CYBER READINESS
INSTITUTE

Guia de autenticação multifator

Siga estas diretrizes para compreender e implementar a autenticação multifator na sua organização

As pequenas e médias empresas que procuram formas práticas de melhorar a sua cibersegurança devem implementar a autenticação multifator (MFA) na sua organização. 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 (também conhecida como autenticação de 2 fatores, "2FA") e ajudam-no a saber como implementar esta capacidade de melhorar a sua cibersegurança e a da sua organização.

O que é a MFA?

A MFA requer que os utilizadores apresentem mais do que um comprovativo (credencial) sempre que o utilizador iniciar sessão numa conta de empresa (por exemplo, e-mail da empresa, folha de pagamentos, recursos humanos, etc.). Normalmente, a MFA enquadra-se em três categorias: **algo que o utilizador conhece** (palavra-passe de 15 carateres), **algo que o utilizador possui** (impressão digital) ou **algo que o utilizador recebe** (um código enviado para a conta de e-mail ou o telefone do utilizador).

info@cyberreadinessinstitute.com

Por que razão a MFS é importante?

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, ao capacitar os seus colaboradores para utilizar a MFA, protege as suas informações e dados comerciais, bem como os deles.

É fundamental utilizar palavras-passe fortes de 15 carateres, mas **a MFA oferece uma solução técnica centrada nas pessoas**. 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. A **MFA protege os seus colaboradores e a empresa destes ataques**.

Como posso implementar a MFA?

Implementar a MFA não requer mudanças de hardware nos computadores, dispositivos móveis ou impressoras da empresa. Existem várias ferramentas de software gratuitas e de baixo custo que os utilizadores podem transferir para os dispositivos pessoais e da empresa. Por exemplo, é possível que o seu fornecedor de e-mail ofereça (e encoraje) a MFA. Por isso, pode ser tão fácil como clicar numa opção nas definições para ativar a MFA.

Apesar disso, talvez não saiba qual a melhor forma de implementar a MFA na sua força de trabalho. Primeiro, deve **atualizar as políticas e procedimentos com explicações específicas das suas expectativas**. Por exemplo, todos os colaboradores devem implementar a MFA na conta de e-mail da empresa. Em seguida, deve **realizar sessões informativas para os trabalhadores e formação** em que comunique as políticas de MFA, expectativas e explique a facilidade do processo aos colaboradores. Por último, deve **designar alguém na sua organização que aceite a responsabilidade pela preparação cibernética, para ajudar os colaboradores a resolver problemas** quando começam a utilizar a MFA.

Onde posso obter mais informações?

Agora que tem conhecimentos básicos sobre a importância da MFA para a sua empresa e como a implementar, pode explorar outros recursos de preparação cibernética e práticas em **BeCyberReady.com**.

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**.