Academia de Tecnologia da IBM
White paper de liderança de pensamento

Novembro de 2010

Estratégias para avaliação da segurança da computação em nuvens

Resumo executivo

A computação em nuvem possibilita maior flexibilidade e entrega de serviços de Tecnologia de Informação muito efetiva em termos de custos utilizando como infraestrutura os recursos e padrões utilizados pela Internet. Os recursos de computação em nuvem podem ser rapidamente implantados e facilmente escalados, com todos os processos, aplicações e serviços fornecidos sob demanda, independentemente da localização ou dispositivo do usuário. Consequentemente, a computação em nuvem ajuda as organizações a melhorarem a prestação de serviços, a aperfeiçoar o gerenciamento de TI e alinhar melhor os serviços de TI atendendo às exigências dinâmicas do negócio. A computação em nuvem também pode oferecer suporte simultâneo às principais funções do negócio e fornecer capacidade para serviços inovadores.

Atualmente, estão sendo utilizados os modelos de nuvens pública e privada ou uma abordagem híbrida que utilize os dois modelos. Disponíveis para qualquer indivíduo com acesso à Internet, a nuvem pública é adquirida como um serviço e paga de modo correspondente ao consumo ou por assinatura. A nuvem privada é de propriedade e utilizadas por uma única organização. Oferece muitos dos benefícios da nuvem pública, com maior flexibilidade e controle.

Embora os benefícios da computação em nuvem sejam claros, assim também é a necessidade de desenvolver uma segurança adequada para as implementações de computação em nuvem – pública ou privada. Adotar a computação em nuvem sem os controles de segurança adequados pode colocar em risco toda a infraestrutura de TI. A computação em nuvem apresenta outro nível de risco porque os serviços fundamentais, muitas vezes, são terceirizados, tornando difícil manter a integridade e privacidade dos dados, oferecer suporte à disponibilidade dos dados e serviços e demonstrar a conformidade. Mesmo se for feita a transição das cargas de trabalho de TI à nuvem, os usuários ainda são responsáveis pela conformidade e segurança dos dados. Como resultado, os usuários devem estabelecer relações de confiança com seus provedores de serviços de nuvem e compreender os riscos apresentados pelos ambientes público e/ou privado de computação em nuvem.

Desafios de segurança na nuvem – a necessidade de avaliação por um terceiro

Uma das diferenças mais significativas entre a segurança da computação em nuvem e a segurança tradicional de TI provém do compartilhamento de infraestrutura em massa. Os usuários que compreendem diferentes corporações e níveis de confiança, muitas vezes, interagem com o mesmo conjunto de recursos de computação. Os serviços de nuvem pública estão sendo cada vez mais oferecidos por uma cadeia de provedores – todos eles armazenam e processam dados externamente em diversas localidades não especificadas.

Dentro da nuvem, é difícil de localizar fisicamente onde os dados são armazenados. Os processos de segurança que eram visíveis, agora estão escondidos por camadas de abstração. Esta falta de visibilidade pode causar preocupações sobre a exposição dos dados e comprometer a confiança dos serviços, a capacidade de demonstrar conformidade e cumprir os Contratos de Nível de Serviço (SLAs) e o gerenciamento geral de segurança.

A visibilidade pode ser principalmente crítica para a conformidade. A lei Sarbanes-Oxley, a lei de Responsabilidade e Portabilidade de Seguro de Saúde (HIPAA), as leis de privacidade européias e muitos outros regulamentos exigem recursos abrangentes de auditoria. Muitas nuvens públicas podem, de fato, ser uma caixa preta para o usuário e,

portanto, os clientes podem não ser capazes de demonstrar conformidade. (Uma nuvem privada ou híbrida, por outro lado, pode ser configurada para atender essas exigências).

Além disso, muitas vezes, os provedores precisam oferecer suporte às auditorias de terceiros ou às iniciativas de e-Discovery e investigações. Isso reforça ainda mais a importância em manter uma visibilidade adequada na nuvem. A descoberta legal dos dados de um co-locatário pode afetar a confidencialidade dos dados de outro locatário, se os dados não forem devidamente segmentados. Isso pode significar que alguns dados sensíveis podem não ser adequados para certos ambientes de computação em nuvem.

As organizações que consideram serviços com base em computação em nuvem devem compreender os riscos associados e garantir a visibilidade adequada. As diretrizes da IBM para proteção das implementações de nuvem concentram-se nas seguintes áreas:

- Criação de um programa de segurança
- Proteção de dados confidenciais
- Implementação de proteção de acesso e identidade
- Provisionamento e desprovisionamento de aplicativos
- Gerenciamento de auditoria da governança
- Gerenciamento de vulnerabilidades
- Testes e validação

Já que a computação em nuvem está disponível em diversos modelos de serviços (e formas híbridas desses modelos), cada um deles apresenta níveis diferentes de responsabilidade pelo gerenciamento da segurança. Parceiros confiáveis podem ajudar as empresas a aplicar as melhores práticas de segurança na computação em nuvem de acordo com suas necessidades comerciais específicas.

Desenvolvimento de um guia estratégico de segurança em computação na nuvem com a IBM

Não há um modelo único para segurança na computação em nuvem. As organizações têm exigências diferentes de segurança que são determinadas pelas características exclusivas da carga de trabalho comercial que pretendem migrar para a computação em nuvem ou dos serviços que prestam a partir de sua nuvem. Ao avaliar os riscos de um modelo de computação em nuvem, é importante que haja uma estratégia de segurança desenvolvida.

Com a experiencia em segurança da IBM, os clientes podem se beneficiar das metodologias e melhores práticas comprovadas de avaliação que ajudam a garantir resultados consistentes e confiáveis. Eles também podem aproveitar as estruturas abrangentes que abordam a estratégia, implementação e gerenciamento de computação em nuvem da empresa em uma abordagem holística que maximiza o valor comercial dos investimentos em nuvem, ao mesmo tempo em que minimiza o risco comercial.

Definição das estratégias do negócio e de TI

A primeira etapa para compreender os riscos de segurança apresentados por um modelo de computação em nuvem é analisar as estratégias de TI e do negócio. Qual valor das informações que serão armazenadas, acessado e transmitido através da nuvem? Ele é fundamental e/ ou confidencial para o negócio? Ele é sujeito a conformidade regulamentar? Os clientes também devem considerar as exigências de disponibilidade. Após determinar a estratégia de TI e do negócio e avaliar os dados, os clientes podem tomar uma decisão mais fundamentada e com base nos riscos acerca de qual modelo de computação em nuvem adotar.

Identificação dos riscos

Cada tipo de nuvem – pública, privada e híbrida – possui um nível diferente de risco de segurança à TI. Os especialistas em segurança da IBM podem ajudar os clientes a identificar as vulnerabilidades, ameaças e outros valores em risco com base na arquitetura de nuvem pública, privada ou híbrida. A partir disso, a IBM trabalhará com os clientes para projetar os mecanismos e controles iniciais para atenuar riscos e destacar os procedimentos de manutenção e testes que auxiliarão a garantir uma atenuação contínua dos riscos.

Documentação do plano

Os clientes IBM se beneficiarão de um guia documentado que aborda a estratégia de segurança em nuvem. O plano deve identificar os tipos de cargas de trabalho ou aplicações que são candidatas à computação em nuvem e deve considerar as exigências legais, regulamentares e de segurança. A IBM trabalhará com os clientes para planejar os controles de compensação para atenuar os riscos percebidos, inclusive como abordar o gerenciamento de acesso e identidade e como equilibrar os controles de segurança entre o provedor de serviços de nuvem e o assinante.

Avaliação da segurança em computação em nuvem com a IBM

Além de desenvolver uma estratégia de segurança da nuvem, a IBM pode realizar uma avaliação de segurança para as ofertas de nuvens públicas ou privadas. Esse serviço pode fornecer uma due diligence útil para os provedores de serviços de nuvem ou ajudar os assinantes a compreender a postura de segurança da nuvem de seu provedor.

A avaliação de segurança de computação em nuvem da IBM revisa a arquitetura da solução de um ponto de vista de segurança, incluindo as políticas e processos de acesso e armazenamento de dados. Os especialistas em segurança da IBM avaliam o estado atual da segurança em relação às melhores práticas e aos próprios objetivos de segurança dos provedores. As exigências de segurança e os critérios de melhores práticas são dados com base nas características exclusivas da computação em nuvem de cada um, incluindo a carga de trabalho, nível de confiança dos usuários finais, exigências de proteção de dados e outros. Por exemplo, as nuvens que oferecem suporte a e-mail terão exigências de segurança diferentes das que oferecem suporte a e-mail terão exigências de segurança diferentes das que oferecem suporte a Protected Health Information (ePHI) eletrônicas.

Uma avaliação das lacunas em relação aos objetivos de segurança e melhores práticas revelará os pontos fortes e fracos da arquitetura e dos processos atuais de segurança. Os especialistas da IBM farão recomendações de melhorias e medidas contínuas de segurança para eliminar as lacunas. Essas recomendações podem incluir a utilização de controles adicionais de segurança de rede, modificações nas políticas e procedimentos existentes de segurança, implementação de novos controles de gerenciamento de identidade e acesso, aquisição de serviços gerenciados de segurança para transferir as principais tarefas de gerenciamento de segurança ou qualquer número de outras etapas para solução.

Além de uma revisão completa do programa de segurança em computação em nuvem, a IBM recomenda um teste técnico do estado estável da infraestrutura de rede da nuvem e dos aplicativos de suporte através de penetração remota e testes dos aplicativos. Isso oferece uma visão de “hacker” dos componentes da nuvem e dá idéias sobre como os pontos fracos de segurança podem causar impactos significativos sobre os dados e a proteção das informações.

Por que a IBM?

Para se beneficiarem totalmente da computação em nuvem, os clientes devem garantir que os dados, aplicações e sistemas sejam devidamente protegidos para que a infraestrutura de nuvens não coloquem a organização em risco. A computação em nuvem tem as exigências comuns da segurança tradicional de TI, embora apresente um nível agregado de risco por causa dos aspectos externos de um modelo de nuvem. Isso pode dificultar a manutenção da integridade e privacidade dos dados, o oferecimento de suporte à disponibilidade de dados e serviços e demonstrar conformidade.

Avaliar os riscos associados à computação em nuvem, como a integridade dos dados, recuperação, privacidade e isolamento de locatários é fundamental à adoção de tecnologias de computação em nuvem. Esses riscos pedem uma segurança completamente automatizada com um enfoque maior em forte isolamento, integridade e resistência para oferecer visibilidade, controle e automação em toda a infraestrutura de computação em nuvem.

A IBM ajuda os clientes a implantarem as estratégias de gerenciamento de riscos, transformando a segurança de custos para realização de negócios a uma maneira de melhorar o negócio. A IBM conta com uma ampla carteira de serviços de consultoria, softwares, hardwares e serviços gerenciados de segurança que possibilitam uma abordagem voltada aos negócios para proteger sua computação em nuvem e seus ambientes físicos de TI.

Os recursos IBM possibilitam aos clientes monitorar e quantificar dinamicamente os riscos à segurança, permitindo que eles:

- Compreendam as ameaças e vulnerabilidades em termos de impacto ao negócio,
- Respondam aos eventos de segurança com controles que otimizem os resultados do negócio,
- Priorizem e equilibrem seus investimentos em segurança.

A IBM também opera de modo seguro em suas próprias soluções de computação em nuvem,, incluindo o IBM LotusLive™, e investe continuamente em pesquisa e desenvolvimento de isolamentos mais fortes em todos os níveis da rede, servidor, hipervisor, processo e infraestrutura de armazenamento para oferecer suporte a uma multi-locação massiva, ao mesmo tempo em que atenua os riscos.

Através de soluções líderes que abordam os riscos em todos os aspectos de seu negócio, a IBM ajuda os clientes a criar uma infraestrutura inteligente que reduz os custos, é segura e é tão dinâmica quanto o mundo dos negócios e ambiente comercial atual. As soluções e serviços de segurança de nuvens da IBM contam com a forte base da estrutura de segurança da empresa para estender os benefícios dos ambientes tradicionais de TI aos ambientes de computação em nuvem.

Para mais informações

Para saber mais sobre os Serviços de Segurança de Nuvens da IBM, entre em contato com seu representante de marketing IBM, Parceiro Comercial IBM ou visite: **ibm.com**/cloud

Além disso, as soluções de financiamento do IBM Global Financing permitem um gerenciamento de fundos efetivo, proteção contra obsolescência tecnológica, melhor custo total de propriedade e retorno sobre os investimentos. Nossos Serviços Globais de Recuperação de Ativos ajudam a abordar as preocupações ambientais com soluções novas e mais eficientes em termos energéticos. Para mais informações sobre o IBM Global Financing, visite: **ibm.com**/ibm/academy/índex.html

Route 100
Somers, NY 10589
EUA

Produzido nos Estados Unidos da América
Outubro de 2010

SEW03022-USEN-01