A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Backup & Restauração

Visão Geral

Se você usa um computador ou dispositivo móvel há algum tempo, cedo ou tarde alguma coisa dará errado e você perderá arquivos pessoais, documentos ou fotos. Por exemplo, você pode acidentalmente apagar arquivos errados, ter um problema de hardware, perder o aparelho ou ser infectado com um malware como um Ransomware. Nessas horas o backup será a única alternativa para você reconstruir sua vida digital. Nesta edição vamos explicar o que são backups, como fazer backup dos seus dados e desenvolver uma estratégia simples que funcione para você.

Editor Convidado

Keith Palmgren é um professional de Segurança Cibernética com mais de 30 anos de experiência em Segurança de T/I. É instrutor Sênior do SANS e autor do curso SANS SEC301; “Introduction to Information Security” (Introdução à Segurança da Informação). Keith é consultor de segurança reconhecido e pode ser encontrado no Twitter como **@kpalmgren**.

Backups: O quê, Quando e Como

Backups são cópias das suas informações armazenadas em algum lugar diferente do seu computador ou dispositivo móvel. Quando você perde dados importantes, você pode recuperar esses dados usando seus Backups. Infelizmente, muitas pessoas falham em fazer backups regulares, mesmo quando são simples e baratos. O primeiro passo a tomar é decidir o que você quer backupear (guardar). Existem duas abordagens: (1) dados específicos e importantes para você; ou (2) tudo, incluindo o sistema operacional inteiro. Muitas soluções de backup são configuradas por padrão para utilizar a primeira abordagem. Elas fazem o backup dos dados existentes nas pastas mais comuns de arquivo. Em muitos casos isso será suficiente para você. Contudo, se não estiver certo sobre o que backupear ou quiser tomar cuidado extra, faça backup de tudo.

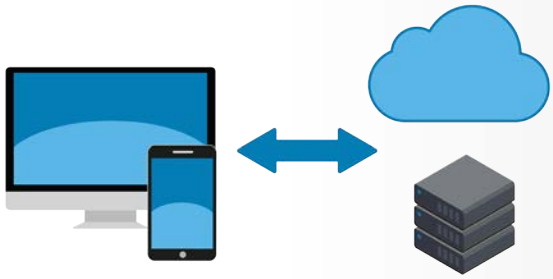
Segundo, você precisa decidir com que frequência fará o backup. Programas de backup embarcados como o Time Machine da Apple ou o Windows Backup and Restore da Microsoft permitem criar uma agenda do tipo “configure e esqueça”. Opções comuns incluem backup por hora, dia, semana, etc. Outras soluções oferecem “proteção contínua”, onde arquivos novos ou alterados são backupeados imediatamente a cada vez que você salva o documento. Minimamente, nós recomendamos backups diários automáticos.

Por último você precisa decidir como fará o backup. Existem duas formas de backupear seus dados: em mídia física ou em nuvem. Cada abordagem tem vantagens e desvantagens. Se não tiver certeza sobre qual escolher, você pode usar ambas simultaneamente. Mídias físicas são dispositivos que você controla, como discos USB externos ou dispositivos de rede acessíveis por Wi-Fi. A vantagem de usar suas próprias mídias é que elas permitem fazer backup e restauração de quantidades grandes de dados muito rapidamente. A desvantagem é que se você for infectado com um malware como um

© SANS Institute 2017

Backup & Restauração

Ransomware, existe a possibilidade dele se espalhar até seus backups. E também, se você passar por um desastre como um incêndio ou furto, você pode perder não só seu computador, mas também os backups. Por isso, se você usar mídias físicas para backup, você deverá guardar uma cópia do seu backup em um lugar seguro e diferente de onde estão seu computador e dados. Certifique-se também de que os backups armazenados em outro local estejam apropriadamente identificados com uma etiqueta.



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

Soluções baseadas em nuvem são serviços online que armazenam seus dados na Internet. Tipicamente, você instala uma aplicação no seu computador. A aplicação faz então o backup dos seus arquivos automaticamente, seja seguindo um agendamento ou quando você os modifica. Uma vantagem de soluções de nuvem é sua simplicidade. Os backups são muitas vezes automáticos e você pode acessar seus arquivos normalmente de qualquer lugar. Além disso, como seus dados estão na nuvem, desastres em casa, como incêndio ou furto, não afetarão seu backup. Finalmente backups em nuvem podem ajudá-lo a se recuperar de uma infecção por malware como Ransomware pois muitas soluções em nuvem permitem que você recupere arquivos de versões anteriores à infecção. A desvantagem é que o backup e a recuperação de grandes quantidades de dados podem consumir muito tempo. Além disso, a privacidade e segurança são importantes. O provedor do serviço oferece fortes controles de segurança, como criptografia dos dados e verificação em duas etapas?

Finalmente, não esqueça seus dispositivos móveis. Com os dispositivos móveis, muitos dos seus dados, como email, calendário, eventos e contatos já são armazenados na nuvem. Porém, a configuração dos seus aplicativos móveis, fotos recentes e preferências de sistema não são armazenadas na nuvem. Ao fazer backup do seu dispositivo móvel, você não só protege essas informações, mas torna fácil transferir seus dados quando fizer um “upgrade” para um novo aparelho. Um iPhone ou iPad podem fazer o backup automático para a nuvem da Apple. Em aparelhos Android ou com outros sistemas operacionais vai depender do fabricante ou provedor de serviço ter adicionado o recurso. Em alguns casos você pode ter que comprar um aplicativo móvel desenvolvido especificamente para fazer backups.

Restauração

Fazer backup dos seus dados é só metade da batalha. Você precisa ter certeza de que consegue recuperá-los. Verifique periodicamente se seus backups estão funcionando, fazendo a recuperação de um arquivo e certificando-se de que esteja igual ao original. Além disso, certifique-se de fazer um backup completo do seu sistema antes de fazer alguma grande mudança (como mover para um novo computador ou dispositivo móvel) ou um grande reparo (como uma troca de disco de dados) e verificar que ele é restaurável.

© SANS Institute 2017

Backup & Restauração

Pontos Chave

- Independente de qual solução utilizar para fazer o backup dos seus dados, certifique-se de automatizá-los e testá-los periodicamente;
- Quando tiver que reconstruir um Sistema a partir de um backup, certifique-se de reaplicar as últimas atualizações e correções antes de utilizá-lo novamente;
- Backups desatualizados e desnecessários são uma responsabilidade. Destrua-os para prevenir o acesso por pessoas não autorizadas;
- Se estiver utilizando solução em nuvem, pesquise as políticas de uso e a reputação do fornecedor e certifique-se de que eles atendem seus requerimentos. Por exemplo, eles criptografam seus dados? Suportam autenticação forte 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 securingthehuman.sans.org/ouch/archives.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Frases de Acesso:	https://securingthehuman.sans.org/ouch/2017#april2017
Verificação em duas etapas:	https://securingthehuman.sans.org/ouch/2015#september2015
Usando a nuvem com segurança:	https://securingthehuman.sans.org/ouch/2016#november2016
Criptografia:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

OUCH! é publicado pelo "SANS Securing the Human" e distribuído sob o licenciamento Creative Commons BY-NC-ND 4.0 license. A distribuição ou utilização desta publicação em programas de treinamento é permitida desde que seu conteúdo não seja modificado. Para traduções ou mais informações entre em contato pelo ouch@securingthehuman.org

Board Editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser