Práticas recomendadas de Segurança Operacional do Azure

Este artigo fornece um conjunto de práticas recomendadas operacionais para proteger seus dados, aplicativos e outros ativos no Azure.

As recomendações baseiam-se um consenso de opinião, e trabalhar com recursos da plataforma Windows Azure atuais e conjuntos de recursos. As opiniões e tecnologias mudam ao longo do tempo e este artigo é atualizado regularmente para refletir essas alterações.

Definir e implantar práticas fortes de segurança operacional

A segurança operacional do Azure refere-se a serviços, controles e recursos disponíveis aos usuários para proteger seus dados, aplicativos e outros ativos no Azure. A segurança operacional do Azure se baseia em uma estrutura que incorpora o conhecimento adquirido por recursos exclusivos da Microsoft, incluindo o SDL (Security Development Lifecycle), o programa Microsoft Security Response Center e o conhecimento profundo do cenário de ameaças de segurança cibernética.

Gerenciar e monitorar senhas de usuário

A tabela a seguir lista algumas das práticas recomendadas relacionadas ao gerenciamento de senhas de usuário:

Melhor prática: Verifique se você tem o nível apropriado de proteção por senha na nuvem.
Detalhe: Siga as orientações em diretrizes de senha da Microsoft, que tem como escopo os usuários das plataformas de identidade da microsoft (Azure Active Directory, Active Directory e conta Microsoft).

Melhor prática: Monitorar ações suspeitas relacionadas às suas contas de usuário.
Detalhe: Monitore para usuários em risco e entradas arriscadas usando os relatórios de segurança do Azure AD.

Melhor prática: Detectar e corrigir automaticamente as senhas de alto risco.
Detalhe: Azure ad Identity Protection é um recurso da edição Azure ad Premium P2 que permite:

- Detectar possíveis vulnerabilidades que afetam as identidades da sua organização
- Configurar respostas automatizadas para ações suspeitas detectadas que se relacionem com as identidades da sua organização
- Investigue incidentes suspeitos e execute as ações apropriadas para resolvê-los

Receber notificações de incidentes da Microsoft

Certifique-se de que sua equipe de operações de segurança receba notificações de incidentes do Azure da Microsoft. Uma notificação de incidente permite que sua equipe de segurança saiba que você comprometeu os recursos do Azure para que eles possam responder rapidamente e corrigir possíveis riscos de segurança.

No portal de registro do Azure, você pode garantir que as informações de contato do administrador incluem detalhes que notificam as operações de segurança. Informações de contato são um número de telefone e um endereço de email.

Organizar assinaturas do Azure em grupos de gerenciamento

Se a organização tiver muitas assinaturas, talvez seja necessário gerenciar de maneira eficiente o acesso, as políticas e a conformidade dessas assinaturas. Os grupos de gerenciamento do Azure fornecem um nível de escopo acima das assinaturas. Você organiza as assinaturas em contêineres chamados grupos de gerenciamento e aplica suas condições de governança aos grupos de gerenciamento. Todas as assinaturas dentro de um grupo de gerenciamento herdam automaticamente as condições aplicadas ao grupo de gerenciamento.

Você pode criar uma estrutura flexível de grupos de gerenciamento e assinaturas em um diretório. Cada diretório recebe um único grupo de gerenciamento de nível superior chamado grupo de gerenciamento raiz. Esse grupo de gerenciamento raiz é compilado na hierarquia para que todos os grupos de gerenciamento e assinaturas sejam dobrados nele. O grupo de gerenciamento raiz permite que as políticas globais e as atribuições de RBAC sejam aplicadas no nível do diretório.

Aqui estão algumas práticas recomendadas para o uso de grupos de gerenciamento:

Melhor prática: Verifique se as novas assinaturas aplicam elementos de governança como políticas e permissões à medida que são adicionadas.
Detalhe: Use o grupo de gerenciamento raiz para atribuir elementos de segurança de toda a empresa que se aplicam a todos os ativos do Azure. Políticas e permissões são exemplos de elementos.

Melhor prática: Alinhe os principais níveis de grupos de gerenciamento com a estratégia de segmentação para fornecer um ponto de controle e consistência de política dentro de cada segmento.
Detalhe: Crie um único grupo de gerenciamento para cada segmento no grupo de gerenciamento raiz. Não crie nenhum outro grupo de gerenciamento na raiz.

Melhor prática: Limite a profundidade do grupo de gerenciamento para evitar confusão que atrasa as operações e a segurança.
Detalhe: Limite sua hierarquia a três níveis, incluindo a raiz.

Melhor prática: Selecione cuidadosamente quais itens aplicar a toda a empresa com o grupo de gerenciamento raiz.
Detalhe: Verifique se os elementos do grupo de gerenciamento raiz têm uma clara necessidade de serem aplicados em cada recurso e se eles têm baixo impacto.

Os bons candidatos incluem:

- Requisitos regulatórios que têm um impacto comercial claro (por exemplo, restrições relacionadas à soberania de dados)
- Os requisitos com um impacto negativo quase zero potencial em operações, como política com efeito de auditoria ou atribuições de permissão de RBAC que foram revisadas cuidadosamente

Melhor prática: Planeje e teste cuidadosamente todas as alterações em toda a empresa no grupo de gerenciamento raiz antes de aplicá-las (política, modelo de RBAC e assim por diante).
Detalhe: As alterações no grupo de gerenciamento raiz podem afetar todos os recursos no Azure. Embora eles forneçam uma maneira poderosa de garantir a consistência em toda a empresa, os erros ou o uso incorreto podem afetar negativamente as operações de produção. Testar todas as alterações no grupo de gerenciamento raiz em um laboratório de teste ou em um piloto de produção.

Simplifique a criação do ambiente com plantas

O serviço de plantas do Azure permite que os arquitetos de nuvem e os grupos de tecnologia da informação central definam um conjunto repetível de recursos do Azure que implementam e aderem aos padrões, padrões e requisitos de uma organização. As plantas do Azure possibilitam que as equipes de desenvolvimento compilem e criem rapidamente novos ambientes com um conjunto de componentes internos e a confiança de que eles estão criando esses ambientes dentro da conformidade organizacional.

Monitorar serviços de armazenamento quanto a mudanças inesperadas no comportamento

Questões de diagnóstico e de solução de problemas em um aplicativo distribuído hospedado em um ambiente de nuvem podem ser mais complexas que em ambientes tradicionais. Aplicativos podem ser implantados em uma infraestrutura PaaS ou IaaS, local, em um dispositivo móvel ou em alguma combinação desses ambientes. Tráfego de rede do seu aplicativo pode passar por redes públicas e privadas, e seu aplicativo poderá usar várias tecnologias de armazenamento.

Você deve monitorar continuamente os serviços de armazenamento que o aplicativo usa para qualquer mudança inesperada em comportamento (como tempos de resposta mais lentos). Use o log para coletar dados mais detalhados e analisar o problema em profundidade. As informações de diagnósticos que você obtiver tanto do monitoramento quanto do registro em log o ajudarão a determinar a raiz do problema que o seu aplicativo encontrou. Você poderá solucionar o problema e determinar as etapas apropriadas para corrigi-lo.

A Análise de Armazenamento do Azure executa o registro em log e fornece dados de métrica para uma conta de armazenamento do Azure. Recomendamos que você use esses dados para rastrear solicitações, analisar tendências de uso e diagnosticar problemas com sua conta de armazenamento.

Evitar, detectar e reagir a ameaças

A central de segurança do Azure ajuda você a prevenir, detectar e responder a ameaças, fornecendo maior visibilidade sobre (e controlar) a segurança dos recursos do Azure. Ela permite o gerenciamento de políticas e o monitoramento da segurança integrada entre suas assinaturas do Azure, ajuda a detectar ameaças que poderiam passar despercebidas e funciona com um diversas soluções de segurança.

A camada gratuita da central de segurança oferece segurança limitada apenas para os recursos do Azure. A camada Standard estende esses recursos para locais e outras nuvens. A central de segurança Standard ajuda a localizar e corrigir vulnerabilidades de segurança, aplicar controles de acesso e de aplicativo para bloquear atividades mal-intencionadas, detectar ameaças usando análise e inteligência e responder rapidamente quando sob ataque. Você pode experimentar a Central de Segurança Standard sem nenhum custo pelos primeiros 60 dias. Recomendamos que você Atualize sua assinatura do Azure para a central de segurança Standard.

Use a central de segurança para obter uma exibição central do estado de segurança de todos os seus recursos do Azure. Verifique rapidamente se os controles de segurança apropriados estão em vigor e configurados de maneira correta, além disso, identifique com rapidez os recursos que exigem atenção.

A central de segurança também se integra à ATP (proteção avançada contra ameaças) do Microsoft defender, que fornece recursos de EDR (detecção e resposta de ponto de extremidade) abrangentes. Com a integração do Microsoft defender ATP, você pode identificar anormalidades. Você também pode detectar e responder a ataques avançados em pontos de extremidade de servidor monitorados pela central de segurança.

Quase todas as organizações empresariais têm um sistema SIEM (gerenciamento de informações e eventos de segurança) para ajudar a identificar ameaças emergentes, consolidando informações de log de diferentes dispositivos de coleta de sinais. Os logs são então analisados por um sistema de análise de dados para ajudar a identificar o que é "interessante" do ruído que é inevitável em todas as soluções de coleta e análise de logs.

O Azure Sentinel é uma solução de disparar (gerenciamento de informações de segurança e segurança) escalonável, nativa de nuvem, de Siem (Information and Event Management). O Azure Sentinel fornece análise de segurança inteligente e inteligência contra ameaças por meio de detecção de alertas, visibilidade de ameaças, busca proativa e resposta automatizada contra ameaças.

Aqui estão algumas práticas recomendadas para impedir, detectar e responder a ameaças:

Melhor prática: Aumente a velocidade e a escalabilidade de sua solução SIEM usando um SIEM baseado em nuvem.
Detalhe: Investigue os recursos e as capacidades do Azure Sentinel e compare-os com os recursos do que você está usando no momento no local. Considere a adoção do Azure Sentinel se ele atender aos requisitos de SIEM de sua organização.

Melhor prática: Encontre as vulnerabilidades de segurança mais sérias para que você possa priorizar a investigação.
Detalhe: Examine sua Pontuação de segurança do Azure para ver as recomendações resultantes das políticas e iniciativas do Azure incorporadas à central de segurança do Azure. Essas recomendações ajudam a resolver os principais riscos, como atualizações de segurança, proteção de ponto de extremidade, criptografia, configurações de segurança, WAF ausentes, VMs conectadas à Internet e muito mais.

A pontuação segura, que é baseada em controles de CIS (Center for Internet Security), permite que você benchmark a segurança do Azure de sua organização em relação a fontes externas. A validação externa ajuda a validar e enriquecer a estratégia de segurança da sua equipe.

Melhor prática: Monitore a postura de segurança de máquinas, redes, armazenamento e serviços de dados e aplicativos para descobrir e priorizar possíveis problemas de segurança.
Detalhe: Siga as recomendações de segurança na central de segurança começando, com os itens de prioridade mais alta.

Melhor prática: Integre alertas da central de segurança à sua solução SIEM (gerenciamento de eventos e informações de segurança).
Detalhe: A maioria das organizações com um SIEM a utiliza como uma câmara de compensação central para alertas de segurança que exigem uma resposta de analista. Os eventos processados produzidos pela central de segurança são publicados no log de atividades do Azure, um dos logs disponíveis por meio de Azure Monitor. O Azure Monitor oferece um pipeline consolidado para qualquer um dos seus dados de monitoramentos de roteamento para uma ferramenta do SIEM. Consulte integrar soluções de segurança na central de segurança para obter instruções. Se você estiver usando o Azure Sentinel, consulte conectar a central de segurança do Azure.

Melhor prática: Integre os logs do Azure ao SIEM.
Detalhe: Use Azure monitor para coletar e exportar dados. Essa prática é essencial para habilitar a investigação de incidentes de segurança e a retenção de log online é limitada. Se você estiver usando o Azure Sentinel, consulte conectar fontes de dados.

Melhor prática: Acelere seus processos de investigação e busca e reduza os falsos positivos integrando recursos de EDR (detecção de ponto de extremidade e resposta) à sua investigação de ataque.
Detalhe: Habilite a integração do Microsoft defender ATP por meio da sua política de segurança da central de segurança. Considere usar o Azure Sentinel para a busca de ameaças e a resposta a incidentes.

Acompanhar monitoramento de rede baseado em cenário de ponta a ponta

Os clientes criam uma rede de ponta a ponta no Azure, combinando recursos de rede como rede virtual, ExpressRoute, Gateway de Aplicativo e balanceadores de carga. O monitoramento está disponível em cada um dos recursos da rede.

O Observador de Rede do Azure é um serviço regional. Use suas ferramentas de diagnóstico e visualização para monitorar e diagnosticar condições em um nível de cenário de rede no Azure, para o Azure e do Azure.

A seguir estão as melhores práticas para as ferramentas disponíveis e monitoramento de rede.

Melhor prática: automatizar o monitoramento remoto de rede com a captura de pacote.
Detalhe: monitore e realize o diagnóstico de problemas de rede sem fazer logon em suas VMs usando o Observador de Rede. Disparar captura de pacote por meio da configuração de alertas e obter acesso a informações de desempenho em tempo real no nível de pacote. Ao ver um problema, você poderá investigar os detalhes para um diagnóstico melhor.

Melhor prática: obter insights sobre o tráfego de rede usando os logs de fluxo.
Detalhe: desenvolva um entendimento aprofundado sobre padrões de tráfego de rede usando os logs de fluxo do grupo de segurança de rede. As informações em logs de fluxo ajudam a coletar dados para conformidade, auditoria e monitoramento do seu perfil de segurança de rede.

Melhor prática: diagnosticar problemas de conectividade de VPN.
Detalhe: use o Observador de Rede para diagnosticar os problemas mais comuns de Gateway de VPN e conexão. Você pode não apenas identificar o problema, como também usar logs detalhados para investigar ainda mais.

Implantação segura usando ferramentas do DevOps comprovadas

Use as seguintes práticas recomendadas de DevOps para garantir que suas equipes e sua empresa sejam produtivas e eficientes.

Melhor prática: automatizar a compilação e a implantação de serviços.
Detalhe: infraestrutura como código é um conjunto de técnicas e práticas recomendadas que ajudam os profissionais de TI a remover a sobrecarga de compilação e do gerenciamento diários da infraestrutura modular. Habilit a os profissionais de TI a criar e realizar a manutenção do ambiente de servidor moderno de maneira semelhante a como os desenvolvedores de software criam e mantêm o código do aplicativo.

Você pode usar o Azure Resource Manager para provisionar seus aplicativos usando um modelo declarativo. Em um modelo único, você pode implantar vários serviços, juntamente com suas dependências. Use o mesmo modelo para implantar repetidamente seu aplicativo em cada estágio do ciclo de vida do aplicativo.

Melhor prática: compilar e implantar automaticamente serviços de nuvem ou aplicativos Web do Azure.
Detalhe: Você pode configurar seu Azure DevOps Projects para Compilar e implantar automaticamente em aplicativos Web ou serviços de nuvem do Azure. O Azure DevOps implanta automaticamente os binários depois de fazer uma compilação no Azure após cada check-in de código. O processo de build do pacote é equivalente ao comando Package no Visual Studio, e as etapas de publicação equivalem ao comando Publish do Visual Studio.

Melhor prática: Automatize o gerenciamento de liberações.
Detalhe: o Azure Pipelines é uma solução para automatizar a implantação em vários estágios e gerenciar o processo de lançamento. Crie pipelines de implantação gerenciados e contínuos, a fim de lançar com rapidez, facilidade e frequência. Com o Azure Pipelines, você pode automatizar o processo de liberação e pode ter fluxos de trabalho de aprovação predefinidos. Implante localmente e na nuvem, estenda e personalize conforme a necessidade.

Melhor prática: Verificar o desempenho de seu aplicativo antes de iniciá-lo ou implantar atualizações na produção.
Detalhe: Executar testes de carga baseados em nuvem para:

- Localizar problemas de desempenho em seu aplicativo Web.
- Melhorar a qualidade da implantação.
- Garantir que seu aplicativo esteja sempre disponível.
- Garantir que seu aplicativo possa lidar com o tráfego da sua próxima campanha de marketing ou de seu próximo lançamento.

O Apache JMeter é uma ferramenta de software livre gratuita e popular com um forte suporte de comunidade.

Melhor prática: Monitorar o desempenho do aplicativo.
Detalhe: O Azure Application Insights é um serviço de gerenciamento de desempenho de aplicativo (APM) extensível para desenvolvedores da Web em várias plataformas. Use o Application Insights para monitorar seu aplicativo Web em tempo real. Ele detecta anomalias de desempenho automaticamente. Ele inclui ferramentas de análise para ajudar você a diagnosticar problemas e entender o que os usuários realmente fazem com seu aplicativo. Ele foi projetado para ajudar você a aprimorar continuamente o desempenho e a usabilidade do seu aplicativo.

Atenuação de riscos e proteção contra DDoS

Ataque de DDoS (negação de serviço distribuído) é um tipo de ataque que tenta esgotar os recursos do aplicativo. A meta é afetar a disponibilidade do aplicativo e sua capacidade de lidar com solicitações legítimas. Esses ataques estão se tornando cada vez mais sofisticados e maiores tanto em termos de tamanho quanto de impacto. Eles podem ser direcionados a qualquer ponto de extremidade publicamente acessível pela Internet.

Projetar e criar para garantir a resiliência contra DDoS exige planejar e projetar para uma variedade de modos de falha. A seguir, estão as melhores práticas para a criação de serviços resilientes a DDoS no Azure.

Melhor prática: Garanta que a segurança seja uma prioridade durante todo o ciclo de vida de um aplicativo, desde o design e implementação até a implantação e as operações. Os aplicativos podem ter bugs que permitam que um volume relativamente baixo de solicitações use muitos recursos, resultando em uma interrupção de serviço.
Detalhe: Para ajudar a proteger um serviço em execução no Microsoft Azure, você deve ter uma boa compreensão da arquitetura de seus aplicativos e se concentrar nos Cinco pilares de qualidade de software. Você deve conhecer os volumes de tráfego típicos, o modelo de conectividade entre o aplicativo e outros aplicativos e os pontos de extremidade de serviço expostos à Internet pública.

O mais importante é garantir que um aplicativo seja resiliente o suficiente para lidar com uma negação de serviço direcionados ao próprio aplicativo. A segurança e a privacidade estão incorporadas na plataforma do Azure, começando com o SDL (Security Development Lifecycle). O SDL trata da segurança em cada fase do desenvolvimento e garante que o Azure seja atualizado continuamente para torná-lo ainda mais seguro.

Melhor prática: projetar seus aplicativos para escalar horizontalmente para atender à demanda de uma carga amplificada, especificamente em caso de ataque de DDoS. Se seu aplicativo depender de uma única instância de um serviço, ele criará um único ponto de falha. O provisionamento de várias instâncias torna o sistema mais resiliente e mais escalonável.
Detalhe: Para o Serviço de Aplicativo do Azure, selecione um Plano do Serviço de Aplicativo que ofereça várias instâncias.

Para Serviços de Nuvem do Azure, configure cada uma das suas funções para usar várias instâncias.

Para Máquinas Virtuais do Azure, verifique se sua arquitetura de VM inclui mais de uma VM e se cada uma delas está incluída em um conjunto de disponibilidade. É recomendável usar conjuntos de dimensionamento de máquinas virtuais para obter recursos de dimensionamento automático.

Melhor prática: Dispor as defesas de segurança em camadas em um aplicativo reduz a possibilidade de um ataque ser bem-sucedido. Implemente designs seguros para seus aplicativos ao utilizar recursos internos da plataforma Azure.
Detalhe: o risco de ataque aumenta conforme o tamanho (área da superfície) do aplicativo. Você pode reduzir a área da superfície usando a lista de permissões para fechar o espaço de endereços IP exposto e portas de escuta que não são necessários em balanceadores de carga (Azure Load Balancer e Gateway de Aplicativo do Azure).

Grupos de segurança de rede são outra maneira de reduzir a superfície de ataque. Você pode usar marcas de serviço e grupos de segurança de aplicativo para minimizar a complexidade da criação de regras de segurança e a configuração da segurança de rede, como uma extensão natural da estrutura do aplicativo.

Você deve implantar os serviços do Azure em uma rede virtual sempre que possível. Esta prática permite que os recursos de serviço se comuniquem por meio de endereços IP privados. O tráfego do serviço do Azure de uma rede virtual usa Endereços IP Públicos como endereços IP de origem por padrão.

Usar pontos de extremidade de serviço altera o tráfego de serviço para usar endereços de rede virtual privados como endereços IP de origem ao acessar o serviço do Azure de uma rede virtual.

Muitos recursos locais dos clientes são atacados juntamente com seus recursos no Azure. Se você estiver conectando um ambiente local ao Azure, minimize a exposição dos recursos locais à Internet pública.

O Azure tem duas ofertas de serviço contra DDoS que fornecem proteção contra ataques de rede:

- A proteção básica é integrada à plataforma do Azure por padrão, sem custos adicionais. A escala e a capacidade da rede implantada globalmente do Azure fornecem defesa contra ataques de camada de rede comum por meio de monitoramento de tráfego sempre ativo e mitigação em tempo real. A básica não exige nenhuma alteração ao aplicativo ou à configuração do usuário e ajuda a proteger todos os serviços do Azure, incluindo serviços de PaaS, como o DNS do Azure.
- A proteção Standard fornece funcionalidades avançadas de atenuação de DDoS contra ataques de rede. Se ajusta automaticamente para proteger os recursos específicos do Azure. É muito simples habilitar a proteção durante a criação de redes virtuais. Isso também pode ser feito após a criação e não requer nenhuma alteração de aplicativo ou recurso.

Habilitar Azure Policy

Azure Policy é um serviço no Azure que você usa para criar, atribuir e gerenciar políticas. Essas políticas impõem regras e efeitos sobre seus recursos, para que esses recursos permaneçam em conformidade com seus padrões corporativos e contratos de nível de serviço. O Azure Policy atende a essa necessidade, avaliando os recursos quanto a não conformidade com políticas atribuídas.

Habilite Azure Policy para monitorar e impor a política de escrita da sua organização. Isso garantirá a conformidade com os requisitos de sua empresa ou de segurança regulatória gerenciando centralmente políticas de segurança em suas cargas de trabalho de nuvem híbrida. Saiba como criar e gerenciar políticas para impor a conformidade. Consulte estrutura de definição de Azure Policy para obter uma visão geral dos elementos de uma política.

Aqui estão algumas práticas recomendadas de segurança a serem seguidas depois que você adotar Azure Policy:

Melhor prática: A política dá suporte a vários tipos de efeitos. Você pode ler sobre eles na estrutura de definição de Azure Policy. As operações de negócios podem ser afetadas negativamente pelo efeito de negação e o efeito de correção , portanto, comece com o efeito de auditoria para limitar o risco de impacto negativo da política.
Detalhe: Inicie as implantações de política no modo de auditoria e, posteriormente, progresso para negar ou corrigir. Teste e examine os resultados do efeito de auditoria antes de mover para negar ou corrigir.

Para obter mais informações, consulte criar e gerenciar políticas para impor a conformidade.

Melhor prática: Identifique as funções responsáveis pelo monitoramento de violações de política e garanta que a ação de correção correta seja executada rapidamente.
Detalhe: Ter a conformidade do monitor de função atribuída por meio da portal do Azure ou por meio da linha de comando.

Melhor prática: Azure Policy é uma representação técnica das políticas escritas de uma organização. Mapeie todas as políticas do Azure para políticas organizacionais para reduzir a confusão e aumentar a consistência.
Detalhe: O mapeamento de documentos na documentação da sua organização ou na própria política do Azure adicionando uma referência à política organizacional na descrição da política do Azure ou na descrição da iniciativa de política do Azure.

Monitorar relatórios de risco do Azure AD

A grande maioria das violações de segurança ocorre quando os invasores conseguem acessar a um ambiente roubando a identidade de um usuário. Descobrir identidades comprometidas não é uma tarefa fácil. O Azure AD usa algoritmos de aprendizado de máquina e heurística adaptáveis para detectar ações suspeitas relacionadas às contas do usuário. Cada ação suspeita detectada é armazenada em um registro chamado detecção de risco. As detecções de risco são registradas nos relatórios de segurança do Azure AD. Para obter mais informações, leia sobre o relatório de segurança de usuários em risco e o relatório de segurança de entradas arriscadas.