Microsoft Azure

Cinco práticas recomendadas para a segurança na nuvem

A segurança na nuvem é um cenário fundamentalmente novo para muitas empresas. Embora muitos dos princípios de segurança permaneçam os mesmos que na infraestrutura local, a implementação é muitas vezes muito diferente. Esta visão geral fornece um instantâneo das cinco práticas recomendadas para segurança na nuvem: controle de identidade e acesso, gerenciamento de postura de segurança, aplicativos e segurança de dados, proteção contra ameaças e segurança de rede.

01 Reforçar o controle de acesso

As práticas de segurança tradicionais não são suficientes para se defender contra os ataques de segurança modernos. Portanto, a prática de segurança moderna é "suposição de violação": proteger como se o invasor tivesse violado o perímetro da rede. Hoje, os usuários trabalham em muitos locais com vários dispositivos e aplicativos. A única constante é a identidade do usuário, razão pela qual está o novo plano de controle de segurança.

Estabelecer autenticação multifatorial

Forneça outra camada de segurança, exigindo dois ou mais dos seguintes métodos de autenticação:

- Algo que você sabe (normalmente uma senha)
- Algo que você tem (um dispositivo confiável que não seja facilmente duplicado, como um telefone)
- Algo que você é (biometria)

Aproveitar o acesso condicional

Domine o equilíbrio entre segurança e produtividade levando em conta *como* um recurso é acessado em uma decisão de controle de acesso. Implemente decisões automatizadas de controle de acesso para acessar seus aplicativos de nuvem que são baseados em condições.

Operar em um modelo de confiança zero

Verifique a identidade de tudo e qualquer coisa que tente autenticar ou se conectar antes de conceder acesso.

02 Melhorar a postura de segurança

Com mais e mais recomendações e vulnerabilidades de segurança identificadas, é mais difícil fazer a triagem e priorizar a resposta. Certifique-se de que você tem as ferramentas necessárias para avaliar seus ambientes e ativos atuais e identificar possíveis problemas de segurança.

Melhorar sua postura atual

Use uma ferramenta como Secure Score na Central de Segurança do Azure para entender e melhorar sua postura de segurança implementando as práticas recomendadas.

Educar as partes interessadas

Compartilhe o progresso sobre sua classificação de segurança com as partes interessadas para demonstrar o valor que você está fornecendo à organização à medida que melhora a segurança organizacional.

Colaborar com sua equipe de DevOps em políticas

Para sair do modo reativo, você deve trabalhar com suas equipes de DevOps com antecedência para aplicar as principais políticas de segurança no início do ciclo de engenharia como DevOps seguro.

03 Proteger os aplicativos e dados

Proteja dados, aplicativos e infraestrutura por meio de uma estratégia em camadas de defesa profunda em identidade, dados, hosts e redes.

Criptografar

Criptografe dados em repouso e em trânsito. Considere criptografar dados em uso com tecnologias de computação confidenciais.

Seguir as práticas de segurança recomendadas

Certifique-se de que suas dependências de open source não tenham vulnerabilidades. Além disso, treine seus desenvolvedores nas práticas recomendadas de segurança, como Security Development Lifecycle (SDL).

Compartilhar a responsabilidade

Quando uma empresa opera principalmente na infraestrutura local, ela possui toda a pilha e é responsável por sua própria segurança. Dependendo de como você usa a nuvem, suas responsabilidades mudam, com algumas responsabilidades sendo transferidas para o seu provedor de nuvem.

- IaaS: para aplicativos em execução em máquinas virtuais, a pressão é maior sobre o cliente, para garantir a segurança do aplicativo e do sistema operacional.
- PaaS: à medida que você migra para o PaaS nativo de nuvem, provedores de nuvem como a Microsoft assumem mais a responsabilidade de segurança no nível do sistema operacional.
- SaaS: no nível SaaS, a responsabilidade se afasta mais do cliente. Veja o modelo de responsabilidade compartilhada.

04 Reduzir as ameaças

A postura de segurança operacional (proteger, detectar e responder) deve ser informada por uma inteligência de segurança incomparável para identificar ameaças em rápida evolução desde o início, para poder responder rapidamente.

Ativar a detecção para todos os tipos de recursos

Verifique se a detecção de ameaças está ativada para máquinas virtuais, bancos de dados, armazenamento e IoT. A Central de Segurança do Azure possui detecção interna de ameaças que oferece suporte a todos os tipos de recursos do Azure.

Integrar inteligência contra ameaças

Use um provedor de nuvem que integre inteligência de ameaças, fornecendo o contexto, a relevância e a priorização necessários para você tomar decisões mais rápidas, melhores e mais proativas.

Modernizar suas informações de segurança e gerenciamento de eventos (SIEM)

Considere um SIEM nativo de nuvem que se adapta às suas necessidades, usa a IA para reduzir o ruído e não requer infraestrutura.

05 Proteger a rede

Estamos em um momento de transformação para a segurança da rede. À medida que o cenário muda, suas soluções de segurança devem enfrentar os desafios do cenário de ameaças em evolução e dificultar a exploração das redes pelos invasores.

Manter uma forte proteção de firewall

A configuração do firewall ainda é importante, mesmo com o gerenciamento de identidade e acesso. Os controles precisam estar em vigor para proteger o perímetro, detectar atividades hostis e criar sua resposta. Um firewall de aplicativo web (WAF) protege aplicativos da web de explorações comuns, como injeção de SQL e scripts entre sites.

Ativar proteção de DDoS (Negação de Serviço Distribuído)

Proteja os ativos e redes da Web do tráfego malicioso, direcionando as camadas de aplicativo e rede, para manter a disponibilidade e a performance, enquanto contém custos operacionais.

Criar uma rede microssegmentada

Uma rede plana facilita a movimentação lateral dos invasores. Familiarize-se com conceitos como rede virtual, provisionamento de sub-rede e endereçamento IP. Use a microssegmentação e adote um conceito totalmente novo de microperímetros para oferecer suporte a redes de confiança zero.

O que vem a seguir

Entre em contato conosco

Você está procurando fortalecer a segurança de seus workloads de nuvem?

Saiba mais sobre segurança no Azure