White paper

Uma nova abordagem a senhas de mainframe: livre-se delas

opentext™

Uma nova abordagem a senhas de mainframe: livre-se delas

Senhas são uma necessidade corporativa. Seu trabalho é garantir que somente usuários autorizados possam acessar seu bem mais precioso: a informação. Devido a essa função essencial, não basta ter uma senha qualquer. A senha ideal é longa e complexa. Ela é diferente para cada aplicativo. E exige atualizações regulares.

As senhas também são uma ameaça corporativa. Criar, lembrar e mudar constantemente as senhas é um fardo para os usuários. Tentar gerenciar e assegurar o uso obrigatório de políticas de senha é um fardo para a TI. Felizmente, os modernos sistemas de NetIQ Identity and Access Management "Gerenciamento de Identidade e Acesso" (IAM), juntamente com o Single Sign-On (SSO), têm ajudado a diminuir esse problema. Os usuários só precisam fazer login uma vez para acessar a maioria dos recursos da empresa.

A maioria, mas não *todos*. Infelizmente, o IAM e o SSO não funcionam com seus sistemas mais críticos: aqueles que, de fato, movem sua empresa. Os sistemas mainframe.

"Forneça acesso a qualquer hora, em qualquer lugar e por qualquer dispositivo ao mainframe"

Os usuários de hoje esperam um acesso a qualquer hora, em qualquer lugar e por qualquer dispositivo a todos os recursos da empresa, inclusive o mainframe. Mas dar acesso irrestrito ao mainframe deixa os administradores de rede de TI e os administradores de sistemas mainframe preocupados.

Por quê? Porque quando se trata de fornecer acesso seguro, a rede e o mainframe são como duas ilhas autônomas. Cada um usa seu próprio sistema de controle de acesso. Cada um tem seu próprio sistema de regras. E nenhum desses sistemas deseja renunciar ao controle do seu domínio para acomodar o outro.

Apesar das dependências mútuas e dos benefícios obtidos ao se trabalhar em conjunto, os sistemas de regra de cada ilha não enxergam uma maneira de superar os obstáculos de integração.

Ilha de redes

Os administradores de redes de TI têm um interesse direto em reforçar a segurança para o acesso ao mainframe, porque eles gerenciam os aplicativos de emulação de terminal que tornam o acesso possível. Mas não é possível estender a forte segurança da rede, que tem senhas fortes facilitadas pelo IAM, para a ilha de mainframes.

A maioria dos aplicativos de mainframe foi programada há décadas, em uma época mais segura. Não existiam redes abertas, arquiteturas orientadas por serviço e hackers mal-intencionados. Os aplicativos de mainframe eram codificados com senhas fracas de oito caracteres, pois isso era suficiente. Não mais.

Reprogramar aplicativos de mainframe atualmente, mesmo que você se depare por um acaso com um programador de mainframe ainda empregado, é uma tarefa arriscada, incômoda e cara. A única outra forma de assegurar o uso obrigatório de uma única senha para acessar todos os recursos da rede, inclusive o mainframe, é simplificar as senhas de toda a empresa para oito caracteres. Ninguém quer fazer isso.

Ilha de mainframes

Os administradores de sistema mainframe sabem que depois de ser ignorado por décadas pela comunidade de hackers, o mainframe agora é um grande alvo. Eles não têm IAM, mas têm RACF ou Top-Secret para autenticar e autorizar o acesso ao mainframe. Isso é muito bom, exceto pelo fato de que eles ainda estão presos a senhas fracas de oito caracteres.

Por mais que eles queiram fortalecer suas senhas, e o controle de acesso, os administradores de sistema mainframe são irredutíveis no que diz respeito a uma coisa: em nenhuma circunstância eles colocarão em risco o recorde de confiabilidade de 99,999 por cento do mainframe. Mas, na mente deles, é exatamente isso que eles estariam fazendo se tentassem integrar o acesso ao mainframe com servidores de rede na ilha de redes. E eles simplesmente não podem arcar com o tempo de espera constante normalmente associado a problemas de segurança da rede.

Problemas de senha do mainframe

Apesar de sua capacidade, os mainframes têm algumas peculiaridades que os tornam um caso isolado em empresas modernas. Uma dessas peculiaridades é a senha de aplicativos de mainframe. Este é o motivo do problema:

- **Autenticação fraca**
  Pergunte a qualquer especialista em segurança se ele acha que senhas de oito caracteres que não diferenciam maiúsculas de minúsculas são fortes o suficiente para proteger dados confidenciais. A resposta será um retumbante "Não!". Políticas rígidas são associadas a senhas corporativas. Mas, pelos motivos mencionados acima, essas políticas não podem ser aplicadas ao acesso ao mainframe.

Defesa aprofundada com o MSS

Você pode adicionar ainda mais camadas de segurança emparelhando o MSS com estes componentes complementares:

- **MSS Security Proxy Add-On**
  Entregue a criptografia ponto a ponto e assegure o uso obrigatório do controle de acesso ao perímetro com a tecnologia de segurança patenteada.
- **MSS Advanced Authentication Add-On**
  Permite a autenticação baseada em vários fatores para autorizar o acesso aos seus valiosos sistemas de host.
- **Login automatizado para complemento de mainframe do MSS**
  Permite o login automatizado para aplicativos IBM 3270 por meio do seu sistema de gerenciamento de identidade e acesso.
- **MSS PKI Automated Sign-On Add-On**
  Login automatizado de aplicativo permitido pelo PKI aos seus principais sistemas empresariais.
- **MSS Terminal ID Management Add-On**
  Aloca dinamicamente IDs de terminal com base no nome de usuário, nome DNS, endereço IP ou pool de endereços.

Com o MSS e seus produtos complementares, finalmente, há uma forma prática para modernizar a segurança do mainframe sem qualquer recodificação.

Como o login automatizado para mainframe funciona

Trabalhando com o DCAS (Digital Certificate Access Server, servidor de acesso com certificado digital) do IBM z/OS, o Login automatizado para mainframe obtém um PassTicket R de uso único por um período limitado para o aplicativo almejado. Ele retorna a ID de usuário do mainframe e o PassTicket para a macro de login do emulador de terminal, que envia as credenciais para o mainframe para fazer o login do usuário no aplicativo.

- **Comportamento arriscado do usuário**
  Nessa era de acesso instantâneo, a etapa de login adicional necessária para o acesso ao mainframe é uma perda de tempo para a maioria dos usuários. Pense nisso. Quem quer digitar uma senha diferente sempre que abrir um novo aplicativo, principalmente se você costuma abrir cinco ou seis por dia? Por isso, os usuários procuram soluções alternativas convenientes, como negligenciar o logout ou sair das estações de trabalho ainda conectado (e desprotegido).
- **Redefinições de senha do mainframe — Que chato!**
  Os usuários que acessam vários aplicativos em vários mainframes têm várias senhas para memorizar. Ninguém pode fazer isso, portanto, eles recorrem a lembretes de segurança informais em post-its ou pequenas mudanças de senha em tempos de atualização. Mas os usuários são esquecidos e precisam redefinir as senhas. Ao contrário das senhas de rede, as senhas de mainframe não podem ser redefinidas pelo usuário. Um colaborador de TI que tem um custo alto deve parar o que está fazendo para executar essa tarefa trivial e demorada.

De riscos à segurança à usabilidade e problemas de gerenciamento de TI, fazer login no mainframe com uma senha de oito caracteres é uma prática que precisa de atualização.

A ponte para a felicidade da segurança

Nossas duas ilhas não evoluíram paralelamente. Na ilha de redes, a segurança para acessar aplicativos corporativos tem se tornado mais forte para acompanhar ameaças cada vez mais sofisticadas. Na ilha de mainframes, a segurança programada há décadas nesses aplicativos críticos tem se mantido inerte há décadas.

Felizmente, há uma maneira de estender a forte segurança gerenciada de forma centralizada aos aplicativos de mainframe, sem comprometer as operações da empresa. Ela se chama OpenText™ Host Access Management and Security Server (MSS). O MSS integra o mainframe com o sistema IAM, criando uma ponte entre as duas ilhas.

Mais especificamente, o MSS funciona com seu sistema IAM para gerenciar de forma centralizada e proteger o acesso ao mainframe por meio de emuladores de terminal Micro Focus. Localizado entre o usuário e o mainframe, ele usa a estrutura existente de autenticação de LDAP para validar as credenciais de um usuário antes de conceder acesso ao mainframe. Em outras palavras, os usuários não podem se aproximar da tela de login do host até que tenham sido autenticados e autorizados com fortes credenciais do IAM, ou seja, senhas fortes e complexas.

Combinado com um de seus componentes de complemento, o Login automatizado para Mainframe, o MSS também elimina a necessidade de senhas de mainframe. Isso mesmo. Os usuários não têm mais o trabalho adicional de inserir uma senha para fazer login em seus aplicativos de mainframe depois de efetuar a autenticação no MSS. O MSS faz isso por eles. É uma solução vantajosa para todos os usuários. Chega de memorizar senhas arriscadas de oito caracteres. A TI não é mais consciente em termos de segurança e, finalmente, pode sair do cenário de gerenciamento de senhas.

O MSS pode ser instalado em um servidor ou no mainframe, o que funcionar melhor para sua empresa. Ele fornece uma solução flexível, escalável e segura para o acesso ao mainframe que elimina a necessidade de senhas de mainframe.

Seguro, gerenciável e econômico

Foi-se o tempo em que os dados valiosos do mainframe percorriam um caminho protegido em um terminal confiável. Não mais. Agora, protegê-los contra os malfeitores na estrada da Internet exige a proteção mais forte que existe. É hora de deixar senhas fracas de oito caracteres no passado onde elas pertencem. Em vez disso, crie uma ponte para a autenticação mais forte que há, garantindo que somente usuários autorizados possam acessar seus dados mais valiosos. O MSS oferece uma maneira segura, gerenciável e econômica de fazer isso.

Saiba mais em
www.microfocus.com/opentext

Conecte-se conosco

Blog de Mark Barrenechea,
CEO da OpenText

262-PB0080-001 | O | 09/23 |

opentext™