CYBER READINESS
INSTITUTE

Guia da autenticação multifator

O Cyber Readiness Institute (CRI) realizou recentemente um inquérito global para avaliar a sensibilização e a implementação da autenticação multifator (MFA) entre as pequenas e médias empresas. Descobrimos que 55% das pequenas e médias empresas (PME) não conhecem a MFA e as suas vantagens em termos de segurança. Com este guia atualizado, procuramos sensibilizar as PME para a MFA ao fornecer informações facilmente digeríveis e acionáveis que poderá implementar hoje para proteger a sua organização da maioria dos ciberataques.

Os cibercriminosos querem comprometer as credenciais de início de sessão e recorrem a diversas técnicas, incluindo fazer-se passar pelo seu banco ou por um parceiro de negócios para as obter de forma fraudulenta. No entanto, exigir que os seus colaboradores utilizem a MFA irá proteger as suas informações e dados empresariais, bem como os dos próprios colaboradores. Com a MFA, a palavra-passe do colaborador deixa de ser a única defesa cibernética da sua empresa. Os hackers que procuram roubar os dados da sua empresa não conseguem simplesmente adivinhar ou violar a palavra passe de um colaborador. Em vez disso, a MFA protege os seus colaboradores e a empresa destes ataques.

Se procura a forma mais eficaz de melhorar a sua cibersegurança atualmente, deverá implementar imediatamente a MFA na sua organização. Embora este guia tenha sido redigido para PME, aplica-se a organizações de todas as dimensões. Segundo a Microsoft, 99,9% dos ataques com contas comprometidas podem ser bloqueados apenas com a MFA. As seguintes orientações ajudam-no a conhecer a MFA e ajudam-no a saber como implementar esta funcionalidade para melhorar a sua cibersegurança e a da sua organização.

O que é a autenticação multifator?

A autenticação multifator, por vezes conhecida como autenticação de dois fatores (2FA), é um processo de autenticação eletrónica que exige que os utilizadores validem a sua identidade de duas ou mais formas antes de concederem acesso a contas online. Normalmente, a MFA enquadra-se em três categorias: algo que sabe, algo que tem ou algo que é. Alguns exemplos de MFA com os quais poderá estar familiarizado incluem:

1. **Autenticação por SMS ou e-mail: Recebe e utiliza um código único por texto no seu telemóvel ou por e-mail para provar a sua identidade.**
2. **Autenticação por software: pode descarregar e utilizar uma aplicação móvel para o seu telemóvel para validar a sua identidade**
3. **Autenticação biométrica: poderá utilizar uma impressão digital ou a leitura facial para validar a sua identidade.**
4. **Notificação push: o seu telemóvel solicita que permita ou bloqueie uma tentativa de início de sessão.**

A minha empresa deve utilizar a MFA?

Sim, o utilizador e todos os colaboradores na sua empresa devem utilizar a MFA em todas as contas ligadas às suas operações empresariais. Por exemplo, deve utilizar a MFA nas contas de e-mail, contabilidade e recursos humanos para proteger os dados dos seus clientes, parceiros e colaboradores. De facto, se alguns serviços ou software que utiliza não tiver MFA, deverá ponderar a mudança para uma alternativa que tenha.

Se um cibercriminoso conseguir obter acesso às suas contas da sua empresa, poderá roubar o seu dinheiro e informações. Poderá bloquear a sua atividade durante vários dias, semanas ou ainda mais tempo. A MFA é uma forma importante de manter o seu sistema seguro contra cibercriminosos.

Quem na minha empresa deve ser obrigado a utilizar a MFA?

Todos. A MFA deve ser obrigatória em todos os dispositivos e serviços da empresa, sobretudo no e-mail e na partilha de ficheiros.

A utilização da MFA altera a nossa necessidade de utilizar palavras-passe fortes?

As palavras-passe fortes são uma forma de autenticação e a MFA baseia-se nelas e noutros métodos (ou seja, código de acesso pontual, impressão digital, etc.). Quer esteja a aceder a e-mails de trabalho, a obter ficheiros a partir de uma unidade partilhada ou a iniciar sessão em quaisquer serviços online, a palavra-passe com outra forma de autenticação inclui a MFA.

O que preciso de ter em conta ao selecionar uma solução de MFA para minha empresa?

É importante ter em consideração alguns fatores chave ao selecionar a solução de MFA adequada para a sua empresa:

1. **A solução é acessível a todos os colaboradores, quer estejam a trabalhar no local ou a partir de uma localização remota?**
2. **Qual o grau de dificuldade de utilização?**
3. **Estão disponíveis recursos de formação para apresentar a solução aos meus colaboradores?**
4. **O fornecedor disponibiliza suporte 24 horas por dia?**

Como posso implementar uma política de MFA na minha empresa?

Em primeiro lugar, o CEO deve designar um responsável para gerir o processo de implementação da MFA, que incluirá uma campanha de mensagens e sessões de formação para os colaboradores. É importante designar alguém na sua organização que aceite a responsabilidade pela preparação cibernética para ajudar os colaboradores a resolver os problemas quando começam a utilizar a MFA.

Em seguida, trabalhe com o responsável para dar prioridade aos sistemas e aos dados que precisam de ser protegidos, decidir qual melhor a tecnologia de MFA para essas necessidades específicas e, finalmente, avaliar o impacto nos colaboradores.

É importante ter em conta que implementar a MFA em toda a organização poderá criar desafios, mas uma boa comunicação permitirá uma implementação bem-sucedida. A realização de sessões informativas e formação dos colaboradores em que são comunicas as suas políticas e expectativas em relação à MFA, e em que explica a facilidade do processo aos colaboradores contribuirão para uma implementação eficaz.

Como posso comunicar a importância da MFA aos meus colaboradores?

Crie uma campanha para informar os colaboradores sobre as vantagens da utilização da MFA e o risco de não o fazer. Poderá utilizar cartazes físicos ou faixas publicitárias nos seus edifícios para explicar os motivos para a transição para a MFA. Concentre-se em informar os seus utilizadores e a explicar os motivos para estar a fazer esta alteração, tornando claro para os colaboradores que a MFA irá ajudá-los e proteger as suas contas, e não será um incómodo ou uma política de monitorização no local de trabalho.

Algum tipo de MFA é mais seguro que os outros?

Estão disponíveis várias opções de MFA para a sua empresa, mas o mais importante é ter em conta que qualquer uma destas opções é melhor do que nenhuma. Tenha em conta a dimensão da sua empresa e o número de colaboradores ao selecionar uma opção de MFA que seja segura mas não demasiado pesada para os colaboradores.

Onde posso obter mais informações?

Agora que tem conhecimentos básicos sobre a importância da MFA para a sua empresa e como a implementar, poderá explorar outras práticas e recursos de prontidão cibernética em BeCyberReady.com. Consulte também as informações gratuitas da CISA para obter mais informações sobre a MFA **aqui.**

Sobre o CRI

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para partilhar recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de iniciação ou crie uma cultura de preparação cibernética na sua empresa com o Programa de preparação cibernética online. Os nossos recursos de teletrabalho e guias de local de trabalho híbrido oferecem sugestões oportunas para lidar com a evolução dos desafios cibernéticos da atualidade. Para saber mais, visite **www.BeCyberReady.com**.