1.Segurança em nuvem

Com a rápida adoção da computação em nuvem, praticamente todas as organizações passaram a utilizar pelo menos uma aplicação em nuvens públicas. No entanto, junto com essas aplicações, um grande volume de dados sensíveis também está sendo armazenado nesses ambientes, tornando essencial a implementação de boas práticas de segurança. Infelizmente, muitas empresas ainda falham nesse aspecto. Estudos indicam que 76% das organizações não utilizam autenticação multifator para acessar consoles de administração na nuvem, o que expõe esses sistemas a ataques. Além disso, cerca de 63% do código rodando na nuvem permanece sem atualização, muitas vezes com vulnerabilidades graves classificadas com um CVSS (Common Vulnerability Scoring System) acima de 7, em uma escala de 10.

Quando um serviço é hospedado na nuvem pública, ele fica acessível a qualquer usuário na internet, o que facilita sua utilização, mas também aumenta o risco de ataques. Um invasor pode, por exemplo, realizar um ataque de **negação de serviço (DoS ou DDoS)** para desativar uma aplicação ou explorar falhas de autenticação para obter acesso indevido a dados sensíveis. Caso o sistema não esteja configurado corretamente ou utilize processos de autenticação fracos, qualquer pessoa pode tentar acessá-lo, comprometendo sua segurança.

Um erro comum em servidores web mal configurados é a permissão indevida de *traversal de diretórios*, que permite a um atacante navegar por estruturas internas do servidor. Além disso, vulnerabilidades não corrigidas podem permitir a execução remota de código, possibilitando que um invasor rode programas maliciosos no sistema em nuvem. Casos como as falhas descobertas no **Log4j** e no **Spring Cloud Function** ilustram como uma aplicação desatualizada pode se tornar um alvo fácil para ataques. Essas vulnerabilidades eram simples de explorar e davam controle total sobre os sistemas afetados.

Outro problema frequente é a falta de validação de entrada nos campos de formulários das aplicações, o que permite ataques como **cross-site scripting (XSS)**. Nesse tipo de ataque, um invasor injeta código malicioso em um site legítimo, comprometendo a segurança dos usuários. Outra ameaça similar é a **escrita fora dos limites de memória (out-of-bounds write)**, onde um invasor escreve dados em áreas não autorizadas da memória, podendo executar código malicioso ou causar falhas no sistema.

Além disso, como os dados armazenados na nuvem são um dos principais alvos dos atacantes, técnicas como **injeção de SQL** podem ser usadas para explorar falhas em bancos de dados, permitindo a extração de informações sigilosas. Para evitar esses riscos, é essencial que empresas adotem boas práticas de segurança, como aplicação de patches de segurança regularmente, implementação de autenticação multifator e configurações adequadas para restringir acessos indevidos. A proteção da

infraestrutura em nuvem exige uma abordagem contínua e proativa para minimizar vulnerabilidades e manter a integridade dos dados armazenados.