Recomendação de políticas

Serviços de nuvem seguros e confiáveis

A oportunidade

Na medida em que a computação em nuvem dá origem a novas e poderosas capacidades, ela oferece o potencial de aumentar a produtividade, reduzir os custos e gerar novos níveis de inovação, segurança e resiliência. Mas ela também cria novos riscos permitindo novas avenidas de ataque para invasores e introduzindo novas complexidades que vão exigir uma reavaliação das práticas e políticas atuais.

O desafio

Para lidar com os riscos e as ameaças da era da computação em nuvem, os governos terão de se adaptar a programas e políticas de segurança existentes e melhorar as atuais abordagens para garantir a segurança e a resiliência dos seus sistemas. Para isso, novas estruturas que incorporam a tomada ativa de decisões com base nos riscos e alavancam as parcerias público-privadas serão necessárias. Dada a natureza global das ameaças à segurança, as parcerias transfronteiriças e as abordagens jurídicas harmonizadas também serão importantes.

Recomendação de políticas

Os governos reconhecem que os serviços em nuvem oferecem um enorme valor e podem ajudar os setores público e privado a oferecer novos e melhores serviços aos cidadãos e clientes. Como resultado, os governos estão indo além das questões sobre a possibilidade de aplicar abordagens de computação em nuvem e infraestrutura e agora estão focados na criação de marcos regulatórios para garantir que serviços seguros e confiáveis sejam utilizados, principalmente para atividades que envolvem dados sensíveis.

Para atingir esse objetivo, recomendamos o quanto segue:

Estabelecimento de processos de gestão de risco. As políticas de nuvem devem priorizar a avaliação, a gestão e a mitigação de riscos

na prestação de serviços em nuvem para o governo. Os governos devem implementar processos de gestão de riscos em seus ambientes de TI que lhes permitam melhorar o perfil de risco, seja localmente ou na nuvem. Eles também devem se esforçar para distinguir os riscos que são comuns para governos ou departamentos (como controles de acesso lógico) dos riscos únicos (tais como aqueles associados ao acesso a informações pessoais de saúde). Distinguir riscos comuns de únicos ajudará a determinar a forma de gerir certos riscos e quando aplicar as regras internacionais.

Estruturação de um programa de segurança na nuvem desenhado para atingir objetivos balanceados. O estabelecimento de um programa de garantia de nuvem permite aos governos adotar soluções em nuvem seguras para a entrega e a extensão dos serviços. Tais programas devem ser estruturados para equilibrar as metas de segurança com as metas de desempenho e inovação. A estrutura deve ter em conta o papel que as partes interessadas relevantes devem desenvolver, incluindo governos (tanto como regulador e consumidor), prestadores de serviços e terceiros. Ela também deve estabelecer processos para a realização de uma análise inicial das práticas de segurança em comparação com as linhas de base necessárias e para a realização de avaliações contínuas sobre um conjunto menor de práticas e controles.

Estabelecer medidas de segurança de linha de base alinhadas com ou baseadas nas melhores práticas comprovadas. Como os governos abordam o desenvolvimento e a implementação de linhas de base de segurança terá efeitos profundos sobre a segurança e o desenvolvimento econômico. Abordagens inconsistentes e fragmentadas irão redirecionar os recursos limitados de segurança para compliance. Em vez disso, os governos devem utilizar e adaptar as melhores práticas existentes, como o Marco da Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST) para a promoção da segurança e a criação de oportunidades econômicas.

Requisitos de escopo baseados no modelo de entrega de serviços de nuvem. Os modelos de prestação de serviços de nuvem variam significativamente em termos de arquitetura, função e uso. Portanto, é importante que a segurança seja gerida em proporção aos riscos que surgem em diferentes ambientes. Por exemplo, como a segurança de aplicações de software depende muito dos controles de segurança da infraestrutura subjacente na qual eles são construídos, os requisitos de segurança devem ter como alvo o sistema de infraestrutura diretamente em vez de focar exclusivamente na aplicação.

Preservar e apoiar o intercâmbio voluntária de informação. Muitos governos estão focados no aumento das ameaças virtuais aos seus ambientes de tecnologia e serviços de infraestrutura críticos que funcionam em seus países. Alguns desenvolveram sistemas de notificação obrigatória de incidentes que requerem que a indústria informe os reguladores em caso de incidentes graves. Os governos devem preservar e apoiar as comunidades de intercâmbio de informações existentes que operam com base na confiança mútua. Como a troca de informações é mais eficaz quando é bidirecional, os governos também devem compartilhar informações desenvolvidas através da análise estratégica da divulgação de informações sobre o incidente para ajudar as empresas do setor privado a enfrentar novas ameaças.

Implementar um sistema de classificação de dados para a nuvem. A classificação de dados é o processo de divisão de dados em categorias distintas com base em níveis de sensibilidade e perfis de risco e na articulação dos controles de segurança necessários para que cada nível possa gerenciar os riscos de forma adequada. Um sistema de classificação de dados específicos de nuvem ajudará as empresas e agências governamentais a identificar os seus materiais mais e menos sensíveis e avaliar os custos e benefícios de armazenar diferentes níveis de materiais sensíveis na nuvem. Na medida do possível, os governos podem adaptar esquemas de classificação de dados existentes aos dados armazenados na nuvem.

Tirando proveito das regras globais. Considerando que os governos em todo o mundo têm muitos riscos em comum e que a computação em nuvem utiliza agregação e escala para reduzir os custos e melhorar o desempenho, ao usarem as regras globais como base de suas certificações de segurança na nuvem, os governos podem melhorar a eficiência, reduzir os custos e melhorar a concorrência no mercado. As linhas de base devem ser suficientemente abrangentes para minimizar a necessidade das organizações de adicionar seus próprios controles, mas não tão amplas que abranjam controles únicos que não são amplamente utilizados.

Desenvolvimento de um modelo de cumprimento com regras de segurança comum para TIC. Posto que todos os setores da economia dependem da tecnologia digital, existe um alto grau de analogia nos riscos e controles em todos os setores, mas há também alguns riscos que são únicos para cada um. Para os riscos comuns, os governos devem desenvolver um modelo de segurança que defina metas e normas mínimas de segurança para os setores regulados, mas que também permita que aqueles setores estabeleçam um subconjunto menor de requisitos adicionais apropriados para seus ambientes operacionais únicos.