Necessidades de Segurança

Aspectos de segurança

Não deve ser difícil compreender a importância que a segurança tem no que diz respeito aos serviços na nuvem. Imagine, no exemplo citado da Mercedes-Benz, que guarda as informações de toda a sua área de pesquisa e desenvolvimento em servidores localizados em algum lugar do planeta onde ela não detém ingerência direta sobre a segurança. Qual o valor dos segredos envolvidos com essa área e, consequentemente o valor das informações ali mantidas? Ou as pesquisas de ponta de alguém laboratório farmacêutico? Ou imagine também quanto Netflix ou Home Depot, exemplos também citados, perderiam em valor se os seus serviços parassem de funcionar por algumas horas.

A nuvem mudou o paradigma com o qual as organizações controlam seus dados, que, em grande parte, migrou do que é conhecido como on-premises, ou seja, no local, para algo distribuído por vários cantos do globo, no caso de modelos de negócios baseados em operações também dispersas por muitas áreas geográficas do planeta.

Manter estruturas de data center, com servidores, storages (armazenadores), equipamentos de rede e outros de camada de aplicação demanda vultosos investimentos, e a terceirização dos serviços para empresas especializadas que cobram apenas pela parcela utilizada otimizou muito esses custos. O custo da área física para colocação dos equipamentos e o gasto de energia, infraestrutura para conectividade, também fazem parte dessa conta e servem como um reforço para a mudança de abordagem.

A área de computação, observada de forma ampla, conta com uma subárea bastante importante que se preocupa com a manutenção de princípios associados à informação, como confidencialidade, integridade e disponibilidade.

No ramo geral da Tecnologia da Informação, essa área é conhecida como **segurança da informação**, e especificamente no ramo dos serviços de computação em nuvem existe uma subárea do conhecimento conhecida como **cloud security** (“segurança da nuvem”), encontrada também na literatura em português como **nuvem segura**.

Os mesmos princípios gerais que norteiam a segurança da informação precisam ser adotados pelos provedores de serviço em nuvem com as devidas adaptações associadas ao contexto e ao ambiente no qual as informações são guardadas e transmitidas não apenas da origem para o destino, mas também por todos os equipamentos incluídos no caminho entre eles e que estejam sob controle do provedor do serviço.

Atenção!

Independentemente do modelo de serviço implantado, a nuvem pode ser de propriedade, gerenciada e operada pela organização cliente, por terceiros ou por alguma combinação deles, e pode existir dentro ou fora das instalações da organização do cliente. Além disso, o cliente consumidor do serviço pode ter um nível de controle sobre a configuração do serviço em si bastante baixa, dependendo do modelo de serviço contratado.

O tema segurança também sofreu adaptações em termos de emprego de mecanismos a partir do novo paradigma da computação em nuvem. Vejamos alguns **aspectos comparativos** entre o modelo tradicional de data centers on-premise e os ambientes em nuvem mais atuais.

Gestão de vulnerabilidades

Neste vídeo, serão apresentados os aspectos específicos da gestão de vulnerabilidades.

Segurança física

No modelo on-premise o responsável pela segurança física era a própria organização, mas, pelo novo paradigma, fica a cargo do provedor do serviço em nuvem. Uma vez que os equipamentos estejam hospedados nas dependências do provedor, o controle de acesso físico às respectivas áreas é de responsabilidade exclusiva do provedor do serviço.

Onde está localizado o dado

No modelo on-premise a organização tinha total controle sobre esse quesito, já que abrigava todos os equipamentos dentro de suas próprias instalações. No

extremo oposto do novo paradigma, o dado pode estar em qualquer lugar do planeta onde o provedor de serviços em nuvem tenha equipamentos e mantenha suas operações. Dependendo do modelo de implantação, pode existir algum nível de decisão e controle sobre a localização dos dados que esteja sob responsabilidade da organização cliente.

Gestão das vulnerabilidades

O paradigma atual da computação em nuvem tirou a responsabilidade pelo gerenciamento de atualizações de patches dos sistemas envolvidos da mão da organização cliente. De maneira geral, essa gestão passou a ser um encargo do provedor de serviço em nuvem, podendo ser compartilhado com a organização dependendo do modelo de serviço adotado.

Resposta a incidentes

Mais uma responsabilidade que se modificou a partir do novo paradigma. Nos data centers on-premise, todo o encargo de ações referentes a uma resposta a incidente ficava delegado à própria organização que cuidava dos equipamentos e dados abrigados em local de sua inteira responsabilidade. Já pelo novo paradigma dos serviços em nuvem, essa responsabilidade passou a ser compartilhada entre provedor de serviço e organização cliente, cabendo a cada um atuar dentro de uma esfera de ações.

Cumprimento de regulações normativas e legais

A respeito desse aspecto, a abordagem segue a do item anterior, cabendo tanto ao provedor de serviço em nuvem como à organização cliente tomar medidas que suportem as questões legais e normativas vigentes, dependendo dos territórios e jurisdições as quais estejam submetidos.

Muitas organizações, devido à natureza sensível dos dados com os quais têm de lidar, não estão dispostas a migrar para um modelo de implantação tipo "nuvem pública". Por motivos gerais de segurança – porque os servidores físicos estão localizados fora do seu controle direto e, às vezes, até mesmo geograficamente fora de uma jurisdição para a qual tenham um nível adequado de compreensão –, aquelas organizações adotam modelos de implantação com níveis de controle mais enquadrados sob sua própria responsabilidade.

O fato é que a responsabilidade pelos aspectos de segurança não é tratada de forma estritamente binária, estando totalmente a cargo do provedor de serviço ou sob a organização cliente, como era no caso de um data center on-premise.

O modelo de negócios trazido pelo aumento de escala do novo paradigma fez com que os grandes provedores de serviço de nuvem investissem muito

dinheiro na proteção de seus data centers, construindo serviços cada vez mais seguros, especializando mais seus funcionários e identificando incidentes de segurança e corrigindo-os mais rapidamente.

Pela escala alcançada com o novo modelo de negócio dá para arriscar dizer que os provedores de serviço em nuvem despendem mais atenção e investimento em segurança que a grande maioria das organizações seria capaz de fazer em observância a seus data centers locais. A razão para os vultosos investimentos dos grandes provedores é simples: manutenção do nível de confiança no serviço em padrão elevado.

Reflexão

Imagine o estrago que uma violação de segurança poderia provocar à imagem de um provedor de serviços em nuvem. A confiança de seus clientes poderia ser abalada a ponto de tal provedor ficar sem negócios.

Contudo, o retorno dos investimentos empregados em segurança pelos provedores de serviço em nuvem faz sentido uma vez que eles empregam seus métodos de forma padronizada com ganho de escala, alcançando de maneira eficiente objetivos como diminuição da superfície de ataque e conformidade com as regulamentações em amplitude global, a partir da padronização de boas práticas com o uso de ferramentas automatizadas.

Modelo de Responsabilidade Compartilhada

Cumprimento de regulações normativas e legais

A responsabilidade pela segurança não é uma variável binária, estando sob cuidados exclusivos da organização cliente ou do provedor de serviço em nuvem. Dependendo do modelo de serviço contratado, parte dessa responsabilidade pode ser passada para uma ou outra ponta. Existe uma associação óbvia com o preço pago por cada tipo de serviço, mas podemos explicar, de forma mais ampla, o funcionamento dessa divisão de encargos por meio de algo que é conhecido como **modelo de responsabilidade compartilhada**.

A partir dos três modelos de serviço, **IaaS**, **PaaS** e **SaaS**, podemos traçar uma linha divisória no ponto focal da responsabilidade, delegando a cada polo do contrato de serviço maior ou menor responsabilidade sobre os segmentos em

particular. Um modelo de responsabilidade compartilhada é uma estrutura de segurança em nuvem que determina as obrigações de segurança de um provedor de computação em nuvem e suas organizações clientes, para garantir a responsabilidade de cada um.

Atenção!

Quando falamos em organização cliente, devemos pensar até mesmo em um usuário comum, pessoa física, cliente que contrate uma máquina virtual para rodar algum tipo de aplicação específica na nuvem. Porém, para efeito didático, chamaremos simplesmente de cliente o polo contratante do serviço e provedor o polo contratado.

Também para efeito didático, iremos calcar a explicação do conceito de responsabilidade compartilhada no modelo de implantação "nuvem pública", pois é o modelo mais extremo de delegação de responsabilidade ao provedor do serviço em nuvem. A ideia é explicar como as responsabilidades são distribuídas dependendo do provedor e do modelo de serviço específico com base na implantação tipo "nuvem pública". Alguns exemplos de provedores serão apresentados com foco mais intenso nos três principais já mencionados: AWS, Azure e GCP. De forma geral, o tipo de modelo de serviço em nuvem determina quem é responsável por quais atividades relacionadas à segurança.

De acordo com o Cloud Standards Customer Council, um famoso grupo de advocacia dedicado a acelerar a adoção de computação em nuvem e defender usuários da nuvem em esfera judicial, as responsabilidades dos usuários geralmente aumentam à medida que passam de SaaS para PaaS e IaaS.

A Cloud Security Alliance (CSA) é uma organização sem fins lucrativos cuja missão é “promover o uso das melhores práticas para fornecer garantia de segurança na computação em nuvem e educação sobre os usos da computação em nuvem para ajudar a proteger todas as outras formas de computação”. A CSA também enxerga, de maneira geral, que responsabilidade sobre a segurança pende mais para o lado do cliente no modelo IaaS, como a situação oposta no modelo SaaS e o modelo PaaS ocupando o meio do caminho.

Grau de responsabilidade sobre a segurança de acordo com o modelo de serviço.

De forma geral, e com base em exemplos práticos, a distribuição de responsabilidades ante o modelo de serviço pode ser explicada da seguinte maneira:

SaaS

O provedor é responsável por quase todos os aspectos da segurança, desde a infraestrutura subjacente ao sistema aplicativo que suporta o negócio do cliente – por exemplo, uma ferramenta de ERP ou CRM – até os dados que o aplicativo produz. Ficam delegadas ao cliente algumas responsabilidades de segurança, como proteger as credenciais de login contra os ataques de phishing ou engenharia social. Serviços como Dropbox, Zoom, Microsoft 365 e Google Workspace são exemplos do tipo software como serviço e facilitam a compreensão do papel extremo que o provedor dos serviços tem, inclusive com os dados produzidos pelos softwares e armazenados na infraestrutura associada ao serviço.

PaaS

O provedor, oferecendo a plataforma como serviço, assume, em geral, uma responsabilidade que se estende aos aplicativos e sistemas operacionais da plataforma. Mas cabe ao usuário a responsabilidade pela segurança de qualquer código, dado ou outro conteúdo produzido na plataforma. Como exemplos dessa modalidade podemos citar serviços como Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine e Red Hat OpenShift, que cuidam de todas as camadas abaixo da virtualização, porém

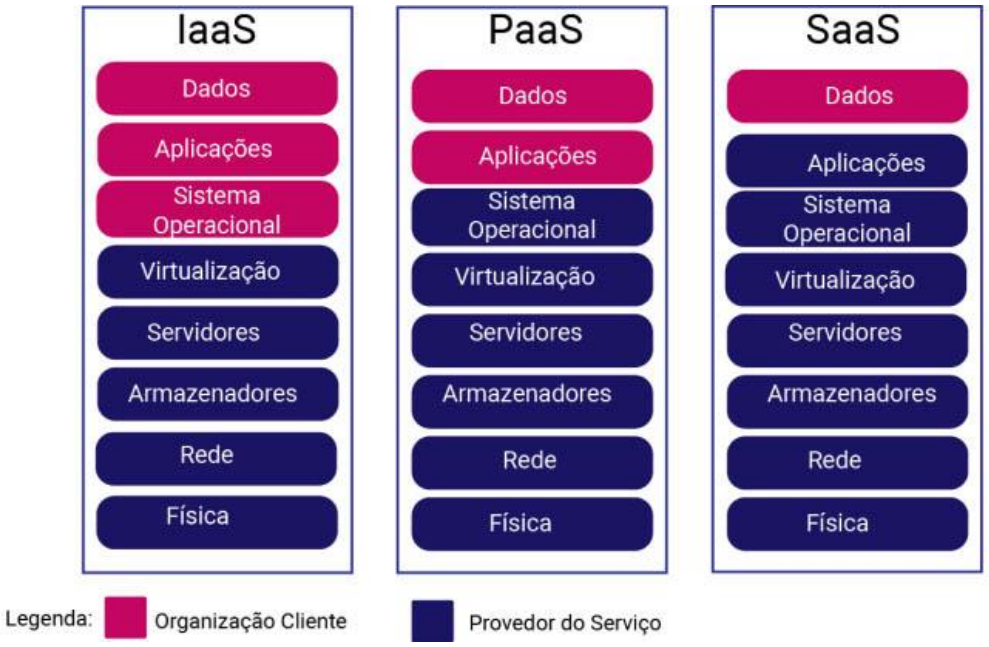
não se preocupam com a segurança do que é executado nas máquinas virtuais.

IaaS

O provedor de nuvem é responsável pelos serviços e armazenamento, que inclui os componentes básicos da infraestrutura de nuvem, como camada de virtualização, discos e redes. O provedor também é responsável pela segurança física dos data centers que abrigam sua infraestrutura. Os usuários de IaaS, no entanto, se responsabilizam geralmente pela segurança do sistema operacional e de toda a pilha de software necessária para executar seus aplicativos, bem como seus dados. Exemplos de serviços que podem ser citados são aqueles que servem como base para os de maior abstração: Microsoft Azure, Amazon Web Service e Google Compute Engine, ou seja, os equipamentos mais básicos, servidores e armazenadores, e os motores que garantem seu funcionamento correto.

Embora a computação em nuvem seja uma tecnologia bem-estabelecida, o conceito de responsabilidade compartilhada pode parecer confuso porque não existe um consenso de mercado para sua aplicação. De qualquer maneira, o conceito traz benefícios para modelar as linhas de demarcação de responsabilidade de segurança sob encargo de cada parte no contrato do serviço.

Para explicar o emprego geral, tomaremos como base uma pilha de elementos organizados em camadas. Considerando os três modelos de serviço e a visão sistêmica oferecida pela pilha de elementos constituintes de um serviço em nuvem, apresentamos, na imagem a seguir, a segmentação das responsabilidades com cortes em diferentes fronteiras entre camadas, caracterizando a segmentação de responsabilidades entre cliente e provedor de acordo com o modelo de serviço contratado.



Grau de responsabilidade sobre a segurança de acordo com o modelo de serviço.

Exemplificando em termos práticos, ao trabalhar com IaaS, o cliente pode selecionar uma imagem pré-instalada de um sistema operacional (com ou sem software adicional instalado dentro da imagem), implantar seus aplicativos e gerenciar permissões para acesso seus dados, sendo responsável pela segurança de todas as camadas acima do sistema operacional.

Ao trabalhar com PaaS, os clientes podem ter a capacidade de controlar o código em um ambiente gerenciado (serviços como AWS Elastic Beanstalk, Azure Web Apps e Google App Engine) e gerenciar permissões para acessar nossos dados, assumindo responsabilidade pela segurança apenas das próprias aplicações e de seus dados.

Ao trabalhar com SaaS, o cliente recebe um serviço totalmente gerenciado, e tudo o que deve fazer é gerenciar permissões para acessar seus próprios dados.