CRÓNICA VISÃO ELECTRÓNICA
Nº 259 / 2014-01-02
http://www.gestaodefraude.eu
Edgar Pimenta

>> A (difícil) arte de escolher uma *password*

Quando acedemos a um *site*, a um computador ou a alguma aplicação podemos ter que comprovar a nossa identidade, apresentando para isso as credenciais de acesso. Esse processo designa-se de autenticação.

Este processo de autenticação baseia-se sobretudo em duas informações: utilizador e palavras-passe (vulgo *password*). Quando acedemos a um *site*, podemos ter de introduzir estas credencias para aceder à nossa conta.

No entanto, algo que se sabe pode ser descoberto (inferido) por terceiros, sobretudo porque tendemos a usar todos o mesmo tipo de esquemas mentais para escolher *passwords*, nomeadamente através da utilização de informação pessoal. Algo que se sabe pode também ser facilmente "partilhado" com terceiros. Por isso, a autenticação baseada em algo que "eu sei" é considerado um dos métodos de autenticação mais falível.

Outros métodos de autenticação podem basear-se em algo que "eu tenho" – por exemplo, um cartão – ou algo que "eu sou" – impressão digital, leitura da íris. Estes métodos, embora mais robustos em termos de segurança, podem ser de implementação mais complicada ou onerosa.

Obviamente, quanto mais métodos em simultâneo se usarem, mais robusto é o processo de autenticação. Quando se usa, por exemplo, algo que sabemos e algo que temos, estamos a fazer uma autenticação com dois elementos (*two-factor authentication*). Um excelente exemplo é a utilização de caixas multibanco: autenticamo-nos com algo que temos (o cartão MB) associado a algo que sabemos (o PIN).

Mas voltemos às passwords, pois são o método de autenticação mais usado e é sobre elas que teceremos algumas considerações.

Dizem as boas práticas que uma password apresente, nomeadamente, as seguintes regras (que idealmente existem cumulativamente mas podem também existir individualmente):

CRÓNICA VISÃO ELECTRÓNICA
Nº 259 / 2014-01-02
http://www.gestaodefraude.eu
Edgar Pimenta

1: Deve ter pelo menos 8 caracteres

Atenção que nem todas as combinações de oito caracteres são convenientes: "12345678" é muito comummente utilizada. Qualquer data (nascimento do próprio ou familiar, casamento, etc..) permite também cumprir com este requisito e são, por isso usadas com excessiva frequência. Usar "password" como *password* é também algo já muito visto.

2: Deve misturar letras e números

Quando esta regra existe, as *passwords* mais comuns passam por colocar um nome (ou alcunha) seguido do respectivo ano de nascimento. Ou o clube de futebol e o ano do último campeonato ganho, etc... Já sabe que estas são combinações a evitar.

3: Deve ter maiúsculas e minúsculas

A forma mais comum passa por colocar como maiúscula a primeira letra. Mais uma vez, o melhor será optar por colocar como maiúscula outra(s) letra(s) para além (em vez) da primeira.

4: Deve ter caracteres não alfa-numéricos

É nesta altura que começamos a pensar quem é que inventou estas regras, para que servem, etc..., e começamos sem saber o que fazer... colocar um "+" a separar o nome do ano é uma hipótese... De forma mais elaborada começamos a pensar em substituir o "S" por "$" ou o "l" por "1" ou "!". Afinal, ninguém se havia de lembrar disso...

Finalmente, cumprindo as regras lá conseguimos criar uma *password*!

Mas dizem também as boas práticas que as *passwords* devem ser alteradas periodicamente. E a nova deve ser bastante diferente da anterior. Agora apetece mesmo colocar a *password* num post-it para não esquecer (o que é, obviamente, totalmente desaconselhado).

E se multiplicarmos esta exemplificação pelas dezenas (senão centenas) de aplicações, sites e sistemas onde temos de usar passwords, e considerando que as mesmas devem ser diferentes em cada um deles, torna-se complicado ter memória para tanto.

CRÓNICA VISÃO ELECTRÓNICA
Nº 259 / 2014-01-02
http://www.gestaodefraude.eu
Edgar Pimenta

E qual a solução para criar e gerir *passwords*?

Existem várias e a sua aplicação depende de vários fatores.

- Para construir *passwords* mais robustas, um dos métodos mais frequentes é a escolha de uma frase da qual se seleciona o primeiro caracter de cada palavra: "O meu Ferrari vai dos 0 aos 100 em 6 segundos!" -> "OmFvd0a1e6s!".
- Para facilitar a alteração periódica das *passwords*, poderá ser usado um texto que nos seja familiar. E quando for necessário mudá-ls, passa-se para a frase seguinte.
- Para mudar periodicamente de *password*, pode ser usado algum tipo de mnemónica que permita não a esquecer. Por exemplo, ser composta por um país e a sua capital, seguida do mês que foi alterada e com um ponto de exclamação (ex: Portugal!Lisboa12). Quando for preciso alterar a *password*, segue-se os restantes países e capitais da Europa.
- Outra solução passa por usar *passphrases* em vez de *passwords*. As *passphrases* consistem em frases normais ao invés de palavras: "As armas e os barões assinalados!"
- São mais fáceis de decorar e são bastante robustas. No entanto, apresentam algumas desvantagens: nem todos os sistemas permitem *passphrases* e a sua introdução em alguns equipamentos (ex: *tablets* e *smartphones*) não é muito prática (expedita).
- Para arquivo das *passwords*, existem ferramentas específicas. Algumas também permitem gerar *passwords* aleatórias. Qualquer que seja a aplicação usada, a *password* master que dá acesso a todas as outras deve ser muito robusta já que é o ponto de partida de todas as restantes.
- Quando possível, deve ser utilizado o *two-factor authentication*. Existem já alguns sites que utilizam aplicações do telemóvel para permitir a respetiva autenticação, ou pens USB desenhadas pera o efeito.

Como uma obra de arte é específica, pessoal, imaginativa e complexa, assim também o é mudar periodicamente de *password*. Que cada um utilize a sua criatividade para construir um método que

CRÓNICA VISÃO ELECTRÓNICA
Nº 259 / 2014-01-02
http://www.gestaodefraude.eu
Edgar Pimenta

funcione e que garanta que aquela é robusta, variada e diferente. Mas a arte também é técnica, pelo que se conseguir conjugar a *password* com outros métodos de autenticação, ainda melhor.