OUCH! | Novembro de 2016

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Usando a nuvem com segurança

Visão geral

“A Nuvem” pode significar diferentes coisas para diferentes pessoas, mas geralmente significa usar um provedor de serviços na Internet para armazenar e gerenciar seus sistemas e / ou dados de computação. Uma vantagem da nuvem é que você pode facilmente acessar e sincronizar os dados de vários dispositivos em qualquer lugar do mundo, e você também pode compartilhar suas informações com quem quiser. Chamamos esses serviços “a nuvem”, porque muitas vezes não se sabe onde os dados estão fisicamente armazenados. Exemplos de computação em nuvem incluem a criação de documentos no Google Docs, compartilhamento de arquivos via Dropbox, configurar seu próprio servidor no Amazon Cloud, armazenar dados de cliente no Salesforce ou arquivar as suas músicas ou fotos no iCloud da Apple. Esses serviços online podem torná-lo muito mais produtivo, mas eles também vêm com riscos específicos. Neste boletim abordamos como você pode utilizar “a nuvem” com segurança.

Editor Convidado

Dave Shackleford (**@daveshackleford**) é consultor profissional, dono da Voodoo Security e autor de vários cursos de formação SANS, incluindo “SANS Security 579: Virtualization and Private Cloud Security” e “Security 524: Cloud Security Fundamentals”.

Selecionando um provedor de nuvem

A Nuvem não é boa nem má, é apenas uma ferramenta para fazer as coisas, tanto no trabalho como em casa. No entanto, quando você usa esses serviços você cede seus dados privados para os outros. E você espera que eles os mantenham seguro e disponível. Então, você quer ter certeza de estar escolhendo seu provedor de nuvem com sabedoria. Para os seus computadores de trabalho ou relacionados ao trabalho, verifique com seu supervisor de TI se sua empresa permite a utilização de serviços em nuvem. Se você tem permissão para utilizar a nuvem, confirme quais serviços de nuvem você pode usar e quais políticas deve seguir ao usá-la. Se você está procurando um serviço de nuvem para uso pessoal, considere o seguinte:

1. **Suporte**: Quão fácil é obter ajuda ou ter uma pergunta respondida ? Existe um endereço de email para entrar em contato, fóruns públicos onde você possa fazer perguntas ou uma lista de Perguntas Mais Frequentes no site da empresa ?
2. **Simplicidade**: Quão fácil é utilizar o serviço ? Quanto mais complexo o serviço, maior a probabilidade de você cometer erros e, acidentalmente, expor ou perder suas informações. Selecione um provedor de nuvem fácil de entender, configurar e usar;
3. **Segurança**: Quais dados são coletados sobre você, se isso acontecer ? Como os seus dados vão do seu computador

Usando a nuvem com segurança

para a nuvem e como ele é armazenado na nuvem - são encriptados ? E se forem, quem pode decriptar seus dados ?

4. **Termos de Serviço**: Tire um momento para rever os Termos de Serviço (são muitas vezes surpreendentemente fáceis de ler). Confirme quem pode acessar seus dados e quais são seus direitos legais, bem como quaisquer responsabilidades de segurança assumidos pelo prestador ou exigidos de você.

A nuvem pode tornar as informações mais acessíveis e você mais produtivo, mas tenha cuidado com a forma como você acessa e compartilha suas informações.

Proteção dos seus dados

Depois de ter selecionado um provedor de nuvem, o próximo passo é certificar-se de usar os serviços em nuvem corretamente. A forma de acessar e compartilhar seus dados pode muitas vezes ter um impacto maior sobre a segurança deles do que qualquer outra coisa. Alguns passos fundamentais que você pode seguir incluem:

1. **Autenticação**: Use uma senha forte e exclusiva para autenticar sua conta na Nuvem. Se o seu provedor de nuvem oferecer verificação em duas etapas é altamente recomendável que você ative-a. Este é um dos passos mais importantes que você pode tomar para proteger sua conta;
2. **Compartilhamento de arquivos / pastas**: A nuvem torna muito simples o compartilhamento de arquivos, as vezes até simples demais. No pior cenário, você pode pensar que está compartilhando seus arquivos com apenas um indivíduo específico, mas pode acidentalmente tornar seus arquivos ou mesmo pastas inteiras disponíveis publicamente para toda Internet. A melhor maneira de se proteger é não compartilhar qualquer um dos seus arquivos com qualquer pessoa por padrão. Em seguida, permitir que apenas pessoas específicas (ou grupos de pessoas) tenham acesso aos arquivos ou pastas específicas, com base na necessidade de saber. Quando alguém não precisar mais acessar seus arquivos, remova-a da lista de autorização. O seu provedor de nuvem deve fornecer uma maneira fácil de você controlar quem tem acesso aos seus arquivos e pastas;
3. **Compartilhamento de arquivos / pastas usando links**: Uma característica comum de alguns serviços em nuvem é a capacidade de criar um link que direciona para seus arquivos ou pastas. Este recurso permite compartilhar esses arquivos com quem quiser, simplesmente fornecendo o link da web. No entanto, esta abordagem tem muito pouca segurança, qualquer um que conheça este link pode ter acesso a seus arquivos pessoais ou pastas. Se você enviar o link para apenas uma pessoa, essa pessoa poderia compartilhar esse link com os outros ou ele poderia aparecer em mecanismos de busca. Se você compartilhar dados por meio de um link, certifique-se de desativar o link uma vez que não seja mais necessário, fixando uma data de validade ou, se possível, protegendo o link com uma senha;

Usando a nuvem com segurança

4. **Configurações**: Entenda as configurações de segurança disponíveis no seu provedor de Nuvem. Por exemplo, se você compartilhar uma pasta com outra pessoa, ela pode, por sua vez, compartilhar com terceiros sem o seu conhecimento? Verifique também se há maneiras de ver quem visualizou seu conteúdo compartilhado e quando foi visualizado. E se você pode restringir o compartilhamento para "somente leitura" ao invés de "leitura + escrita" onde as pessoas também podem modificar os arquivos;
5. **Antivírus**: Certifique-se de ter a versão mais recente do seu software antivírus instalada no seu computador e em qualquer outro computador usado para compartilhar seus dados. Se um arquivo que você está compartilhando for infectado, outros computadores que acessarem o mesmo arquivo também poderão ser infectados.

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
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

Recursos

Verificação em duas etapas:	https://securingthehuman.sans.org/ouch/2015#september2015
Frases Secretas:	https://securingthehuman.sans.org/ouch/2015#april2015
Gerenciadores de Senhas:	https://securingthehuman.sans.org/ouch/2015#october2015
O que é um Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Conceitos básicos de segurança na nuvem (em Inglês):	https://sans.org/sec524

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

