OUCH! | Agosto de 2014

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Criptografia

O que é criptografia?

Você talvez ouça as pessoas usando o termo “criptografia” e como devemos utilizá-la para proteger a nós mesmos e nossas informações. No entanto, o conceito de criptografia pode parecer confuso. Além disso, a criptografia não pode protegê-lo de tudo, tem suas limitações. Nesta publicação vamos explicar em termos simples o que é a criptografia, por que você deve utilizá-la e como implementá-la corretamente.

Editor Convidado

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) é consultor da região de Washington, DC. Ele é o principal instrutor do curso em Segurança de Dispositivos Móveis e Hacking Ético (SEC575) do Instituto SANS e autor de Gerenciamento do Time de Respostas a Incidentes (MGT535).

Você tem uma quantidade enorme de informações sigilosas em seus dispositivos, tais como documentos financeiros, imagens, e-mails, ou registros médicos. Se você tivesse um de seus dispositivos perdido ou roubado, toda essa informação sigilosa poderia ser acessada por qualquer um que tivesse acesso ao seu equipamento. Além disso, você pode realizar transações confidenciais on-line, tais como os serviços bancários ou as compras online. Se um criminoso cibernético estivesse monitorando suas atividades online, eles poderiam roubar todas as suas informações, como sua conta bancária ou números de cartões de crédito. A criptografia protege você nestas situações, garantindo que pessoas não autorizadas não possam acessar ou modificar suas informações.

Quando a informação não é criptografada, ele é chamada de texto simples. Isto significa que qualquer pessoa pode facilmente ler ou acessar essa informação. A criptografia converte essas informações em um formato não legível chamado texto-cifrado. A criptografia funciona usando operações matemáticas complexas e uma chave única para converter as informações em texto cifrado. A chave é o que bloqueia ou desbloqueia as informações, assim como uma chave pode bloquear ou desbloquear uma porta. Um exemplo comum de uma chave é uma senha, apenas as pessoas que têm essa senha podem descriptografar e acessar suas informações. Para proteger a sua informação criptografada você precisa proteger sua chave. Em geral a criptografia trabalha de duas maneiras, você pode criptografar dados em repouso (como os dados armazenados em seu laptop) e dados em movimento (como a transmissão de informações on-line).

Criptografando Informações em Repouso

O principal objetivo da criptografia em repouso é proteger as informações no caso de seu computador ou dispositivo móvel ser perdido ou roubado. Quinze anos atrás, isso não era um problema, como a maioria dos computadores era grande e pesado e os desktops eram muito difíceis de se transportar. Hoje, muitos laptops pesam apenas alguns poucos quilos, enquanto um dispositivo móvel pode pesar apenas alguns gramas. Estes dispositivos são extremamente poderosos e

Criptografia

mantém uma quantidade enorme de informação, mas também são muito fáceis de perder. Além disso, outras mídias móveis podem conter informações confidenciais, como pen drives ou CD-ROM. Uma técnica comum para criptografar informações nestes dispositivos é chamada de Full Disk Encryption (FDE). Isso significa que tudo no sistema é automaticamente criptografado, você não tem que decidir o que ou o que não criptografar. A maioria dos sistemas operacionais hoje em dia vem com Full Disk Encryption embutido, você simplesmente tem que habilitá-lo. Por exemplo, o Mac OS X inclui FileVault enquanto algumas versões do Windows incluem o Bitlocker. Se o seu computador é compatível com Full Disk Encryption, recomendamos que você ative-o. Além disso, a maioria dos celulares suporta Full Disk Encryption para os seus dispositivos de armazenamento interno. Por exemplo o iOS, sistema operacional para iPhones e iPads, aplica automaticamente Full Disk Encryption uma vez que um código de acesso seja definido. Para saber se o seu computador ou dispositivo móvel do trabalho suporta Full Disk Encryption, pergunte ao seu suporte técnico ou supervisor. Para os seus computadores pessoais, entre em contato com o fabricante do computador ou veja a documentação on-line.

A criptografia é uma maneira poderosa de proteger suas informações, mas é tão forte quanto a sua chave.

Criptografando Informações em Trânsito

A informação também é vulnerável quando está em trânsito. Se os dados não são criptografados, eles podem ser monitorados e capturados online. É por isso que você quer assegurar que quaisquer comunicações online sigilosas, tais como serviços bancários on-line, envio de e-mails ou até mesmo acesso a sites de mídia social sejam criptografados. O tipo mais comum de criptografia on-line é o HTTPS. Isso significa que todo o tráfego entre o seu navegador e um site é criptografado. Procure por https:// na URL, por um cadeado em seu navegador, ou uma barra onde fica a URL ficando verde. Estes são todos sinais de que a comunicação é criptografada. Dependendo do seu navegador e do site, você poderá ver todos os três ao mesmo tempo. Além disso, sempre que você se conectar a uma rede Wi-Fi pública, certifique-se de também usar a criptografia quando possível. Finalmente, ao enviar ou receber e-mails verifique se o seu cliente de e-mail está configurado para transmitir o seu e-mail por um canal criptografado. A maioria dos clientes de e-mail fornece criptografia, além disso o seu provedor de acesso à Internet pode ser capaz de ajudá-lo a ativar a criptografia do seu cliente de e-mail.

Implementando a Criptografia Corretamente

Independentemente de qual tipo de criptografia você esteja utilizando ou de como você à utiliza, quase todas as formas de criptografia compartilham alguns passos em comum para a utilizarmos corretamente.

Criptografia

- Sua criptografia é tão forte quanto a sua chave. Se alguém adivinha ou compromete a sua chave, eles terão acesso aos seus dados. Você precisa proteger a sua chave.
- Se você estiver usando um código de acesso ou uma senha para a sua chave, certifique-se de que é uma senha longa e segura e não a perca ou esqueça. Se você esquecer, você estará trancado fora de seus próprios dados.
- Sua criptografia é tão forte quanto a segurança do seu computador. Se o seu computador foi invadido ou infectado, criminosos cibernéticos podem ignorar a sua criptografia. Por isso, não se esqueça de manter o seu computador ou dispositivo móvel seguro também.
- Se você possui diferentes opções de criptografia, sempre escolha o método mais forte.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

Mac OS X Filevault:	http://support.apple.com/kb/HT4790?viewlocale=pt_BR
Criptografia no iOS:	http://support.apple.com/kb/HT4175?viewlocale=pt_BR&locale=en_US
Criptografia no Android (em Inglês):	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Criptografia no Windows:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Protegendo seu computador:	http://www.securingthehuman.org/ouch/2012#december2012
Gerenciadores de senhas:	http://www.securingthehuman.org/ouch/2013#october2013

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Katia Lucia da Silva, Rodrigo Gularte, Marta Visser