Microsoft para exigir autenticação de vários fatores em logins do portal do

Data: 2025-09-02 06:14:02

Autor: Inteligência Against Invaders

A Microsoft anunciou que será aplicável a autenticação multifatorial (MFA) para todas as tentativas

de login no portal do Azure e outras interfaces administrativas.

O novo requisito, que se baseia no compromisso de longa data da Microsoft com a segurança, visa bloquear o acesso não autorizado a recursos em nuvem de alto valor, adicionando uma camada extra de verificação além das senhas.

De acordo com a própria Microsoft pesquisarA ativação do MFA pode impedir mais de 99,2 % dos ataques de compromisso da conta, tornando -o uma das defesas mais eficazes contra roubo de credenciais.

Com essa estatística em mente, a empresa apresentou um plano de lançamento em duas fases, projetado para dar às organizações tempo suficiente para cumprir e preparar.

Fase 1: Interfaces de portal e administrador

A partir de outubro de 2024, qualquer conta assinando o Azure Portal, o Microsoft ENTRA Admin Center ou o Microsoft Intune Admin Center para executar operações de criação, leitura, atualização ou exclusão devem usar o MFA. Essa mudança será lançada gradualmente para todos os inquilinos globalmente.

A partir de fevereiro de 2025, a aplicação do MFA se estende ao Microsoft 365 Admin Center. Os administradores que já aplicam o MFA, ou que usam métodos sem senha (como Passkeys ou Fido2), não terão alterações em sua experiência de assinatura.

Fase 2: Ferramentas de linha de comando e API

A partir de 1º de outubro de 2025, a Microsoft exigirá que o MFA para operações realizadas através da CLI do Azure, do Azure PowerShell, do aplicativo móvel do Azure, das ferramentas de infraestrutura-código (IAC) e dos pontos de extremidade da API de REST de controle de controle ao criar, atualizar ou deletar recursos.

Os comandos somente leitura permanecerão não afetados. Esta fase garante que os fluxos de trabalho de automação e script, quando autenticados com as credenciais do usuário, também se beneficiem da proteção da MFA.

Uma lista detalhada de nomes de aplicativos, IDs e datas de partida de execução acompanha o anúncio.

Os principais alvos da fase 1 incluem o portal do Azure (ID do aplicativo: C44B4083-3BB0-49C1-B47D-974E53CBDF3C) e o Microsoft ENTRA Admin Center, ambos começando na segunda metade de 2024.

Aplicações da fase 2, como o Azure PowerShell (ID do aplicativo: 1950A258-227B-4E31-A9CF-717495945FC2) e CLI Azure (ID do aplicativo: 04B07795-8DDB-461A-BBEE-02F9E1BF7B46), Will ENFOTE.

A Microsoft adverte o uso de contas de usuário para tarefas automatizadas. As organizações são incentivadas a migrar contas de serviço baseadas no usuário para proteger identidades de carga de trabalho baseadas em nuvem, como identidades gerenciadas ou diretores de serviço.

Essas identidades não estão sujeitas às fases de aplicação do MFA e fornecem uma alternativa mais segura para scripts e automação.

Para se preparar, os administradores devem revisar as políticas de acesso condicional existentes ou permitir que os padrões de segurança exigem o MFA.

Para os inquilinos que exigem tempo adicional, a Microsoft permite o adiamento da Fase 1 até 30 de setembro de 2025 e Fase 2 até 1º de julho de 2026, através de portais de gerenciamento designados.

No entanto, a Microsoft alerta que o atraso no MFA aumenta o risco, pois os sinais administrativos continuam sendo alvos principais para os atacantes.

À medida que as cibernéticas continuam a evoluir, o requisito de MFA da Microsoft reforça sua estratégia de segurança zero-confiança.

Ao garantir que todas as ações administrativas do Azure sejam autenticadas com vários fatores, a empresa pretende proteger as cargas de trabalho do cliente e defender a integridade dos ambientes em nuvem em todo o mundo.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.