09/04/2013 - Segurança: a batalha sem fim entre medidas de proteção e medidas defensivas

*Por Phil Scarfo**

Desde que existem sistemas de segurança destinados a nos proteger, há também aqueles com o único propósito de derrotá-los. A triste verdade é que nós sabemos com certeza que qualquer sistema em uso hoje para impedir o acesso não autorizado ou detectar uma identidade fraudulenta é vulnerável a ataques. E que nenhum sistema, não importa quão bem projetado, é totalmente seguro por muito tempo.

Sabemos também que empresas e prestadores de serviços pertencem a uma de duas categorias: aqueles que sabem que estão sendo hackeados e os que não sabem que estão sendo hackeados. Infelizmente, todos são vulneráveis e suscetíveis a ataques. Então, a única diferença entre eles é o que fazem a respeito, que medidas podem tomar para se posicionar um passo à frente nesse interminável jogo de “gato e rato” em termos de segurança.

Ironicamente, vivemos em um mundo de complexidade cada vez maior. Temos mais e mais transações entre pessoas e máquinas. Isso significa que temos um número crescente de identidades virtuais e múltiplas formas de identificação pessoal. Embora o risco seja muito maior hoje, continuamos a depender fortemente de métodos e de uma tecnologia introduzida mais de 60 anos atrás: senhas e códigos.

Temos tornado tudo tão mais complexo que praticamente não é mais possível memorizar todos eles. Nós anotamos e os hackers invadem nossos sistemas e se apropriam dos nossos dados. E os riscos também vão ficando maiores. Vieram os smart cards, os tokens de identificação e as senhas de uso único (OTP). Mas, mais uma vez, alcançamos um nível de segurança temporária. Esse nível é que vem sendo mais e mais aumentado através de inovações e tecnologias avançadas.

Assim também ocorre no campo da biometria, onde a promessa era substituir a autenticação do indivíduo pelo que ele tem ou sabe por “quem” ele é. Infelizmente, ainda muitas dessas tecnologias têm sido comprometidas por vulnerabilidades e ataques fraudulentos.

Portanto, a questão é: Para onde vamos a partir daqui? Como é que uma organização ou uma pessoa se protege de um ataque inevitável? Guardadas as devidas proporções, a resposta é: transformando a segurança em algo em camadas. Isto é, criando uma condição em que vários fatores ou formas de autenticação são utilizados para aumentar o nível de segurança. A autenticação eficiente é, por natureza, mais forte porque há dois, ou talvez três fatores de autenticação acoplados, de tal modo que se qualquer um deles for comprometido ainda estará protegido pelo outro.

Também é necessário garantir que o sistema ou a tecnologia adotada possa ser melhorada ou adaptada para lidar com as novas vulnerabilidades e novas ameaças que vão se tornando conhecidas. Assim como a indústria de vírus de computador está se aprimorando continuamente, adicionando e alterando mecanismos de proteção para responder a novas ameaças e vulnerabilidades conhecidas, também no segmento de identificação pessoal deve ser feito o mesmo.

Felizmente, existem soluções disponíveis projetadas para enfrentar tais desafios e que podem se adaptar para fornecer autenticação multifatorial em um único dispositivo, o que aumenta a

barra sem aumentar a complexidade ou risco para o usuário. Graças a uma tecnologia chamada “imagem multiespectral”, um único dispositivo biométrico pode autenticar de forma confiável uma ampla gama de usuários, sob uma ampla gama de condições ambientais.
A imagem multiespectral também é a única capaz de discriminar de forma muito mais consistente o dedo uma pessoa de verdade de um artefato fabricado com fins fraudulentos. A imagem multiespectral também é a única capaz de autenticar pessoas e outras formas físicas de autenticação, como um código de barras impresso, uma credencial de identificação, ou até mesmo uma credencial virtual ou código digital em um dispositivo inteligente.
Tudo isso pode ser feito em um único dispositivo. A imagem multiespectral também é única ao oferecer aos usuários uma autenticação singular ou multifatorial: a autenticação biométrica ou a combinação da autenticação biométrica com algum outro tipo de identificação. O importante é sua capacidade de modificar, atualizar e responder a novas vulnerabilidades e novas ameaças, atualizando o nível de segurança e se provando um investimento de longo do tempo.
Em resumo, nenhuma forma de autenticação é 100%. Nenhum método de autenticação do usuário pode garantir 100%. Para realmente atingirmos uma autenticação totalmente segura é preciso investir numa tecnologia multifatorial, em que não há dependência de um único fator para obter 100% de segurança. Por isso, a tecnologia deve ser adaptável – a fim de se provar confiável e eficiente ao longo do tempo.

*Phil Scarfo é vice-presidente sênior de vendas e marketing mundial da Lumidigm (www.lumidigm.com).

Press Página