download**.

intel Security

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com