OUCH! | Setembro de 2014

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Utilize a Nuvem com Segurança

Visão Geral

"A Nuvem" é uma tecnologia poderosa que está sendo adotada rapidamente tanto por empresas quanto por usuários domésticos. Nuvem pode ter diferentes significados para pessoas diferentes, mas geralmente significa utilizar um provedor de serviços na Internet para armazenar e gerenciar seus dados por você. A vantagem da Nuvem não é apenas o fato de você poder acessar e sincronizar os dados de vários dispositivos em qualquer lugar do mundo, mas também poder compartilhar informações com quem você quiser. O motivo pelo qual chamamos esse serviço de "A Nuvem" é que geralmente não se sabe onde dados estão fisicamente armazenados. Exemplos de computação na Nuvem incluem a criação de documentos no Google Docs, o compartilhamento de arquivos via Dropbox, configurar seu próprio servidor na Nuvem da Amazon, ou armazenar suas músicas e fotos no iCloud da Apple. Esses serviços online têm o potencial de torná-lo muito mais produtivo, no entanto eles também vêm acompanhados de riscos particulares. Nesta edição abordaremos como você pode aproveitar a Nuvem com segurança.

Editor Convidado

James e Kelli Tarala (**@isaudit** / **@kellitarala**) são os principais consultores da Enclave Security e foram autores de inúmeros cursos de formação da SANS, incluindo o SANS Auditoria 566: Implementação e Auditoria dos Vinte Controles Críticos de Segurança e MGT 415: Uma Introdução Prática à Avaliação de Riscos.

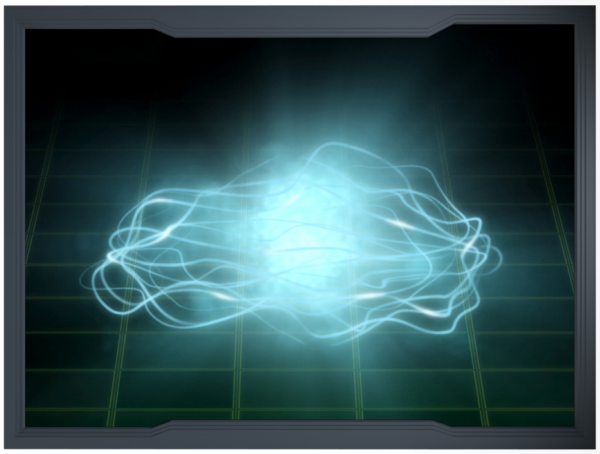
Escolha um Provedor de Serviços em Nuvem

A computação em Nuvem não é boa nem ruim, mas é um recurso que auxilia na execução de suas tarefas, tanto no trabalho quanto em casa. Porém, quando você utiliza esses serviços, está entregando seus dados privados nas mãos de estranhos e espera que eles os mantenham seguros e disponíveis. Por isso, você deve ter certeza de escolher com sabedoria. Para o computador do trabalho ou para usar informações do seu trabalho, verifique com seu supervisor se você pode utilizar os serviços de computação em Nuvem. Se tiver permissão para usar a Nuvem, certifique-se de confirmar quais serviços na Nuvem você pode utilizar e quais são as politicas para utilizá-los. Se estiver pensando em um serviço em Nuvem para uso pessoal, considere o seguinte:

1. **Suporte**: É fácil obter ajuda sobre o serviço ou obter resposta a uma pergunta? Há um número de telefone que você possa ligar ou um endereço de e-mail que você possa usar para entrar em contato? Existem outras alternativas de suporte, tais como fórum público ou Perguntas Frequentes no site do provedor?
2. **Simplicidade**: O serviço é fácil de usar? Quanto mais complexo for o serviço, mais propenso você estará a cometer erros e expor acidentalmente ou perder suas informações. Utilize um provedor serviços em Nuvem que você considere fácil de entender, configurar e usar;

Utilize a Nuvem com Segurança

3. **Segurança**: Como os dados serão transferidos do seu computador para a Nuvem? A conexão é protegida por criptografia? Como seus dados são armazenados? São criptografados e, se sim, quem pode decriptá-los ?
4. **Termos dos Serviços**: Reserve um momento para revisar os Termos dos Serviços (muitas vezes eles são surpreendentemente fáceis de ler). Confirme quem pode ter acesso aos seus dados e quais são seus direitos legais.



A Nuvem pode tornar seus dados mais acessíveis e ajudá-lo a ser mais produtivo. No entanto, tenha cuidado ao compartilhar suas informações.

Proteja seu Dados

Uma vez que tenha escolhido um provedor de serviços em Nuvem, o próximo passo é se certificar de usar os serviços em Nuvem corretamente. A maneira como compartilha seus dados pode muitas vezes ter bem mais impacto na segurança dos seus arquivos que qualquer outra coisa. Alguns passos fundamentais que você pode seguir incluem:

1. **Autenticação**: Utilize uma senha forte e exclusiva para se autenticar em sua conta na Nuvem. Se seu provedor de serviços em Nuvem oferece uma verificação de duas fases, recomendamos fortemente que você a utilize.
2. **Compartilhamento de Arquivos e Pastas**: A Nuvem torna o compartilhamento mais simples, às vezes simples demais. No pior dos casos, você pode, acidentalmente, tornar arquivos ou até mesmo pastas inteiras disponíveis publicamente para todos na Internet. A melhor maneira de se proteger é adotar o padrão de não compartilhar seus arquivos com ninguém. E então permitir que somente pessoas específicas (ou grupo de pessoas) acessem arquivos ou pastas específicas de acordo com a necessidade. Quando alguém não precisar mais de acesso aos arquivos, remova-os. Seu provedor de serviços na Nuvem deve fornecer um mecanismo fácil para rastrear quem tem acesso aos seus arquivos e pastas.
3. **Compartilhamento de Arquivos e Pastas com o uso de Links**: Uma característica comum em alguns serviços em Nuvem é a capacidade de se criar links que apontam para arquivos ou pastas. Esse recurso permite que você compartilhe seus arquivos com quem quiser, fornecendo somente um link de Internet. No entanto, essa abordagem tem pouca segurança, qualquer um que conheça esse link pode ter acesso aos seus arquivos ou pastas pessoais. Se você enviar o link para apenas uma pessoa, ela pode compartilhar esse link com os outros ou ele pode aparecer em algum mecanismo de busca. Se você compartilhar dados por meio de um link, certifique-se de desabilitá-lo caso ele não seja mais necessário ou, se possível, proteja-o com uma senha.
4. **Configurações**: Entenda as configurações de segurança oferecidas pelo provedor de serviços em Nuvem. Por exemplo, se você compartilhar uma pasta com alguém, ele pode, em contrapartida, compartilhar seus dados com outras pessoas sem o seu conhecimento?
5. **Antivírus**: Garanta que a última versão do software de antivírus esteja instalada em seu computador e em qualquer

Utilize a Nuvem com Segurança

outro computador utilizado para compartilhar seus dados. Se um arquivo que você estiver compartilhando for infectado, outros computadores que tenham acesso ao mesmo arquivo poderão ser infectados também.

6. **Backup**: Mesmo que seu provedor de serviços na Nuvem esteja fazendo backup dos seus dados, considere fazer regularmente suas próprias cópias de segurança. Isso não só protege seus dados caso o provedor pare de fornecer o serviço, fique indisponível ou inacessível por algum motivo, mas também pode ser bem mais fácil recuperar grandes volumes de dados das suas cópias locais em vez de baixá-los da Nuvem. Além disso, confirme a frequência com que o provedor faz backup dos seus arquivos, eles permitem que você recupere versões anteriores de seus arquivos? E por quanto tempo eles mantêm seu backups disponíveis?

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

Senhas Fortes:	http://www.securingthehuman.org/ouch/2013#may2013
Gerenciadores de Senhas:	http://www.securingthehuman.org/ouch/2013#october2013
Backup:	http://www.securingthehuman.org/ouch/2013#september2013
Termos de Segurança (em Inglês):	http://www.securingthehuman.org/resources/security-terms
Termos comuns de Segurança:	http://cartilha.cert.br/glossario

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

