A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

Nesta edição

- O Problema
- A Solução
- Um Exemplo

Autenticação por Dois Fatores

EDITOR CONVIDADO

Fred Kerby é o editor convidado para esta edição. Ele é um ex-gerente da segurança de informação da Naval Surface Warfare Center Dahlgren Division. Ele também é um Instrutor SANS sênior e líder para o curso Introdução à Segurança da Informação (SEC301 - Information Security course). Fred também ensina Liderança na Segurança da Informação (MGT512 - Information Security Leadership) e Fundamentos de Segurança (SEC401 - Security Essentials).

O PROBLEMA

Para usar muitos dos serviços da internet hoje, como e-mail, banco online ou compras online, você deve primeiro provar que você é quem você diz ser. Este processo de provar a sua identidade é conhecido como autenticação. A autenticação é feita usando algo que você sabe (como sua senha), algo que você tem (como o seu smartphone), ou algo exclusivo de você (como mapeamento da retina ou impressão digital). Tradicionalmente uma das formas mais comuns de autenticação tem sido um nome de usuário e uma senha. O problema de usar apenas uma senha para autenticação é simples: tudo o que um atacante precisa fazer é adivinhar ou obter a sua senha para ganhar acesso instantâneo à sua conta e suas informações. Se você usar o mesmo nome de usuário e senha para várias contas, o dano pode ser muito maior ainda. Para proteger melhor as suas contas online, os sites de internet estão disponibilizando métodos de autenticação mais fortes que requerem o uso de mais de um fator para autenticar. Vamos explicar o que é isso, como funciona e por que você deve usá-lo.

A SOLUÇÃO

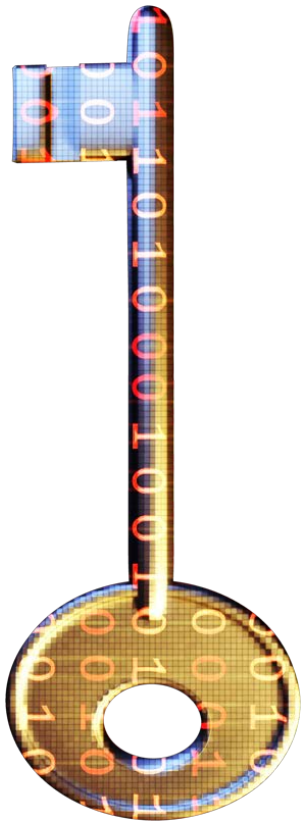
Autenticação mais forte usa maisde um fator. Você não só tem que saber algo como a sua senha, mas tem que ter algo (como o seu smartphone) ou apresentar algo exclusivamente seu (como sua impressão digital). Autenticação por dois fatores é exatamente o que diz, você precisa de dois fatores para provar quem você é, em vez de apenas um. Um exemplo comum de autenticação por dois fatores é o seu cartão do Banco. Para acessar seu caixa eletrônico você precisa ter alguma coisa (o seu cartão do Banco) e você precisa saber alguma coisa (a sua senha). Se um atacante rouba o seu cartão do Banco, isso não lhe servirá pra nada, a menos que também saiba a sua senha (o que explica a recomendação de não escrevê-la no cartão). Ao exigir dois fatores de autenticação você está mais protegido, ao invés de apenas um.

Autenticação por Dois Fatores

A autenticação por dois fatores online funciona de forma semelhante ao seu cartão e senha do Banco, combinados. Você usa o seu nome de usuário e senha quando quer acessar suas contas online. No entanto depois de digitar corretamente sua senha, em vez de ir diretamente para sua conta,o site pede um segundo fator de autenticação, como um código de verificação ou sua impressão digital. Se você não tem o segundo fator, o acesso não é concedido. Este segundo passo protege você. Se um atacante obteve sua senha, você e sua conta ainda estão seguros pois o atacante não pode completar o segundo passo sem ter o segundo fator.

EXEMPLOS

Vamos examinar um exemplo de como a autenticação por dois fatores funciona. Um dos serviços mais utilizados online é o Gmail. Muitas pessoas autenticam a sua conta do Gmail ou de outros serviços do Google com seu nome de usuário e senha. O Google agora oferece maior segurança com autenticação por dois fatores, ou o que o Google chama de "Verificação em duas etapas". A "Verificação em duas etapas" do Google exige duas coisas para a autenticação: sua senha (algo que você sabe) e seu smartphone (algo que você tem). Para provar que você tem o seu smartphone, o Google vai solicitar que você digite um código de verificação, válido para uma utilização apenas, que será enviado a você por SMS (note que as tarifas de SMS/Torpedos podem ser aplicadas - verifique seu plano com sua operadora de celular para confirmar). E você, então, digita esse código. Além disso, se você preferir, em vez de usar o envio de código via SMS pelo Google, você pode instalar um aplicativo no smartphone que gera o código exclusivo para você.



Use autenticação por dois fatores, sempre que possível. Ela é uma das alternativas mais fortes de proteger o acesso às suas contas e informações.

Assim você não precisa sequer do acesso à sua operadora, apenas do seu smartphone. O valor desta autenticação mais forte é que mesmo que um atacante tenha obtido sua senha do Google, ele não poderá acessar suas contas do Google, a menos que também tenha acesso físico ao seu smartphone. Você e suas informações valiosas estão protegidos.

Autenticação por Dois Fatores

Tenha em mente que os códigos de verificação enviados para o seu smartphone são únicos - eles serão diferentes a cada vez que se autenticar. Por isso você terá que passar por este processo de duas etapas sempre que autenticar sua conta Google. Além disso, este recurso não é habilitado por padrão. Para ativá-lo, faça login na sua conta do Google, entre em Configurações -> Contas e Importação -> Outras Configurações da Conta do Google -> Segurança e clique na opção Editar do item "Verificação em duas Etapas". Siga então as instruções para configurar.

Outros sites online também oferecem autenticação por dois fatores, como o Dropbox, Paypal ou talvez até mesmo o seu banco. Alguns desses serviços podem ter suporte para seu smartphone, enquanto outros, como o PayPal, pode lhe enviar um token (semelhante aos usados por alguns bancos) para gerar seus códigos de verificação únicos. Outros sites podem usar dispositivos especiais que se conectam à portaUSB do seu computador, como Yubikey. Se qualquer um dos serviços que você usa oferece autenticação por dois fatores, recomendamos fortemente que você ative e use.

FONTES

Alguns destes links foram encurtados para melhor legibilidade usando o serviço TinyURL. Para reduzir problemas de segurança, OUCH! Sempre usa o recurso de visualização doTinyURL, que mostra o destino final do link e pede sua permissão antes de proceder a ela.

Google Verificação de duas etapas:
http://preview.tinyurl.com/cncte9n

PayPal (e EBay) Security Key:
http://preview.tinyurl.com/838dpds

CERT.br – Glossário de segurança:
http://cartilha.cert.br/glossario/

Dica de segurança SANS do Dia (em Inglês):
http://preview.tinyurl.com/6s2wrkp

SAIBA MAIS

Assine a publicaçãomensal OUCH! de sensibilização de segurança, acesse os arquivos OUCH! e aprenda mais sobre as soluções de sensibilização de segurança do SANS nos visitando em http://www.securingthehuman.org.

VERSÃO BRASILEIRA

Traduzida por:
Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Marcello Belloni Gomes, Arquiteto de Segurança de TI - twitter.com/marcellobelloni
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutoraautônoma

Time Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner