Computação em Nuvem

Segurança e privacidade em nuvem

Você sabia que seu material didático é interativo e multimídia? Isso significa que você pode interagir com o conteúdo de diversas formas, a qualquer hora e lugar. Na versão impressa, porém, alguns conteúdos interativos ficam desabilitados. Por essa razão, fique atento: sempre que possível, opte pela versão digital. Bons estudos!

O objetivo desta webaula é apresentar os fundamentos da segurança em Computação em Nuvem. Então, vamos aprender as principais propriedades que caracterizam, de forma geral, um sistema computacional seguro. Depois, vamos explicar as ameaças e as vulnerabilidades para aplicações em ambientes de nuvem, além de alguns dos mecanismos que podem ser usados para melhorar a segurança das soluções. Esses assuntos são de extrema relevância, principalmente para aplicações críticas ou para aquelas que envolvem dados sigilosos.

Comunicação segura e confiável

Embora a Computação em Nuvem possa trazer vários benefícios, existem alguns desafios na adoção de soluções. Você conhece as principais dificuldades apontadas pelas empresas em relação ao uso de serviços em provedores de nuvem pública? Entre essas dificuldades, pode-se destacar as questões de segurança e privacidade, de acordo com um estudo realizado em 2018 (TUCKER, 2019). Isso acontece porque o acesso às aplicações nos provedores é feito por meio da Internet. Assim, existe uma maior exposição dos dados e serviços em comparação ao cenário no qual uma empresa mantém sua própria infraestrutura de TI, com a comunicação entre os componentes realizada através de uma rede local. Dessa forma, a maior exposição dos dados na internet, no modelo de Computação em Nuvem, aumenta as chances de ataques que buscam violar a segurança das aplicações.

Portanto, esse tipo de projeto exige muito cuidado com aspectos da segurança dos serviços e da privacidade dos dados. São imprescindíveis o uso de mecanismos de segurança e o estabelecimento de uma estratégia de gerenciamento de riscos.

Antes de conhecer as principais vulnerabilidades de aplicações em nuvem e os principais mecanismos de segurança, precisamos compreender os princípios de segurança da informação e quais são as propriedades de um sistema seguro. Conforme apresentado na literatura (KUROSE; ROSS, 2013; TANENBAUM; STEEN, 2008), as propriedades básicas de uma comunicação segura e confiável são as elencadas a seguir.

Confidencialidade

Sigilo do conteúdo dos pacotes transmitidos na rede.

Integridade

Garantia de que os dados transmitidos não podem ser alterados.

Autenticidade

Confirmação da identidade das partes envolvidas na transmissão dos dados.

Disponibilidade

Garantia de que um sistema estará apto para realizar as operações de transmissão ou processamento dos dados.

Ameaças e vulnerabilidades

Conforme explicado em (ERL; PUTTINI; MAHMOOD, 2013), as principais ameaças de segurança para aplicações em nuvem são: interceptação de tráfego, negação de serviço e ataques de virtualização. Saiba mais a seguir.

Interceptação de tráfego

Ocorre quando uma entidade não autorizada é capaz de obter as informações transmitidas entre provedor em nuvem e clientes, de forma que a confidencialidade dos dados é violada (ERL; PUTTINI; MAHMOOD, 2013).

Negação de serviço

Tem o objetivo de afetar a disponibilidade dos serviços. Esse ataque consiste em sobrecarregar o serviço com um grande volume de requisições de forma que não consiga mais responder aos clientes legítimos com um desempenho satisfatório (ERL; PUTTINI; MAHMOOD, 2013).

Ataques de virtualização

Buscam explorar eventuais falhas e vulnerabilidades nas ferramentas de virtualização utilizadas pelos provedores (ERL; PUTTINI; MAHMOOD, 2013). Nesse caso, o atacante pode conseguir algum nível de controle sobre a infraestrutura de TI do provedor. Outro problema é que pode haver violação da privacidade dos dados dos clientes do provedor.

Além das ameaças relacionadas com segurança de dados e redes, os provedores de Computação em Nuvem também precisam lidar com ameaças relacionadas a outras categorias de segurança, como governança, conformidade e questões legais (GONZALEZ *et al.*, 2013). Entre os principais problemas nessas categorias podemos citar:

- Baixo nível de controle administrativo sobre a segurança dos dados por parte dos clientes de um provedor.
- Dependência das tecnologias e políticas de segurança adotadas pelo provedor.
- Problemas relacionados aos requisitos de confiabilidade e políticas de auditoria estabelecidos em acordos de qualidade de serviço (SLA).
- Jurisdição dependente da localização dos provedores onde estão armazenados os dados, pois alguns provedores possuem *data centers* em países diferentes.

Mecanismos de segurança

Agora que já conhecemos algumas das principais ameaças para aplicações em nuvem, vamos entender os principais mecanismos de segurança disponíveis.

Criptografia

Consiste em técnicas que permitem disfarçar os dados enviados de forma que um atacante não consiga obter nenhuma informação dos dados interceptados (KUROSE; ROSS, 2013). Isso implica codificar os dados de modo que somente o destinatário legítimo poderá decifrá-los, tornando-os, assim, ininteligíveis para terceiros. A principal aplicação da criptografia é assegurar a confidencialidade dos dados armazenados nos provedores de nuvem pública e dos dados transmitidos entre um provedor e seus clientes. Além disso, a criptografia também pode ser usada em mecanismos para garantia de integridade e autenticidade. Uma vez que a criptografia pode ser usada na implementação de diversos mecanismos, ela é considerada um conceito fundamental para segurança de sistemas computacionais.

Gerenciamento de Acesso e Identidade (IAM – *Identity and Access Management*)

É utilizado pelos provedores, principalmente, para implementação de políticas de controle de acesso. O IAM permite o gerenciamento e a autenticação de usuários, assim como o controle de privilégios para grupos de usuários e gerenciamento de credenciais. Esse tipo de recurso é importante na implementação de soluções de segurança para lidar com ataques de negação de serviços, autenticação fraca e violação de privacidade no acesso a dados e serviços. Se um cliente utiliza serviços em vários provedores, então é importante também para questões de controle de acesso o uso de mecanismos de autenticação unificada (SSO – *Single Sign On*). Esses mecanismos oferecem uma solução segura para autenticação em vários provedores utilizando as mesmas credenciais.

Imagens fortalecidas de Máquinas Virtuais de virtualização (*Hardened VM Images*)

É outro recurso bastante utilizado pelos provedores de Computação em Nuvem para aprimorar a segurança dos serviços (ERL; PUTTINI; MAHMOOD, 2013). Sabemos que as instâncias de máquinas virtuais são criadas a partir de imagens disponíveis no provedor. As imagens fortalecidas são aquelas que foram configuradas por especialistas considerando políticas de segurança rigorosas para eliminar possíveis vulnerabilidades. Dessa forma, quando um cliente cria uma VM a partir de uma imagem fortalecida, ele sabe que o sistema operacional dessa VM já foi configurado com as melhores práticas de segurança conhecidas.

Por fim, cabe destacar que os mecanismos de segurança devem ser usados em conjunto e aprimorados continuamente para lidarem com eventuais ações maliciosas contra as aplicações em ambientes de nuvem. É importante ressaltar que a segurança não é reponsabilidade somente do provedor de Computação em Nuvem; o cliente dos serviços também precisa cooperar.

Para visualizar o vídeo, acesse seu material digital.