SISTEMA DE SEGURANÇA DE SENHAS

Senhas ou palavras-chaves são a forma mais comum de verificar a identidade de alguém e, por isso, merecem uma atenção a mais. Tanto na criação quanto na manutenção de uma senha são necessários alguns cuidados que, se forem ignorados, podem trazer uma série de problemas de segurança depois. Em outras palavras, ter uma senha fraca ou não saber como mantê-la secreta é o mesmo que não ter senha nenhuma.

A maioria das pessoas, incluindo aí especialistas em segurança, tem senhas insuficientemente seguras. Não entendem que senhas como a data de aniversário ou qualquer outra informação referente à pessoa, alguma palavra do dicionário de qualquer língua, mesmo que digitada ao contrário ou com substituição de vogais por números, são tão óbvias para elas quanto para qualquer pessoa. E podemos incluir nessa lista de senhas inseguras o uso do próprio nome de usuário, letras ou números em sequência ou ainda um mesmo caractere repetido várias vezes. Ou seja, os usuários geralmente abrem mão da segurança da empresa pela sua própria conveniência, o que torna necessária uma política de senhas, pois é inconcebível que qualquer informação ou serviço importante para uma organização seja colocado em risco só porque um funcionário preguiçoso utilizou como senha o nome do time de futebol.

Uma boa senha é aquela que tem pelo menos oito caracteres (quanto mais, melhor) e combina letras maiúsculas, minúsculas, símbolos, números e caracteres especiais de forma aleatória, sem sentido. Pode-se por exemplo escolher uma frase ou um trecho de música e utilizar a primeira letra de cada palavra, com caracteres e números no meio. Isso torna a senha fácil de ser lembrada e impossível de ser adivinhada. No entanto,

mesmo que leve muito tempo, essa senha ainda pode ser quebrada e, para evitar que isso aconteça, precisa ser substituída por outra regularmente, a cada três meses, por exemplo. Para descobrir senhas, hackers podem utilizar programas de força bruta (testam todas as combinações possíveis de caracteres) ou de dicionário (testam listas de palavras), de preferência executados localmente, evitando assim sua exposição a sistemas de detecção de intrusos.

Ainda que pareça óbvio dizer, senhas individuais foram criadas para serem secretas, então, não devem ser ditas a ninguém e nem escritas (a displicência é tão grande que muitos funcionários escrevem a senha em uma notinha e a deixam colada na tela do computador). Para piorar, há aqueles que usam a mesma senha em tudo. Isso não deve ser feito, pois caso a senha seja roubada, mais de um recurso do sistema será comprometido. Senhas também não devem ser armazenadas em dispositivos móveis, a menos que isso seja feito com algum método seguro e aprovado pela direção. Outro erro é o uso de senhas padrão, que já vêm configuradas com softwares e hardwares: pois se é padrão, todo mundo conhece. Dentre outros fatores que facilitam a ação dos hackers está a utilização de memorização automática de senha, que é bastante comum em navegadores de Internet, e a utilização de uma mesma senha com finalidade profissional e pessoal.

De fato, as organizações não podem esperar que os usuários por livre e espontânea vontade adotem os procedimentos corretos. É tão certo que eles cometerão falhas no uso de senhas, que se torna imprescindível que assinem algum tipo de declaração no ato da contratação que os deixem cientes de suas responsabilidades e os obriguem a agir de acordo com a política de segurança interna.

Não se pode jogar, entretanto, toda a responsabilidade para os funcionários. As organizações em geral também cometem uma série de erros como: não verificar a identidade de um usuário antes de fornecer uma senha a ele, enviar senhas sem criptografia por e-mail, não confirmar o recebimento da senha, fornece senhas padrões ou fáceis de adivinhar, não obrigar a alteração da senha logo após a instalação

de um software, não revisar os direitos de acesso de usuários após mudança de atividade ou fim de contrato ou mesmo para ver se há privilégios indevidos, não registrar os acessos e as concessões de senhas, não alterar senhas após comprometimento do sistema, não treinar seus funcionários contra ataques de engenharia social, não bloquear a senha após algumas tentativas erradas, permitir que sistemas operacionais armazenem senhas em cache(o que traria a possibilidade de um funcionário mal-intencionado capturar a senha de um técnico com privilégios de administrador chamado para reparar algo no sistema) e não remover arquivos de instalação (se alguém instala um sistema novamente a configuração volta a ser default, assim como a senha).

Felizmente, desde que bem utilizadas, ferramentas de armazenamento e gerenciamento de senhas podem solucionar algumas dessas questões. Devem ser confiáveis, usar criptografia, obrigar a escolha de senhas de qualidade e a troca periódica, manter um registro de senhas anteriores e vetar sua reutilização, não mostrar na tela as senhas quando forem digitadas, possibilitar que os usuários modifiquem sua senha e confirmem, identificar os usuários com um nome de usuário e uma senha e unir conveniência e proteção. O problema é que nem sempre essas ferramentas estão disponíveis, o que às vezes torna necessária a memorização da senha.

Ao passo que a maioria das informações é protegida por senhas, não é nenhum exagero que muitas organizações optem por definir as senhas de seus empregados.