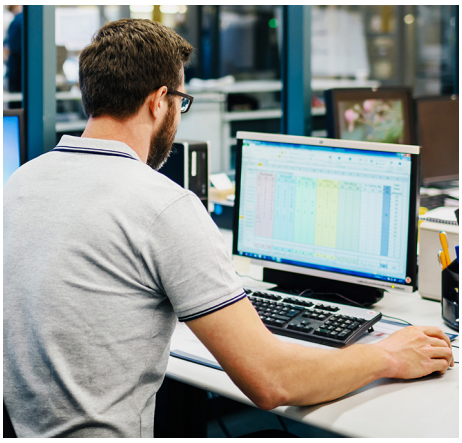
opentext™



Traga sanidade para o acesso ao mainframe com o Automated Sign-On

Albert Einstein disse que fazer a mesma coisa repetidas vezes e esperar resultados diferentes é a definição de loucura. Da mesma forma, aplicar o mesmo nível de segurança para acesso a mainframe ano após ano e esperar magicamente um aumento na segurança é, na verdade, uma loucura.

Embora a segurança para acesso a aplicativos empresariais tenha evoluído para responder às novas ameaças à segurança, a segurança para acesso a aplicativos de mainframe permanece a mesma há décadas. Esta estagnação ocorreu por três motivos principais:

- Em primeiro lugar, aplicativos legados de mainframe ainda fazem o trabalho pesado na maioria das empresas. Alterá-los é arriscado, difícil e caro. Até mesmo encontrar os recursos humanos necessários para atualizar os controles de acesso de segurança para esses aplicativos é quase impossível.
- Segundo, as grandes empresas muitas vezes carecem da vontade interna de se aprofundar no "ninho de vespas" do mainframe. O diálogo de TI costuma ser algo do tipo: "E se estragarmos alguma coisa?" E se for muito mais complicado do que achamos que era? E se nossa empresa parar de funcionar? Não podemos colocar nosso mainframe em um porto seguro e reparar tudo enquanto nossas empresas estão em funcionamento. Além disso, os custos para duplicar o ambiente são muito elevados em termos de tempo e dinheiro.
- Terceiro, existe a percepção de que o mainframe está seguro e protegido atrás do firewall, onde apenas usuários autorizados podem entrar. Mas não há garantia de que alguém mal-intencionado não vá roubar ou hackear as credenciais de login do mainframe de outra pessoa.

  Aqueles aplicativos mais antigos utilizam senhas de oito caracteres fracas e que não diferenciam maiúsculas de minúsculas. Não há um administrador de rede no mundo que acredite que essas senhas são fortes o bastante para proteger qualquer coisa, especialmente as informações intelectuais e de clientes.

A pergunta é: como quebrar um padrão de loucura quando alguns dos motivos para o comportamento são baseados em medos bastante reais e lógicos?

Os sistemas de segurança incompatíveis da empresa

Há dois sistemas de segurança na maioria das empresas. Um é o sistema de Gerenciamento de Identidade e Acesso (IAM, da sigla em inglês) utilizado para fornecer acesso aos recursos e aos aplicativos da empresa. Sistemas de IAM exigem o uso de uma senha forte para obter acesso, geralmente uma com um mínimo de 12 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais. Senhas fortes são infinitamente mais difíceis de se hackear ou roubar.

Sistemas mainframe também têm seu próprio tipo de "IAM", geralmente conhecido como RACF ou Top-Secret. Esses sistemas oferecem autenticação e autorização para recursos do mainframe. O problema ocorre porque, segundo o design original, os aplicativos que utilizam esses sistemas exigem somente senhas fracas de oito caracteres.

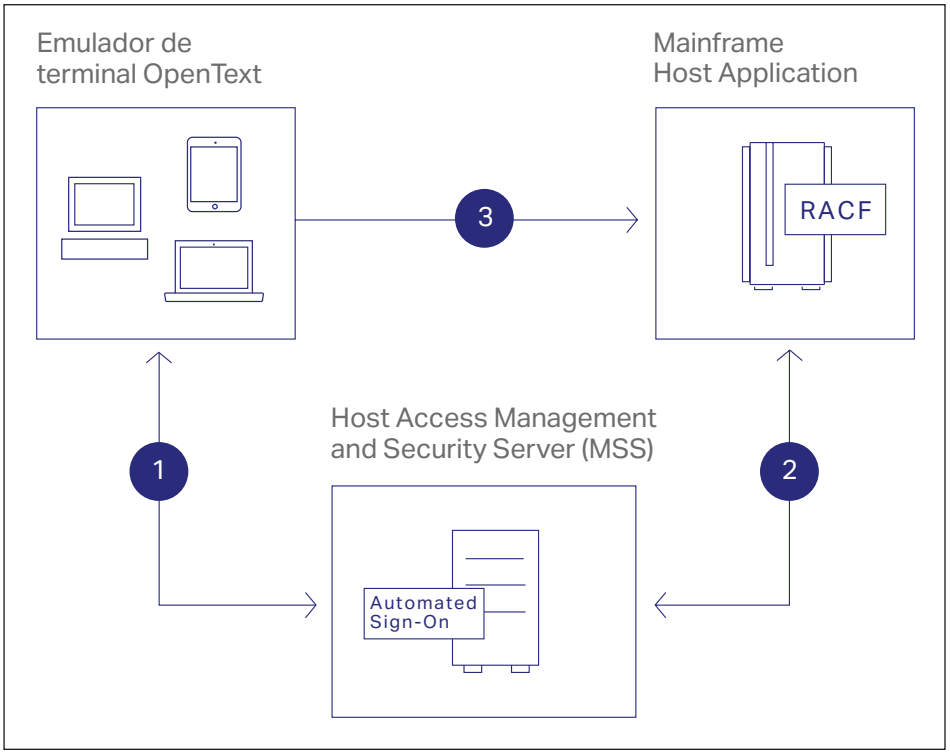
Assim, temos dois sistemas separados fornecendo acesso aos recursos da empresa. Devemos nos perguntar: por qual motivo exigimos autenticação forte para acessar aplicativos da empresa, mas apenas autenticação fraca para acessar aplicativos de mainframe críticos, aqueles que fazem seus negócios funcionarem? Isso é absurdo.

Dê fim à loucura

E se houvesse um modo de usar seu sistema de IAM para controlar e gerenciar o acesso ao seu sistema host? Na verdade, existe. Ela se chama OpenText™ Host Access Management and Security Server (MSS).

O MSS finalmente traz sanidade à empresa integrando seu mainframe ao sistema de Gerenciamento de Identidade e Acesso (IAM) existente. O MSS coloca um ponto de controle de segurança entre os usuários que precisam ter acesso ao mainframe e os sistemas de host. Ele usa sua estrutura de IAM existente (especificamente a autenticação forte) para autorizar o acesso ao mainframe.

O MSS também fornece um produto complementar (o Automated Sign-On for Mainframe) para levar sua sanidade mental a um novo nível. O Automated Sign-On for Mainframe habilita o login automático até o aplicativo de mainframe, o que elimina a necessidade de os usuários inserirem IDs ou senhas. Imagine só. Não usar mais senhas para mainframe.



1. O emulador inicia uma sessão e solicita as credenciais do usuário para acessar o aplicativo host a partir do Automated Sign-On.
2. O Automated Sign-On solicita um PassTicket de uso único a partir do RACF e o envia de volta ao emulador.
3. O emulador usa uma credencial PassTicket de uso único para efetuar login automático do usuário no aplicativo de host.

Outros produtos complementares de MSS oferecem mais segurança essencial para acesso ao host:

- **Complemento do proxy de segurança de MSS:** entregue a criptografia ponto a ponto e imponha o controle de acesso ao perímetro com a tecnologia de segurança patenteada.
- **Complemento de autenticação avançada de MSS:** permita a autenticação baseada em vários fatores para autorizar o acesso aos seus valiosos sistemas de host.
- **Complemento de login automatizado de PKI de MSS:** habilite o login automatizado pelo PKI aos seus principais sistemas empresariais.
- **Complemento de gerenciamento de ID de terminal do MSS:** aloque dinamicamente as IDs de terminal com base no nome de usuário, nome DNS, endereço IP ou pool de endereços.

O MSS e esses complementos aproveitam seus recursos e infraestrutura existentes, utilizando o que já está implementado para proteger e gerenciar o acesso ao host. Eles oferecem valor de negócios prolongado enquanto reduzem o Custo Total de Propriedade. Dessas maneiras, também oferecem tranquilidade para a segurança empresarial.

Saiba mais em
www.opentext.com

Conecte-se conosco

261-PB0182-002 | O | 02/24 | © 2024 Open Text