27/01/2014 - Morte da senha: prepare-se!

Por Phil Scarfo*

É difícil acreditar que em plena Era Digital continuamos sendo obrigados a confiar em um método de autenticação desenvolvido há mais de 50 anos e que se baseia principalmente na memorização de números e letras combinados. Já não era simples quando, no início, tínhamos de decorar uma, duas ou três senhas. Como tudo à nossa volta se transformou nestas últimas décadas, a quantidade de senhas e a complexidade delas também aumentou consideravelmente. Hoje em dia, é praticamente impossível memorizar todas as combinações – e as pessoas acabam anotando em tudo quanto é lugar, aumentando sua vulnerabilidade também.

Nos anos 60, quando foram criadas, as senhas eram usadas em locais bastante restritos, terminais dedicados, com conexão por fio e dentro de um espaço corporativo bem limitado. Ao serem apresentadas ao mundo, o universo da computação era bem menor do que o que temos hoje dentro de um único smartphone. Hoje, um número incrível de pessoas têm acesso à telefonia celular – mais do que têm acesso a água potável e energia elétrica. Até 2017, para se ter uma ideia, o m-commerce atingirá 3,2 trilhões de dólares. Já as operações bancárias online devem alcançar 894 milhões de pessoas em 2015. E só a receita dos anúncios comercializados no Google supera toda a indústria da mídia impressa nos Estados Unidos.

O fato é que o mundo mudou dramaticamente nas últimas décadas. Então, por que continuamos confiando em métodos de autenticação que não são nem seguros, nem convenientes? No cabo de guerra entre segurança e comodidade, esta última geralmente sai ganhando. Num exemplo extremo, as senhas necessárias para disparar mísseis nucleares dos Estados Unidos durante a Guerra Fria foram definidas em 00000000 para garantir que não haveria perda de tempo nem erros durante a digitação.

Em situações mais comuns, embora as senhas não fossem consideradas o método mais seguro, pelo menos eram convenientes e, certamente, mais fáceis de serem implantadas na maioria das organizações. Não exigiam grande empenho nem impunham barreiras tecnológicas. Para adicionar um véu de segurança, bastava fornecer um nome de usuário e uma senha para ter acesso a ambientes protegidos.

Sendo assim, não temos de questionar se o uso de senhas está obsoleto. O mais importante é saber o que é necessário para aumentar o nível de segurança, conveniência e privacidade – substituindo, então, as senhas. Com mais de um bilhão de pessoas hoje com acesso à banda larga (incrível, mas eram apenas 38 milhões em 1999), estamos num ponto de inflexão em que um aplicativo seguro (ou aplicativos) num dispositivo inteligente (um smartphone, por exemplo), combinado com uma solução biométrica, será toda tecnologia necessária para a próxima geração, provendo autenticação segura e conveniente.

Isto não quer dizer que a biometria utilizada deva ser parte integrante do dispositivo inteligente, mas certamente é uma opção. Com credenciais seguras sendo armazenadas de forma igualmente segura e transmitidas por NFC (Comunicação de Campo Próximo), Bluetooth, ou qualquer outro meio num dispositivo inteligente, há condições convenientes e seguras para uma ‘chave digital inteligente’ – que, ao encontrar uma ‘fechadura digital inteligente’, que pode ser um caixa eletrônico com sensor biométrico, ou ainda um serviço online, é possível finalmente entregar a solução simplificada que as pessoas anseiam hoje em dia.

Todos precisamos de segurança, mas o que desejamos mesmo é conveniência. Ninguém quer enfrentar um passo a passo muito difícil nem ser exigido demais sempre que precisa ter acesso a um ambiente seguro. Não se trata de uma gincana. Nesse quesito, o Brasil está bastante avançado, principalmente em se tratando de sistema bancário. Hoje, grande parte dos caixas eletrônicos tem sensores biométricos que facilitam muito o acesso da população à conta corrente. Trata-se, inclusive, de uma solução em que ambas as partes saem ganhando. Enquanto o cliente tem acesso fácil e seguro à sua conta bancária, o banco também está mais protegido contra fraudes e perdas financeiras. Com esse modelo em que todas as partes saem ganhando, é possível antever a morte das senhas. Prepare-se!

* Phil Scarfo é vice-presidente comercial e de marketing da Lumidigm. Com sede em Albuquerque, no Novo México (Estados Unidos), a Lumidigm oferece sensores biométricos com imagem multiespectral e equipamentos de soluções visuais opticamente aprimoradas que atendem às necessidades de clientes do mundo inteiro em termos de controle de acesso físico e lógico em mercados como bancos, instituições de saúde, de ensino, entretenimento, além da identificação civil e governamental. www.lumidigm.com

Press Página