A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Protegendo Sua Rede Doméstica (de casa)

Visão geral

Vários anos atrás, redes domésticas eram relativamente simples, talvez nada mais do que um ponto de acesso sem fios e um computador ou dois usados para navegar na Internet ou jogar online. No entanto redes domésticas tornaram-se cada vez mais complexas. Não só estamos conectando mais dispositivos às redes de nossa casa, mas estamos fazendo mais com elas. Nesta edição vamos abordar alguns passos básicos para a criação de uma rede doméstica mais segura.

Editor Convidado

Kevin Johnson é o CEO da Secure Ideas, conduz o **MySecurityScanner.com** e é um instrutor sênior do SANS Institute. Você pode encontrar mais informações em **www.secureideas.com**.

Sua rede sem fio

Quase toda rede doméstica começa com uma rede sem fio (às vezes chamada de rede Wi-Fi). Isto é o que permite uma conexão sem fio de qualquer de seus dispositivos à Internet desde laptops e tablets à consoles de jogos e televisões. Para que isso aconteça, a sua rede sem fio precisa de algo chamado de ponto de acesso sem fio (também chamado Wireless Access Point ou Wireless AP). É um dispositivo físico que se conecta ao seu roteador de Internet (ou pode ser seu próprio roteador de Internet) e envia um sinal sem fio ao qual seus dispositivos podem se conectar. Uma vez que seus dispositivos se conectam ao ponto de acesso, eles podem se conectar a outros dispositivos na sua rede doméstica, bem como à Internet. Como resultado, seu ponto de acesso sem fio é uma das peças-chave da sua rede doméstica. E recomendamos os seguintes passos para protegê-lo:

- Para a maioria dos pontos de acesso sem fio, o usuário administrador padrão e a senha padrão são bem conhecidos. E muitas vezes até mesmo publicados na Internet. Por isso, não se esqueça de alterar o nome de usuário administrador e a senha padrão para algo que só você saiba. Certifique-se que esta é uma senha única e não é usada para qualquer outra de suas contas;
- Outra opção que você vai precisar para configurar é o nome da sua rede sem fio (às vezes chamado SSID). Este é o nome que seus dispositivos irão ver quando procurarem por redes locais sem fio. Use algo único como nome da rede para que você possa identificá-la facilmente, mas certifique-se de não usar nenhuma informação pessoal. Além disso, ajuda pouco configurar sua rede como oculta (sem transmissão do SSID). A maioria das ferramentas de varredura sem fio ou qualquer atacante experiente pode facilmente descobrir os detalhes de uma rede oculta;
- O próximo passo é garantir que apenas as pessoas que você conhece e confia possam se conectar

Protegendo Sua Rede Doméstica (de casa)

e utilizar a sua rede sem fio, e que essas conexões sejam encriptadas. Queremos ter certeza de que vizinhos ou estranhos não possam se conectar ou monitorar a sua rede. Você pode facilmente diminuir esses riscos, habilitando uma segurança forte em seu ponto de acesso sem fio. Atualmente, a melhor opção é usar o mecanismo de segurança WPA2. Habilitar simplesmente o WPA2 já torna necessária uma senha para que as pessoas se conectem à sua rede doméstica. E uma vez autenticadas essas conexões ficam encriptadas. Certifique-se de não usar métodos antigos e ultrapassados de segurança como WEP ou nenhuma segurança, o que é chamado de "rede aberta". Uma rede aberta permite que qualquer pessoa se conecte à ela sem qualquer tipo de autenticação;

Para proteger a sua rede doméstica verifique se você tem uma rede sem fio segura, se você está usando DNS aberto ou um serviço semelhante, e que todos os dispositivos em sua rede doméstica são atualizados.

- Certifique-se de que a senha que as pessoas irão usar para se conectar à sua rede sem fio é uma senha forte e difícil de adivinhar, e que é diferente da senha do administrador. Lembre-se que você provavelmente terá que digitar a senha apenas uma vez para cada um dos seus dispositivos, pois eles vão guardar e lembrar da senha;
- Muitos pontos de acesso sem fios suportam o que é chamado de Rede de Visitantes (convidados). A Rede de Visitantes permite aos visitantes se conectarem ao ponto de acesso sem fio e acessarem a Internet, mas não permite se conectarem a qualquer dos dispositivos de sua rede doméstica. Se você adicionar uma Rede de Visitante, certifique-se de habilitar o WPA2 e usar uma senha diferente para esta rede;
- Se você não consegue lembrar das diferentes senhas, use um gerenciador de senhas para armazená-las de forma segura.

OpenDNS

Depois de ter sua rede sem fio configurada, recomendamos configurar sua rede doméstica para usar OpenDNS como seus servidores DNS (ou um serviço similar como o "Norton ConnectSafe for Home"). Quando você digita o nome de um site de Internet no seu navegador, o DNS descobre qual servidor na Internet corresponde ao endereço que você quer conectar. Serviços como o OpenDNS identificam sites infectados conhecidos e impedem qualquer dispositivo conectado à sua rede doméstica sem fio de visitá-los acidentalmente. Além disso, esses serviços muitas vezes lhe oferecem a capacidade de filtrar e bloquear sites censuráveis. O que torna esta abordagem tão eficaz é que não é necessário instalar nenhum software nos seus dispositivos, basta uma alteração em seu ponto de acesso sem fio.

Protegendo Sua Rede Doméstica (de casa)

Seus dispositivos

O próximo passo é saber quais dispositivos estão ligados à sua rede doméstica e ter certeza que eles estão seguros. Isto costumava ser simples pois normalmente você só tinha alguns dispositivos conectados. No entanto hoje em dia quase tudo pode se conectar à sua rede doméstica, incluindo TVs, consoles de jogos, babá eletrônica, alto falantes, o termômetro da sua casa, ou talvez até o seu carro. Depois de identificar todos os dispositivos em sua rede doméstica, você pode se surpreender com quantos são. A melhor maneira de manter todos esses dispositivos seguros é garantindo que eles estão sempre rodando a última versão do seu sistema operacional. Certifique-se de ter a atualização automática habilitada. Se isto não for uma opção, então reveja e atualize mensalmente, se possível. Além disso, não deixe de visitar o site do seu provedor de acesso à Internet, pois eles podem fornecer ferramentas e serviços gratuitos para ajudar a proteger a sua rede doméstica.

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

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Scanner de segurança de rede:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Gerenciadores de Senhas:
http://www.securingthehuman.org/resources/newsletters/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