White paper

Host Access Management and Security Server (MSS)
MSS Advanced Authentication Add-On

Uso da autenticação baseada em vários fatores para autorizar acesso ao mainframe

MICRO FOCUS

As senhas são insatisfatórias

Para ser franco, autenticar usuários com nomes de usuário e senhas não é mais um processo eficaz. Por quê? Os usuários são descuidados com as senhas. Eles escolhem senhas óbvias. Eles usam a mesma senha várias vezes. E anotam as senhas em notas adesivas que qualquer pessoa pode ver.

Mas os usuários não são o único problema

Quando você confia em nomes de usuário e senhas, você praticamente entrega aos hackers as chaves da sua casa. Os criminosos experientes escrevem algoritmos avançados para encontrar maneiras de entrar. Depois, quando a mesma senha é usada para vários aplicativos, os hackers que descobriram uma senha podem entrar onde quiserem. Por exemplo, um hacker pode roubar a senha de um usuário no Facebook e, com isso, ter acesso a toda a sua infraestrutura corporativa. É um enorme motivo de preocupação.

O ponto é que nomes de usuário e senhas são algo que um usuário precisa conhecer. Tudo isso pode ser capturado ou roubado com certa facilidade. Por si só, as senhas não são seguras o suficiente.

As senhas dos antigos mainframes são extremamente insatisfatórias

Os problemas de senha que acabamos de descrever também se aplicam às senhas de mainframe. A diferença é que as senhas de mainframe de aplicativos mais antigos, aqueles que gerenciam sua empresa e contêm todos os dados mais confidenciais, são protegidas apenas por senhas de oito caracteres e não diferenciam maiúsculas de minúsculas. Escrito há décadas, numa época mais segura, os aplicativos de mainframe foram codificados com segurança fraca de senha de oito caracteres porque isso era satisfatório. Não é mais.

O que é autenticação baseada em vários fatores (MFA)?

A MFA combina várias fontes de identidade como uma maneira de autorizar o acesso. As soluções mais eficientes de MFA combinam, no mínimo, dois dos três tipos de fontes de identidade a seguir:

- Algo que você *sabe* , como um código PIN ou uma senha.
- Algo que você *tem* , como um cartão de chave, telefone ou token.
- Algo que é *seu*, como impressão digital, verificação de retina, reconhecimento de voz ou reconhecimento facial.

Ao exigir, no mínimo, duas dessas três fontes, você reforça significativamente os requisitos de autenticação e reduz o risco de violação de segurança.

O que não é MFA?

Quando o banco solicita seu PIN e o número do CPF, isso *não é* MFA. PINs e CPFs são coisas que você *sabe*. A MFA combina duas entre três fontes *diferentes* do que você sabe, tem ou possui.

A crescente necessidade de MFA

As organizações estão cada vez mais cientes dos riscos associados à autenticação de fator único para transações on-line. "O relatório de violação de dados da Verizon de 2013 aponta como a autenticação de fator único como a principal responsável por violações de segurança e informa que 76% das invasões de rede em 2012 exploraram o roubo de credenciais fracas." A MFA pode reverter esse problema dispendioso, tornando os pagamentos eletrônicos tão rápidos e confiáveis quanto os pagamentos em dinheiro.

A proliferação de novas regulamentações governamentais, como HIPAA, também está impulsionando a adoção da MFA. Em 26 de março de 2013, as novas regras do U.S. Department of Health and Human Services (Departamento de saúde e assistência social dos EUA) entraram em vigor. Essas regras estenderam os requisitos de segurança e privacidade da HIPAA para parceiros de negócios, incluindo terceiros, fornecedores e colaboradores que executam serviços em nome de um prestador de serviços de saúde ou que oferecem soluções que se integram aos dados de médicos ou pacientes. Devido à aplicação de elevadas multas por não conformidade, muitas organizações estão adotando a MFA.

Se a MFA é tão incrível, por que não a estamos utilizando?

A mudança geralmente vem acompanhada de resistência, e migrar para MFA não é diferente. A resistência à MFA, em geral, está associada a um ou mais dos seguintes motivos:

- **Falta de informações**: os métodos de autenticação biométrica (por exemplo, leitores de impressão digital) já foram incorporados a smartphones e computadores. No entanto, muitas empresas simplesmente não sabem como incorporar essa nova tecnologia às suas infraestruturas de segurança.

- **Medo do desconhecido**: por exemplo, a MFA dificultará a experiência do usuário? Como a facilidade de uso geralmente se traduz em eficiência, as organizações estão hesitantes em alterar o status quo por qualquer motivo, até mesmo pelo fortalecimento da segurança.
- **Medo de falhar**: para aproveitar todos os benefícios da MFA, é necessário configurá-la completamente. Se você não fizer isso, obterá apenas resultados medíocres. A amplitude de implementação necessária pode ser assustadora.

No que diz respeito à implementação da MFA para autorizar acesso ao mainframe, as raízes de resistência são ainda mais difíceis de superar.

MFA e o mainframe

Apesar de a segurança para acessar aplicativos corporativos ter sido fortalecida para atender à ameaças cada vez mais sofisticadas, a segurança integrada em seus aplicativos de mainframe está estática há várias décadas. Pergunte a um profissional de segurança de TI se ele acha que as senhas de oito caracteres que não diferenciam maiúsculas de minúsculas oferecem um nível apropriado de autenticação para dados confidenciais. A resposta será um "Não!". Mesmo assim, o mainframe normalmente fica fora das discussões sobre MFA.

Este é o problema: por mais robusto e confiável que seja, o mainframe fica geralmente isolado do restante da empresa. Os administradores de TI consideram que essa área é melhor atendida pelos especialistas em mainframe. Esses especialistas, os Administradores de sistemas de mainframe, sabem que a reengenharia aplicada nos aplicativos de mainframe para que eles trabalhem com senhas fortes e complexas é arriscada, difícil e cara. Eles não querem arriscar o recorde de confiabilidade de 99,999% do mainframe. Por mais que estejam preocupados com questões de segurança, eles se sentem de mãos atadas.

O que é necessário para superar a resistência deles é uma maneira de estender a segurança forte e gerenciada centralmente até os aplicativos de mainframe, sem comprometer as operações da empresa.

A solução da Micro Focus

Na realidade, há uma maneira segura, gerenciável e econômica de estender a segurança forte e gerenciada centralmente até os aplicativos de mainframe. Ele se chama Micro Focus® Host Access Management and Security Server (MSS). O MSS funciona integrando o mainframe ao Sistema de gerenciamento de Identidade e Acesso (IAM), gerenciando e protegendo o acesso ao mainframe por meio dos emuladores de terminal da Micro Focus.

Localizado entre o usuário e o mainframe, o MSS usa a estrutura de autenticação LDAP existente para validar as credenciais de um usuário antes de conceder acesso ao mainframe. Em outras palavras, os usuários não conseguem se aproximar da tela de logon do host até que tenham sido autenticados e autorizados com credenciais fortes de IAM, ou seja, senhas fortes e complexas.

O MSS funciona com um produto complementar chamado MSS Advanced Authentication para fornecer a autenticação mais forte possível para os sistemas de mainframe. Juntos, esses dois produtos são atualmente compatíveis com 14 diferentes métodos de autenticação, desde cartões inteligentes e códigos de verificação móveis com base em texto até impressão digital e verificação de retina. Entre essa gama de opções, você pode selecionar as que são mais fáceis de serem adotadas e mantidas por sua organização.

O MSS e o MSS Advanced Authentication podem ser instalados em um servidor ou no mainframe, o que funcionar melhor para sua empresa. Eles fornecem uma solução flexível e altamente segura para acesso ao mainframe que não compromete as operações da empresa.

Repensando a MFA para o mainframe

Geralmente, quando uma nova tecnologia é implantada, ela falha porque ninguém pensou em todas as implicações. Antes de começar a implantar a MFA, há vários aspectos que você precisa considerar:

- Estabelecer e implementar uma política de autenticação global, em vez de adotar uma abordagem gradual com aquisições ad-hoc.
- Tornar a MFA fácil de gerenciar evitando diferentes métodos de autenticação para sistemas distintos.
- Tornar a MFA fácil de usar. Considere a implementação simultânea de single sign-on para simplificar o processo de autenticação.

Se utilizada da maneira correta, a MFA facilita o processo de autenticação para os usuários. Afinal, deslizar o dedo em um leitor e inserir um código PIN é mais fácil do que lembrar um nome de usuário e uma senha.

O que esperar de um fornecedor de MFA

Para garantir uma integração simples da MFA, tenha estes fatores em mente durante a pesquisa:

- Procure soluções que ofereçam diversas opções e aplicativos de autenticação.
- Não se prenda a um único tipo de autenticação física. Em outras palavras, não deixe que o hardware escolhido imponha uma filosofia de autenticação.
- Procure fornecedores que se aperfeiçoam com metodologias abertas atualizadas de forma agressiva à medida que novas tecnologias são lançadas.
- Por fim, procure fornecedores que facilitem o sistema para você.

Não faz sentido exigirmos autenticação forte para acessar aplicativos corporativos, mas apenas uma autenticação fraca para acessar aplicativos de mainframe essenciais, isto é, os que fazem sua empresa funcionar. Conforme as ameaças de segurança continuam a aumentar, sua organização precisa enfrentar o desafio. A Micro Focus oferece uma maneira segura, gerenciável e econômica de fazer isso.

Micro Focus
Argentina
+54 11 5258 8899

Brasil
+55 11 3627 0900

Colombia
+57 1 622 2766

México
+52 55 5284 2700

Venezuela
+58 212 267 6568

Micro Focus
Sede da empresa
Reino Unido
+44 (0) 1635 565200

www.microfocus.com

www.microfocus.com