Microsoft Security

Uma equipe de trabalho moderna precisa de segurança integrada baseada em identidade

Proteja-se contra phishing e outros ataques baseados em identidade sem comprometer a produtividade dos funcionários

Sumário

Introdução

Os usuários que acessam ativos corporativos por meio de redes domésticas inseguras e dispositivos não gerenciados são alvos comuns de ciberataques. Como os ambientes de trabalho remotos e híbridos estão se tornando cada vez mais comuns em muitas organizações, **as ameaças também estão ficando mais complexas**. Por isso, as equipes de segurança estão adotando cada vez mais modelos de segurança baseados em identidade para fornecer acesso seguro a ativos corporativos sem comprometer a experiência ou a produtividade do usuário.

A estratégia certa envolve uma abordagem moderna e integrada que combina autenticação robusta, controle de acesso baseado em políticas adaptáveis e detecção proativa e remediação de uso indevido e de violações de identidade.

A necessidade de ter um sistema de segurança robusto baseado em identidade

Mesmo antes da COVID-19, os líderes de segurança procuravam alternativas à segurança tradicional baseada em perímetro para acomodar uma equipe de trabalho cada vez mais móvel, além da migração contínua de dados, aplicações e infraestrutura de TI para a nuvem. A mudança para o trabalho remoto impulsionada pela pandemia aumentou ainda mais a superfície de ataque e deixou as organizações mais vulneráveis a ataques e violações.

Para os criminosos cibernéticos, essa mudança apresentou novas oportunidades para acessar e extrair dados corporativos. O **Relatório de Defesa Digital da Microsoft** constatou que agentes de estado-nação estão adotando técnicas de reconhecimento mais sofisticadas, além da coleta de credenciais e explorações de VPN (rede privada virtual). A aplicação dos controles de segurança tradicionais e das políticas que funcionavam sob a proteção do perímetro de rede tornou-se mais difícil quando os dados confidenciais migraram das instalações corporativas para as casas dos funcionários, cuja segurança de sistemas e redes é fraca.

O número de ameaças à identidade aumentou significativamente desde a início da pandemia. Somente em março de 2020, a **Microsoft detectou** 4,9 bilhões de logons feitos por invasores e mais de 150 mil contas comprometidas. Houve também um **grande aumento no número de ataques** envolvendo métodos de força bruta e comprometimento de email de negócios (BEC) para coletar credenciais corporativas. Uma **pesquisa da Microsoft** feita em 2020 relatou que 28% das organizações sofreram um ataque de phishing bem-sucedido. Muitas vezes, as credenciais comprometidas foram usadas para acessar dados corporativos ou para facilitar ataques futuros. Por exemplo, os invasores usaram credenciais de identidade roubadas para **escolher alvos, passar por pessoas importantes na organização** e cometer fraudes, incluindo a realização de pagamentos ilegítimos e transferências bancárias.

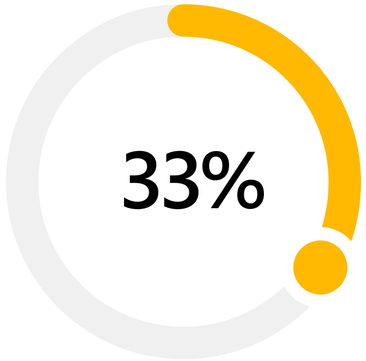
4,9 bilhões

de logons feitos por invasores somente em março de 2020

Mais de 150 mil

contas comprometidas

Os gerentes de segurança sabem que a aplicação de controles de acesso e proteção de identidade mais robustos são cada vez mais necessários. Eles reconhecem que as equipes de segurança também precisam detectar e responder a ameaças no perímetro estendido da equipe de trabalho remota, além de proteger os dados dentro da rede corporativa. O estudo **2020 Security Priorities** (Prioridades de segurança de 2020) do IDG mostrou que 33% dos profissionais de segurança disseram que o aprimoramento dos controles de identidade e acesso é uma das principais prioridades de segurança em 2021 devido ao aumento de ataques baseados em identidade direcionados a trabalhadores remotos.



33% dos profissionais de segurança disseram que o aprimoramento dos controles de identidade e acesso é uma das principais prioridades em 2021

Os benefícios da segurança integrada baseada em identidade

Para fornecer acesso perfeito e seguro aos recursos hospedados na infraestrutura local e na nuvem aos trabalhadores remotos, as organizações precisam de uma estratégia de segurança integrada baseada em identidade que combine autenticação robusta com recursos para proteção proativa contra o uso de identidade indevido.

Os componentes críticos incluem o uso da MFA para proteger o acesso aos recursos corporativos e o suporte a políticas para controlar o que, quando e como um usuário específico pode acessar informações e sistemas usando informações contextuais e em tempo real sobre o usuário, o dispositivo, o local e o risco da sessão. Além disso, a solução deve integrar mecanismos para detectar e responder de forma inteligente a contas comprometidas e a ameaças usando a Inteligência Artificial baseada em nuvem e os recursos de automação.

Abordar a segurança de forma integrada pode simplificar o gerenciamento de identidades, pois fornece aos administradores uma visão unificada de dados de várias fontes em um único console. Essa abordagem oferece às organizações uma maneira de usar indicadores relacionados não só à identidade, mas também em todos os dispositivos, aplicações e redes em uma empresa, o que permite a execução de políticas consistentes de controle de acesso.

A abordagem integrada agiliza a segurança na infraestrutura local e em ambientes multinuvem, abrangendo todos os pontos de extremidade, aplicativos e workloads.

Uma equipe de trabalho moderna precisa de segurança integrada baseada em identidade

A abordagem integrada de segurança da Microsoft, da identidade até a proteção contra ameaças

Segurança baseada em identidade

A solução de gerenciamento de identidade e de acesso da Microsoft, o Azure Active Directory, integra recursos para autenticação robusta e controle de acesso granular usando políticas adaptativas em tempo real e detecção e remediação de risco da identidade automatizadas. O Microsoft Azure Active Directory ajuda as organizações a proteger o acesso a recursos e dados com uma autenticação robusta e políticas de acesso adaptativas baseadas em risco em tempo real.

O Azure AD ajuda as organizações a proteger o acesso a recursos e dados com uma autenticação robusta. Ele simplifica o logon usando métodos de autenticação sem senha, como o Microsoft Authenticator e o Windows Hello, que permitem que os usuários façam a autenticação com segurança em dispositivos móveis e na Web sem a necessidade de inserir senhas. O acesso condicional no Azure AD permite que as organizações controlem o que um usuário pode acessar, quando e como, dependendo de fatores como dispositivo, localização e informações de risco em tempo real.

A proteção de identidade do Azure AD pode detectar e responder automaticamente a contas comprometidas e outros riscos baseados em identidade. O Azure AD usa recursos avançados de aprendizado de máquina, análise de comportamento de usuários e entidades (UEBA) e inteligência relacionada ao comportamento do usuário para monitorar continuamente atividades suspeitas e proteger contra violações de identidades perdidas ou roubadas em tempo real.

Proteção integrada contra ameaças

A interoperação com outros produtos de segurança da Microsoft, como o Microsoft 365 Defender, o Azure Defender e o Azure Sentinel, pode fornecer mais contexto para detectar, analisar e responder a ameaças entre recursos, assim como identidades, com suporte a recursos de Inteligência Artificial para ajudar a unir indicadores e identificar o que é mais importante. A integração permite que as organizações comparem indicadores sobre usuários de risco, logons e outros eventos com dados de ameaças em ambientes híbridos que abrangem aplicativos na infraestrutura local e na nuvem.

A proteção integrada contra ameaças é fundamental porque os invasores usarão qualquer vulnerabilidade que puderem encontrar em aplicativos, dispositivos, serviços de nuvem e, até mesmo, usuários. Quando um agente mal-intencionado encontra uma abertura, ele usará essa base inicial para ganhar privilégios e mover-se lateralmente em uma rede até que encontre o que deseja. Um sistema de segurança integrado baseado em identidade pode ajudar a detectar e responder a essa atividade em todos os pontos de extremidade, aplicativos, workloads, ambientes de nuvem e na infraestrutura local por meio de um único painel de controle.

Os analistas de segurança podem usar um único painel para identificar atividades de usuário suspeitas e correlacionar informações em vários conjuntos de dados para detectar e responder a ataques em vários estágios. As equipes de segurança podem ver uma violação e receber contexto sobre como um invasor entrou na infraestrutura e como ele se espalhou, e, dessa forma, descobrir como evitar futuros ataques.

A segurança integrada baseada em identidade em ação

A integração completa, habilitada com um modelo de segurança baseado em identidade, oferece muitos benefícios para as organizações em todas as indústrias. Veja estes três exemplos.

✓ Vá além das decisões simples de permissão/bloqueio e passe a usar controles de acesso mais granulares:

A Lumen Technologies está aproveitando o suporte para políticas de acesso condicional no Azure Active Directory para definir quais aplicativos e quais dados os funcionários podem acessar em casa ou durante uma viagem ao exterior.

✓ Avaliação de risco em tempo real e mitigação de ameaças baseadas em identidade:

A Bridgewater Associates usa a ferramenta de proteção de identidade no Microsoft Azure Active Directory para identificar tentativas de logon suspeitas e arriscadas e bloquear usuários, redefinir senhas ou exigir autenticação multifatorial baseada em indicadores como locais e endereços IP.

✓ Crie resiliência com a avaliação e o monitoramento de acesso contínuo:

A empresa global de logística de contêineres Maersk implementou as ferramentas de proteção de identidade e acesso condicional do Azure AD para sinalizar comportamentos de risco e tomar medidas, como a revogação de acesso, de forma rápida, evitando que o problema se intensifique.

Comece a usar

Acabe com as lacunas entre as soluções pontuais e obtenha cobertura em todo o seu ambiente multiplataforma e multinuvem.

Saiba mais

Microsoft