Por Fernando Amatte (*)

Redes sociais, e-mails, lojas online, armazenamento na nuvem, tanto no universo corporativo quanto no pessoal, são muitos os serviços utilizados diariamente que solicitam logins e senhas para acesso nos quais, na maioria das vezes, os usuários optam pela facilidade de utilizar os mesmos dados.

Nos últimos anos, temos visto diversos casos de ataques cibernéticos a grandes empresas, como o Linkedin, Last.fm, Ashley Madison, Sony e (recentemente) Dropbox, a fim de conseguir as senhas e dados valiosos dos usuários. Estes vazamentos de informações e falhas de segurança são cada vez mais comuns, empresas e usuários devem estar atentos aos riscos que correm, principalmente pelo mau hábito de se usar e-mail corporativo em sites públicos e senhas iguais em diversos cadastros. Com um vazamento público alguém pode ter acesso aos dados privados da empresa.

A lógica é simples, os hackers sabem do mau hábito do compartilhamento de senhas e e-mail e podem tentar obter acesso aos sistemas de uma companhia ou mesmo outros serviços do usuário testando e-mails e senhas vazados por um site público.

Um estudo recente publicado pelo Instituto Ponemon com cerca de 3 mil trabalhadores que atuam em organizações dos Estados Unidos e Europa, revela que o comportamento dos funcionários é o maior fator para exposição de informações nas empresas. Apenas 39% dos empregados entrevistados afirmaram que tomam todos os passos necessários para proteger informações corporativas.

Na maioria das vezes, as pessoas menosprezam as consequências do que pode acontecer ou não têm noção de quanto valem os dados que elas guardam. Por incrível que possa parecer, senhas sequenciais do tipo "123456" estão sempre entre as mais utilizadas, reforçando a tese de que as pessoas não dão importância à segurança.

Pense o seguinte: o valor do cofre é diretamente proporcional ao bem guardado dentro dele. Logo, é comum o uso de senhas seguras ou complexas em lugares que consideramos guardar algo valioso, como em bancos. O maior problema talvez seja o fato de que as pessoas não tenham conhecimento do valor (monetário ou sentimental) que suas informações têm, até que elas sejam perdidas.

Mas afinal, o que são senhas seguras?

As senhas ainda são compostas por elementos que o usuário se lembre. Usar uma para cada lugar é bem difícil de memorizar e, deste modo, infelizmente algumas situações compactuam para o uso de informações públicas. Por exemplo, quando te pedem uma senha de 4 dígitos, as primeiras coisas que vem à cabeça são o final de um número telefônico, a sequência numérica da placa de um carro ou uma data (dia/mês ou ano).

Uma senha é tão segura ou forte quanto o tempo que se leva para “descobri-la”. O primeiro passo de um hacker são as tentativas de sequências de números ou letras que tenham a ver com a vida da pessoa, tais como: datas significativas (da pessoa ou de próximos), nomes de conhecidos, lugares, times de futebol etc. Sendo assim, o “atacante” começa estudando o “atacado”, montando uma lista com palavras e números, o que se chama de ataque de dicionário. Caso não dê certo, inicia-se o ataque de força bruta em que todas as combinações de letras e números são tentadas sistematicamente (Ex: aaa, aab, aac, aad...).

Para se ter uma ideia da complexidade desse processo, utilizando as 26 letras do alfabeto e contando somente as letras minúsculas, teríamos duzentas e oito bilhões (208.827.064.576) de

combinações para uma senha de oito caracteres (268). Se testássemos uma senha por segundo, levaríamos 2.416.979 dias para testar todas as senhas, aproximadamente 6.621 anos ininterruptos.

Já os computadores podem testar milhares ou milhões de senhas por segundo. Dentro das empresas, provavelmente os sistemas estejam configurados para bloquear um usuário depois de três ou cinco tentativas erradas de senha, visando evitar ataques de dicionário ou ataques de força bruta. Mas, quando existe o vazamento de algum banco de dados o atacante pode testar quantas senhas desejar, pois o atacante controla seu próprio ambiente e não está sujeito às restrições de um ambiente corporativo (ataque offline).

Então, não se esqueça de seguir algumas dicas valiosas:

- Nunca utilize senhas que seguem sequências;
- Utilize letras maiúsculas e minúsculas;
- Não as anote, memorize-as;
- Inclua caracteres especiais;
- Não utilize a mesma senha para diversos serviços.

Ainda que a segurança esteja relacionada à qualidade da senha utilizada, a criptografia dos dados pode ser uma grande forma de ajudar os CSOs (Chief Security Officer) a manterem dados em segurança. Se o problema for memorizar senhas, consulte especialistas para indicar quais são as ferramentas ideais para centralizar a administração, essas soluções armazenam senhas usando bancos de dados com criptografia avançada e uma senha-mestra, que dará acesso a todas.

Como não existem leis relacionadas à responsabilidade do vazamento de senhas no Brasil, raramente sabemos o que vazou, então o empresário brasileiro ainda está pouco atento a este problema. O que falta ainda é uma cultura preventiva e efetiva do comportamento de uso e acesso à informação, pois as tecnologias para combater vazamento de informação e ameaças estão sofisticadas e atendem às principais demandas de proteção.

(*) **Fernando Amatte** é gerente de pré-vendas da Cipher.

Fonte: ComputerWorld, em 20.09.2016.