OUCH! | Agosto de 2015

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- O que fazer backup e quando
- Como fazer backup
- Restauração
- Pontos-chave

Cópia de Segurança (Backup) e Restauração

Visão Geral

Mais cedo ou mais tarde provavelmente algo dará errado e você perderá seus arquivos, documentos pessoais ou fotografias. Exemplos incluem você acidentalmente excluir os arquivos errados, falhas de hardware, perder o seu laptop ou infectar o seu computador. Em momentos como esses, backups são normalmente a única maneira que você tem para reconstruir a sua vida digital. Nesse informativo vamos explicar o que são os backups, como fazer o backup de seus dados e ajudar você a decidir qual a estratégia mais indicada para o seu caso.

Editor Convidado

Heather Mahalik é uma especialista forense reconhecida pela indústria, especializada em forense para smartphones. Ela é co-autora de “Practical Mobile Forensics”, editora técnica de “Learning Android Forensics” e co-autora do “FOR585 Advanced Smartphone Forensics” e “ FOR518 Macintosh Forensics” para o SANS Institute. Siga Heather em **Smarterforesnics.com** e Twitter: **@heathermahalik**.

O Que Fazer Backup e Quando

Backups são cópias de suas informações que são armazenadas em outro lugar. Quando você perder dados importantes, você poderá recuperar os dados a partir de seus backups. O problema é que a maioria das pessoas não realiza tais cópias de segurança, o que é vergonhoso, porque eles podem ser simples e baratos. Existem duas abordagens para decidir o que fazer backup: (1) dados específicos que são importantes para você; ou (2) tudo, incluindo todo o seu sistema operacional. A primeira abordagem simplifica os backups e economiza espaço no disco rígido, no entanto, a segunda abordagem é a mais simples e a mais abrangente. Se você não tem certeza do que fazer backup, recomendamos fazer backup de tudo.

Sua próxima decisão será a frequência com que deseja fazer o backup de seus dados. As opções mais comuns incluem de hora-em-hora, diariamente, semanalmente, etc. Para uso doméstico, programas de backup pessoais, como o Time Machine da Apple ou o Windows Backup e Restore da Microsoft permitem que você crie um agendamento de backup automático do tipo “defina-o e esqueça-o”. Essas soluções fazem backup silenciosamente de seus dados ao longo do dia, enquanto você está trabalhando ou mesmo quando você não está utilizando seu computador. Outras soluções oferecem “proteção contínua”, na qual os arquivos novos ou alterados são imediatamente atualizados no seu backup, tão logo eles sejam fechados. No mínimo, recomendamos que você realize backup diariamente. Em última análise, a questão a se perguntar é: “ Quanta informação eu poderia me dar ao luxo de perder se eu tivesse que restaurar algo a partir de um backup?”

Como fazer backup

Há duas maneiras de fazer backup de seus dados: em meios físicos ou em armazenamento baseado na nuvem. Meio (mídia) físico é qualquer tipo de hardware, tais como DVDs, drives USB ou discos rígidos externos. Sejam quais forem os meios que você escolher, nunca faça o backup de seus arquivos para o mesmo dispositivo que contém os arquivos originais. O problema com a mídia física é que se ela estiver onde houver um desastre (como um incêndio ou roubo), você poderá perder não só o

Cópia de Segurança (Backup) e Restauração

seu computador, mas também os seus backups. Por isso você deve ter um plano para armazenar cópias de backup fora do local de origem, em um local seguro. E se optar por armazená-los fora do local de origem, certifique-se de rotulá-los com o que foi copiado e quando. Para segurança extra, proteja seus backups utilizando criptografia.

Backups automatizados e confiáveis são muitas vezes a sua última linha de defesa na proteção de seus dados.

As soluções baseadas na nuvem são diferentes, é um serviço onde os arquivos estão armazenados em algum lugar na internet. Dependendo da quantidade de dados que quiser fazer backup, você pode ter que pagar pelo serviço. Ele funciona através da instalação de um programa no seu computador que automaticamente faz o backup de seus arquivos para você. A vantagem desta solução é que uma vez que seus backups estejam na nuvem, eles ainda estarão seguros mesmo que um desastre aconteça na sua casa, por exemplo. Além disso, você poderá acessar até mesmo arquivos individuais dos backups, a partir de praticamente qualquer lugar, mesmo quando viajar. A desvantagem é que backups baseados na nuvem (e a recuperação), podem ser mais lentos, especialmente se você tem uma grande quantidade de dados. Se você não tiver certeza de qual opção de backup é a melhor para você (mídia física ou nuvem) tenha em mente que você sempre pode fazer as duas coisas.

Finalmente, não se esqueça de seus dispositivos móveis. A vantagem dos dispositivos móveis é que a maioria dos dados já está armazenado na nuvem, como o seu e-mail, eventos do calendário ou contatos. No entanto, você pode ter informações que não estão armazenadas na nuvem, como suas configurações de aplicativos móveis, fotos recentes e as configurações do sistema. Ao fazer o backup do seu dispositivo móvel, você não só preserva essa informação, como também torna mais fácil restaurá-la em outro dispositivo, como ao comprar um aparelho novo, por exemplo. Um iPhone / iPad pode automaticamente fazer o backup para o iCloud da Apple. Android ou outros dispositivos móveis em geral, dependem do fabricante ou do fornecedor de serviços. Em alguns casos você pode ter que comprar aplicativos móveis projetados especificamente para fazer backups.

Restauração

Fazer o backup dos seus dados é apenas a metade da batalha, você tem que ter certeza de que pode recuperá-los. Verifique mensalmente se seus backups estão funcionando, recuperando por exemplo um arquivo e validando o seu conteúdo. Além disso, não se esqueça de fazer um backup completo do sistema antes de uma grande atualização (como mudar para um novo computador ou dispositivo móvel) ou realizar um reparo importante (como a substituição de uma unidade de disco rígido) e verificar se ele é passível de restauração.

Pontos-chave

- Automatizar seus backups, tanto quanto possível e verificá-los regularmente;

Cópia de Segurança (Backup) e Restauração

- Quando restaurar todo um sistema de backup, certifique-se de reaplicar as atualizações e correções de segurança mais recentes antes de usá-lo novamente;
- Backups desatualizados ou obsoletos podem virar uma responsabilidade adicional e devem ser destruídos para evitar que eles sejam acessados por usuários não autorizados;
- Se você estiver usando uma solução de nuvem, pesquise sobre as políticas de uso e a reputação do fornecedor e verifique se eles atendem às suas necessidades. Por exemplo, eles criptografam seus dados quando ele é armazenado? Quem tem acesso aos seus backups? Será que eles suportam autenticação forte, tal como verificação em duas etapas?

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

Fontes

Frases Secretas:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_pt.pdf
Verificação em Duas Etapas:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_pt.pdf
Segurança na Nuvem:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_pt.pdf
Criptografia:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_pt.pdf
Dica do Dia (inglês):	http://www.sans.org/tip_of_the_day.php

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