Boas práticas em Cibersegurança

Suas senhas são fortes...? Mesmo?

Quando se fala de senhas, a recomendação é muito clara: devem ter pelo menos 8 caracteres, dentre letras maiúsculas e minúsculas, números e caracteres especiais. Você já parou para se perguntar o motivo desta recomendação? Obviamente, uma senha que segue estes padrões é mais difícil de ser "adivinhada". No entanto, mesmo que um hacker não consiga "adivinhar" a sua senha baseado em premissas (a partir, por exemplo, do seu nome, da sua data de nascimento e de outras informações pessoais), ainda assim é possível "quebrar" a sua senha. Isto pode ser feito através de um método denominado "força bruta".

Apesar do nome engraçado, o método não consiste em bater no computador com um pedaço de pau até que ele revele a senha alvejada. Força bruta consiste em tentar, virtualmente, todas as combinações de caracteres possíveis para uma senha, até que, num golpe de sorte, a senha verdadeira seja encontrada.

Se pararmos para pensar um pouco, podemos levantar alguns números a respeito do assunto. Por exemplo: supondo que utilizemos apenas letras minúsculas para formar uma senha de 8 caracteres, quantas senhas possíveis poderíamos formar?

Simples. Dado que o nosso alfabeto tem 26 letras (se considerarmos o "k", o "w" e o "y"), poderíamos formar até:

$$26 \times 26 \times 26 \times 26 \times 26 \times 26 \times 26 \times 26 = 208.827.064.576 \text{ senhas}$$

"Traduzindo", isso dá algo da ordem de 209 bilhões de senhas possíveis. Este número pode parecer grande, mas um computador "normal", muito parecido com este que você provavelmente está utilizando, levaria **meros segundos** para encontrar uma senha assim definida.

Se acrescentássemos letras maiúsculas, dobraríamos o espaço de possibilidades para cada caractere de nossa senha fictícia (portanto, no lugar de 26, 52 letras poderiam ser utilizadas em cada posição). Assim, poderíamos formar até:

$$52 \times 52 \times 52 \times 52 \times 52 \times 52 \times 52 \times 52 = 53.459.728.531.456 \text{ senhas}$$

Ou algo em torno de 53 trilhões de senhas possíveis. Já melhoramos um pouquinho. Um computador normal levaria **alguns minutos** para encontrar uma senha assim definida, isto é, com 8 caracteres, entre letras maiúsculas e minúsculas.

Ainda assim, algo da ordem de minutos é um tempo muito curto. Você estaria disposto a arriscar definir uma senha que pudesse ser encontrada em, digamos, meia hora?

Peralis
IT Innovation

Boas práticas em Cibersegurança

Podemos melhorar ainda mais a nossa senha acrescentando números a ela. Com isso, aumentaríamos o nosso espaço de possibilidades, para cada posição, de 52 caracteres para (52 + 10) = 62 caracteres. Neste caso, quantas possibilidades de senha um hacker teria que testar para garantir que vai encontrar a nossa senha fictícia? A resposta é:

$$62 \times 62 \times 62 \times 62 \times 62 \times 62 \times 62 \times 62 = 218.340.105.584.896 \text{ senhas}$$

Trocando em miúdos, 218 trilhões de senhas possíveis. Continuando nosso exercício, um computador normal levaria **algumas horas** para encontrar uma senha assim.

Finalmente, se acrescentássemos caracteres especiais à nossa senha teríamos, então, *um número tão grande de possibilidades que nem vale a pena tentar escrever numa única linha*. Podemos esperar que um computador normal levasse cerca de **um ano** para conseguir encontrar uma senha de 8 caracteres contendo letras maiúsculas e minúsculas, números e caracteres especiais.

Provavelmente, um ataque de força bruta a uma senha assim se traduziria em mais esforço (e mais dinheiro) do que a informação protegida por ela vale. **Em outras palavras, para chegar ao ouro, estaríamos gastando mais dinheiro para cavar do que o próprio ouro vale.** Simplesmente não compensaria. Ademais, a maior parte dos mecanismos de autenticação "travaria" a conta que se está tentando acessar depois de algumas poucas tentativas de acesso inválidas.

Obviamente, se a informação protegida por uma senha é de valor *inestimável*, vale a pena utilizar senhas ainda mais seguras. No entanto, este não é o caso para a maior parte dos serviços que utilizamos no dia a dia e senhas de 8 caracteres (letras maiúsculas e minúsculas + números + caracteres especiais) são suficientes.