Construção de confiança em um céu nebuloso

Visão global das organizações de assistência médica

As oportunidades de redução de custos e a rápida digitalização das informações médicas talvez sejam as responsáveis por um fenômeno curioso: o uso de serviços de nuvem pelo setor de assistência médica é um pouco superior à média global do setor. Enquanto 96% dessas organizações usam serviços de nuvem, a média do setor como um todo é de 93%. Assim como as organizações de outros setores, 81% trabalham segundo uma filosofia de "nuvem em primeiro lugar", optando por distribuir um serviço interno somente quando não estiver disponível uma variante adequada para a nuvem. Em decorrência disso, as arquiteturas de TI do setor de assistência médica estão mudando gradualmente de uma infraestrutura de data center de nuvem privada 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.

Esta análise de adoção dos serviços de nuvem pelo setor de assistência médica, suas preocupações e seus planos para o futuro foi extraída da **Pesquisa sobre nuvem de 2016, da Intel Security**. Foram entrevistados tomadores de decisões de TI de nível técnico sênior de diversas localidades: Alemanha, Austrália, Brasil, Canadá, Cingapura, Estados Unidos, França, Golfo Pérsico (Arábia Saudita e Emirados Árabes Unidos), Japão, México e Reino Unido.

Principais descobertas: setor de assistência médica

De acordo com nossa pesquisa, o setor de assistência médica está entre os três setores com maior adoção da nuvem (96%), perdendo apenas para os setores financeiro (99%) e tecnológico (99%). A porcentagem indica a parcela do setor que opera algum tipo de serviço de nuvem. A quantidade média de serviços de nuvem utilizados pelas organizações de assistência médica caiu de 41 em 2015 para 33 em 2016. Essa queda foi menor do que a registrada na média global, de 43 para 29 serviços, mas também indica uma possível consolidação de provedores ou serviços de nuvem.

As arquiteturas de nuvem passaram por uma mudança considerável: se em 2015 elas eram em sua maioria de natureza exclusivamente privada, agora são predominantemente híbridas (privadas/públicas), mas as organizações de assistência médica foram as que menos usaram arquiteturas híbridas. Curiosamente, as organizações de assistência médica figuraram entre as maiores usuárias de serviços de nuvem exclusivamente pública (SaaS, IaaS ou PaaS), com 24%, bem acima da média global de 19%. Os profissionais seniores de TI no setor de assistência médica afirmam ser duas

96%

de adoção de nuvem coloca o setor de assistência médica entre os **três maiores setores** em adoção de nuvem

24%

das organizações de assistência médica usam serviços de nuvem **exclusivamente pública** (SaaS, IaaS ou PaaS)

intel Security

46%

dos entrevistados **atrasaram sua adoção da nuvem** por falta de qualificação em segurança cibernética

60%

das organizações de assistência médica **armazenam dados de clientes (pacientes)** em nuvens públicas

52%

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

38%

dos serviços de nuvem em organizações de assistência médica são **contratados sem o envolvimento da TI, sendo que a TI só tem visibilidade sobre metade deles**

vezes mais propensos a usar SaaS do que IaaS ou PaaS. O modelo SaaS também será o foco principal desse setor no próximo ano: 67% das organizações de assistência médica pretendem aumentar seus investimentos nesses serviços.

Quase metade (46%) dos profissionais de assistência médica entrevistados afirmaram ter atrasado sua adoção da nuvem devido à falta de qualificação na área de segurança cibernética. Isso ficou particularmente claro quando perguntamos a eles sobre suas preocupações com o modelo de IaaS. A qualificação exigida da equipe de segurança de TI foi a maior preocupação dos entrevistados do setor de assistência médica em relação ao IaaS, superando a necessidade de controles de segurança consistentes e integrados (a maior preocupação do grupo geral entrevistado sobre o mesmo assunto).

Ainda que a qualificação exigida na área de segurança esteja diminuindo o ritmo de adoção, a confiança e a percepção dos serviços de nuvem pública continuam aumentando a cada ano entre as organizações de assistência médica. A maioria dessas organizações considera os serviços de nuvem pública tão seguros quanto os de nuvem privada (ou até mais seguros), com chances muito maiores de proporcionar redução dos custos de propriedade e melhor visibilidade dos dados. Mais de dois terços das organizações confiam nas nuvens públicas. Esse aumento de confiança e percepção, bem como a maior compreensão dos riscos pela diretoria sênior, está incentivando mais organizações do setor de assistência médica a armazenar dados confidenciais na nuvem pública. Uma possível explicação é a preocupação acima da média dos entrevistados do setor (37% contra 30% da média global) com o acesso não autorizado a dados confidenciais na nuvem privada. Talvez devido aos prontuários eletrônicos e à natureza interconectada do sistema de assistência médica, essas organizações estão entre as mais propensas a armazenar alguns de seus dados confidenciais (ou todos) na nuvem pública, especialmente dados de pacientes (60%) e da equipe (54%).

Apesar disso, os aplicativos de nuvem continuam sendo um vetor para ataques cibernéticos e mais da metade (52%) dos entrevistados do setor de assistência médica afirmam ter rastreado conclusivamente uma infecção de malware até um aplicativo SaaS. Essas organizações também estão entre as mais afetadas por perda de dados (25% em relação à média global de 22%) ou incidentes de malware (13% em relação à média global de 10%) com provedores de serviços de nuvem.

A TI oculta continua sendo um problema para os departamentos de TI do setor de assistência médica, assim como acontece com os departamentos de TI da maioria dos setores. O uso de SaaS nem sempre recebe o aval do departamento de TI. Os profissionais do setor de assistência médica relatam que serviços de nuvem contratados sem o envolvimento da TI chegam a 38% de seu uso de serviços. A TI só tem visibilidade sobre metade desses aplicativos. Quando um aplicativo de TI oculta não autorizado é detectado, a resposta mais comum é bloquear completamente o acesso ao aplicativo. De modo geral, os profissionais de TI do setor de assistência médica estão bastante preocupados com a TI oculta: 63% deles afirmam que o fenômeno prejudica sua capacidade de manter a segurança na nuvem.

Embora as organizações de assistência médica estejam adotando o modelo SaaS e apresentem uso acima da média dos serviços de nuvem exclusivamente públicos, 26% continuam usando apenas serviços totalmente privados, enquanto 50% usam uma combinação híbrida de serviços públicos e privados. Na área privada, a porcentagem atual de servidores virtualizados no data center está um pouco abaixo da média global (51% contra 52%) e os profissionais de assistência médica afirmam estar entre os maiores usuários de contêiners. A maioria (76%) espera concluir a transição para um data center totalmente definido por software dentro de dois anos.

Conclusões e recomendações

Aparentemente, as organizações de assistência médica são mais propensas a usar aplicativos de SaaS do que outros setores. Elas estão em posição intermediária no uso de nuvens privadas e entre as menores usuárias de nuvens híbridas. Não se sabe ao certo se a culpa é desse uso da nuvem pública, do aumento do valor de seus dados ou de uma combinação das duas coisas, mas o fato é que essas organizações têm registrado mais ataques cibernéticos, incidentes de malware e perda de dados do que as organizações da maioria dos outros setores.

As nuvens vieram para ficar, e as equipes de operações de segurança do setor de assistência médica precisam estar um passo à frente da curva de adoção para manter as organizações protegidas. A ampla variedade de ofertas de nuvem disponíveis permite que as organizações escolham aquela que é mais adequada, atendendo às necessidades de custo e de segurança. Os fornecedores de segurança oferecem as ferramentas necessárias 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.

As organizações de assistência médica têm prontuários médicos valiosos, que atraíram ataques de ransomware (vírus sequestrador) de criminosos cibernéticos no ano passado, de acordo com o **Relatórios do McAfee Labs sobre ameaças de dezembro de 2016**. Ao mesmo tempo, os profissionais de assistência médica estão adotando ativamente tecnologias que aumentam a qualidade e a eficácia do atendimento aos pacientes. Os atacantes continuarão procurando pelos alvos mais fáceis, não importando onde eles estejam. Soluções de segurança integradas ou unificadas são uma defesa forte contra essas ameaças, proporcionando às equipes de operações de segurança visibilidade sobre todos os serviços que a organização utiliza e sobre quais conjuntos de dados podem transitar entre eles.

De acordo com o **Relatório de previsões do McAfee Labs sobre ameaças de 2017**, as credenciais de usuários, especialmente de administradores, serão a forma de ataque mais provável. Certifique-se de que sua proteção seja apropriada em todos os endpoints, incluindo tablets e smartphones. As melhores práticas de autenticação, como o uso de senhas diferentes, a autenticação por múltiplos fatores e a biometria (quando disponível), serão essenciais para a criação de estratégias preventivas que reduzam consideravelmente o risco de infecção ou comprometimento.

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 subutilizadas. 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 trânsito 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 para colocar as operações de segurança em uma posição proativa em vez de reativa.

Para obter informações mais detalhadas, leia o relatório completo, **Construção de confiança em um céu nebuloso**.

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