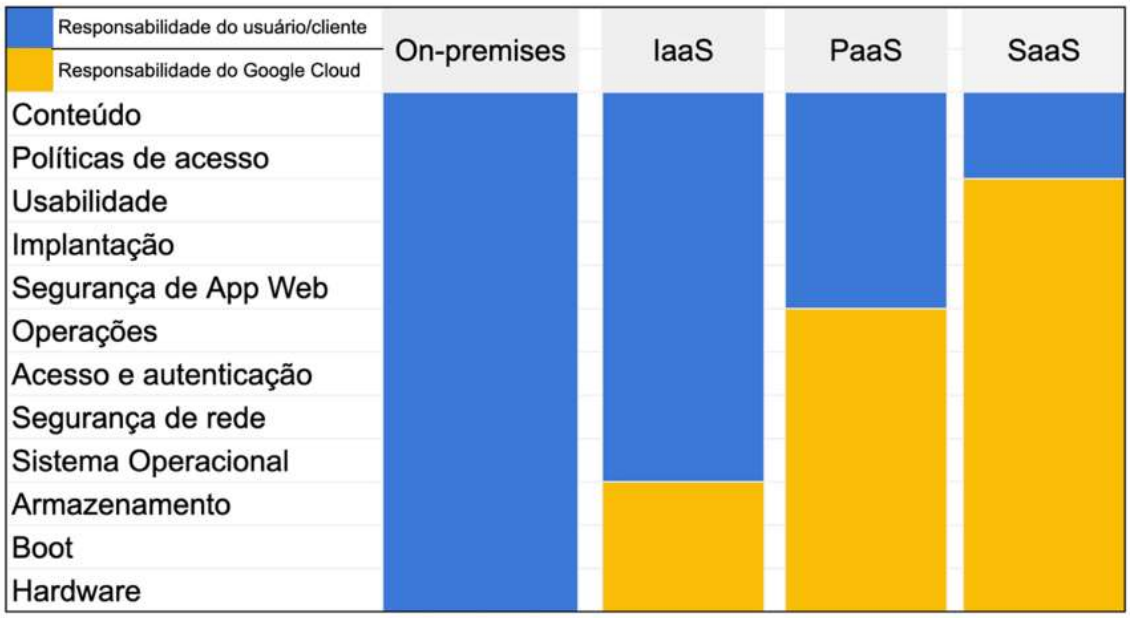
SEGURANÇA E OPERAÇÕES NO GOOGLE CLOUD

Segurança em Google Cloud

O Google Cloud, por mais que seja um provedor de serviços gerenciados, necessita estar alinhado com boas práticas de segurança. Dentro de uma matriz de responsabilidades, em um provedor, existem diferentes níveis para cada tipo de serviço, e cada parte terá sua responsabilidade pela segurança. A imagem a seguir nos mostra essa matriz:



Matriz de responsabilidades de segurança.

Como vemos na imagem, quanto mais gerenciado for o serviço, menor a responsabilidade do usuário com a segurança. Assim, ao utilizar uma infraestrutura como serviço (IaaS), por exemplo, toda a responsabilidade de segurança com hardware e boot é do provedor. Por outro lado, a segurança da aplicação, da implantação dessa aplicação, sistema operacional e rede é totalmente do usuário. Caso utilize uma plataforma como serviço (PaaS), a responsabilidade passa a ser somente em nível de aplicação.

Em um provedor de nuvem, é importante estarmos atentos às normas nas quais ele está adequado. As normas regulamentadoras servem para assegurar um serviço prestado, e podem ser internacionais ou nacionais.

No Brasil, por exemplo, temos a Lei Geral de Proteção de Dados, também conhecida como LGPD, que visa normatizar a utilização e processamento de dados de maneira correta, impondo regras na transferência e circulação de dados pessoais.

Outra norma muito comum é a ISO/IEC 27001, na qual a Organização Internacional de Normatização (ISO) descreve os requisitos de um sistema de gestão de segurança e especifica um conjunto de práticas recomendadas, mostrando detalhes sobre os controles exigidos. O Google Cloud está adequado a essas e inúmeras outras normas, com servidores certificados.

ISO 27001: referência internacional para gestão da segurança da informação.

Toda infraestrutura física do Google Cloud, em todos os servidores, tem um protocolo de segurança extremamente rígido. Para acesso aos datacenters, por exemplo, existem seis camadas de segurança, desde a autorização para entrar no local, passando por câmeras de detecção térmica, segurança 24h, sistemas de alarme, até chegar no acesso ao piso de servidores. Um fato interessante é que apenas funcionários autorizados possuem acesso aos datacenters, e esses funcionários representam menos de 1% do total de funcionários do Google.

Segurança na nuvem

A computação em nuvem trouxe grandes facilidades e agilidade para a inovação. Da mesma maneira, com as ofertas como serviço, tirou do usuário grande parte da responsabilidade de segurança. Mesmo assim, ainda é necessário adotar medidas para garantir a seguridade das aplicações, dados e infraestrutura.

Ameaças

A grande realidade é que, atualmente, existem incontáveis tipos de ameaças, e isso é uma grande preocupação e ponto de atenção para todas as empresas. Qualquer tipo de ataque, seja para sequestros de dados ou para gerar indisponibilidade, impacta diretamente, desestabilizando o negócio.

Segurança na nuvem

Devido a todas essas preocupações, surgiu um termo chamado de “segurança na nuvem” (cloud security), que se refere às melhores práticas de gerenciamento de segurança na nuvem, incluindo tecnologias, políticas, controles e serviços, que mantém dados, aplicativos e infraestrutura sob a maior proteção possível contra ameaças externas e internas.

A segurança na nuvem está muito relacionada a tecnologias e processos que podem ser utilizados, como: gestão de acesso e identidade, segurança contra ataques, lista de bloqueio. Vamos ver como funcionam?

Gestão de acesso e identidade

Também conhecido como IAM (identity and access management), é um processo que visa controlar o acesso às informações, recursos e ações do ambiente. O Google Cloud oferece sua solução de IAM integrada à plataforma e, com isso, é possível gerir todos os usuários e seu nível de acesso.

Exemplo

Se um usuário tem acesso de desenvolvedor, estará autorizado a somente visualizar ou talvez editar configurações relacionadas à sua alçada, não podendo visualizar, utilizar ou configurar nada de infraestrutura, tecnologias ou aplicações que não são de sua responsabilidade.

O login pode ser combinado com mais uma camada de segurança, com múltiplos fatores de autenticação, ou seja, além do padrão usuário e senha, é necessário mais um fator para comprovar a identidade do usuário como, por exemplo, um SMS no telefone celular, ou um token físico como um pen drive.

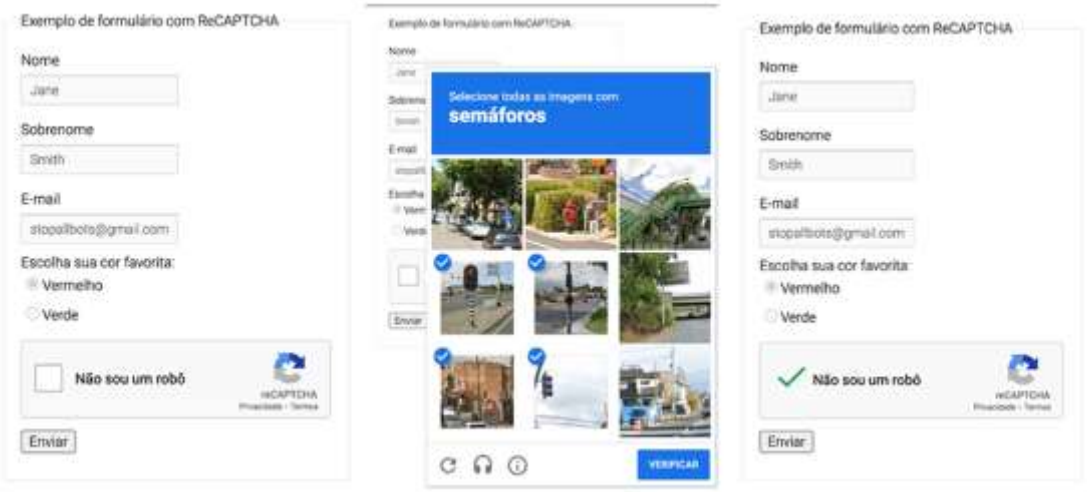
Com esse nível de gestão, utilizando políticas e limites de acesso, evita-se qualquer possibilidade de alguém não autorizado utilizar algo. Ou até mesmo, caso alguma credencial seja roubada, as limitações de acessos dão maior segurança.

Segurança contra ataques

Empresas vêm regularmente sofrendo ataques e, para se proteger contra isso, é necessário uma boa estratégia e ferramentas. O Google Cloud possui uma oferta chamada de Cloud Armor, que consiste em uma tecnologia que utiliza inteligência artificial e aprendizado de máquinas para mitigar ataques contra aplicações e servidores dos clientes.

Por meio de inúmeros dados processados pelo Google, o Cloud Armor consegue entender quando um comportamento é uma ameaça e evitá-lo. Por exemplo, um ataque de negação de serviço distribuída (DDoS), que ocorre por meio de um grande volume de requisições falsas para o serviço, gerando indisponibilidade.

Outra tecnologia que é muito utilizada para segurança contra ataques às aplicações é o reCAPTCHA, uma tecnologia do Google que permite distinguir entre um acesso humano ou automatizado por meio do uso de identificações visuais ou auditivas. Isso é importante pois, a cada dia, cresce o número de bots maliciosos, que visam buscar brechas em sistemas.



Exemplos de reCAPTCHA.

Lista de bloqueio

Outra estratégia muito utilizada é a de lista de bloqueios (blocklist) e lista de permitidos (allowlist). Seu objetivo é ter uma lista de bloqueios ou permissões de acessos ao sistema, e isso pode ser baseado em IPs ou regiões.

Essa estratégia é muito útil para podermos negar o acesso de IPs externos da nossa rede, por exemplo, a uma aplicação. Outra possibilidade é a de bloquear todo acesso que venha de outro país, o que mitiga ataques em massa que utilizam servidores, bots e computadores do mundo todo para atingir nossos ambientes.

Segurança nas aplicações

Como vimos, em ambientes de nuvem utilizando soluções como serviço IaaS ou PaaS, a camada de aplicação é responsabilidade do usuário e, por isso, devemos tomar todas as medidas de segurança possíveis.

Um consenso básico de segurança das aplicações é sempre manter as versões de linguagens de programações e frameworks de código livre (open source) atualizados para a versão estável, o que não significa necessariamente que essa seja a última disponível. Sempre que uma nova versão de algo é lançada, normalmente ela não é estável, pois ainda não teve o período de amadurecimento e, devido a isso, pode possuir brechas de segurança que ainda não foram descobertas.

Outro conceito bem maduro e útil é o DevOps, que é um processo de entrega de software que envolve desenvolvimento e operações juntos. Esses dois times possuem visões diferentes. Enquanto desenvolvedores se preocupam com regras de negócio, linguagens de programação e construir a aplicação, os operadores estão visando à performance, segurança geral e monitoramento do ambiente e, assim, o desempenho de entrega de softwares acaba tornando complexo todo o processo.

Por isso, a teoria do DevOps busca envolver ambos os lados e compartilhar a responsabilidade utilizando, para isso, tecnologia para um desenvolvimento em ciclos. Essa técnica agrega a segurança da aplicação, pois cada persona se preocupa com a segurança de sua especialidade. Desse modo, o desenvolvedor não precisa se preocupar com as configurações de infraestrutura dentro da aplicação, pois as tecnologias padronizam os ambientes. Todo processo de entrega de novas versões de software acaba se tornando mais seguro e documentado, pois existe uma prática por trás, e isso torna-se mais nítido para os envolvidos.

DevOps: utilização de tecnologia para desenvolvimento em ciclos.

Todas essas práticas são recomendadas e adotadas pelo Google Cloud, que também fornece ferramentas e tecnologias para sua execução, como: Cloud Repository, um versionador de códigos fontes GIT; o Cloud Build, um integrador e construtor de aplicações com base em códigos-fontes, que têm como função automatizar todo o processo; e Cloud Deploy, ferramenta de entrega de aplicações em ambientes finais (produtivos) em nuvem.

Operações em Google Cloud

As operações em nuvem consistem no processo de operar ou executar uma infraestrutura em ambiente de nuvem. Isso tudo é complementado com o gerenciamento geral para garantir e assegurar que todos os processos e recursos estejam normatizados, a fim de manter essas operações funcionando, garantindo o máximo desempenho e a disponibilidade para satisfazer as necessidades e expectativas dos clientes.

Uma das principais responsabilidades de operações é o monitoramento e, para que isso seja feito, é necessário identificar as métricas que devem ser analisadas e as tecnologias que podem ser utilizadas.

O monitoramento mais básico possível ocorre por meio de LOGS que, por definição, consistem no registro de eventos relevantes no sistema ou infraestrutura, de maneira geral. Ou seja, é todo o histórico de acontecimentos importantes, com data e hora registrada. Com o uso dos LOGS, é possível

identificar erros, acessos e alterações realizadas, para que, a partir dessas informações, seja possível fazer um trabalho preventivo e corretivo, quando necessário.

Cloud Monitoring: monitoramento de aplicativos e da infraestrutura.

O Google Cloud disponibiliza ferramentas do **Cloud Monitoring** para monitoramento de aplicações e infraestrutura de maneira mais minuciosa, coletando um grande volume de dados para disponibilização, pois o monitoramento de um ambiente é um dos papéis mais importantes em nuvem.

Por meio dessa ferramenta é possível traçar estratégias para melhoria contínua, tomar uma ação preventiva para evitar qualquer problema ou empecilho que possa prejudicar a operação do sistema e, caso ocorra, identificar a falha por meio do registro histórico e agir o mais rápido possível.

O Cloud Monitoring permite coletar dados e métricas de latência, por exemplo, o que nos indicará qual o tempo médio de transações e comunicação entre servidores. Indica também a quantidade de acessos e requisições em nossas aplicações, para que possamos entender e programar a infraestrutura para o volume que está sendo monitorado.

Saiba mais

O Google acredita que a prevenção é sempre mais vantajosa que a remediação. Qualquer problema impacta diretamente o negócio, receita e claramente o time. Estar constantemente analisando as métricas de operações previne esse tipo de problema e auxilia na hora de tomar uma decisão final, que será embasada em dados reais.