



A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

Dispositivos Residenciais Inteligentes

O que são Dispositivos Residenciais Inteligentes ?

Tradicionalmente, apenas alguns dos seus dispositivos residenciais podem se conectar à Internet, como seu laptop, smartphone ou console de jogos. Contudo, hoje mais e mais dispositivos estão se conectando à Internet, desde luminárias à caixas de som da TV, fechaduras e até mesmo seu carro. Em breve quase todos os dispositivos na sua casa poderão estar conectados à Internet. Esses dispositivos conectados são muitas vezes referenciados como Internet das Coisas (IoC ou IoT, da sigla em inglês) ou Dispositivos Residenciais Inteligentes. Ao mesmo tempo em que isso nos oferece uma grande conveniência, também nos traz um perigo único.

Qual é o problema ?

Quanto mais dispositivos conectados à sua rede local você tiver, mais problemas poderá ter. Atacantes podem programar seus dispositivos para atacar outros, fabricantes podem coletar informações excessivas sobre suas atividades ou seus dispositivos podem ficar infectados e bloquear suas atividades. Muitas das empresas que fabricam esses dispositivos não têm experiência em segurança cibernética e veem segurança como um custo. Como resultado, muitos dos dispositivos que você compra têm pouca ou nenhuma segurança embarcada. Por exemplo, alguns equipamentos têm senhas padrão publicamente conhecidas e que não têm opção para troca ou configuração.

Como posso me proteger

Então, o que você pode fazer a respeito? Nós, definitivamente, queremos que você aproveite os dispositivos conectados, de forma segura. Eles podem oferecer recursos para tornar sua vida mais simples. Além disso, com a evolução da tecnologia você pode não ter opção a não ser utilizar os dispositivos inteligentes. Aqui vão passos chave a seguir para você se proteger:



Conecte apenas o que você precisa: A forma mais simples de tornar um dispositivo seguro é não conectá-lo à Internet. Se você não precisa que ele esteja online, não o conecte à sua rede Wi-Fi. Você realmente precisa que sua torradeira envie notificações para seu telefone?



Saiba o que você tem conectado: Quais dispositivos estão conectados à sua rede residencial? Não tem certeza ou não se lembra? Desligue sua rede sem fio e veja quais param de funcionar. Você pode não pegar todos mas poderá se surpreender com quantos se esqueceu;



Mantenha-os atualizados: Assim como seu computador e dispositivos móveis, é crítico manter todo e qualquer dispositivo atualizado. Se seu dispositivo tem a opção de atualização automática, habilite-a;



Senhas: Mude as senhas dos seus dispositivos para uma frase de acesso forte e única que apenas você saiba. Provavelmente você só precisará digitá-la uma vez. Não se lembra da sua frase de acesso? Não se preocupe, nem nós. Considere a possibilidade de usar um gerenciador de senhas para armazenar todas as suas senhas de forma segura;



Opções de privacidade: Se seu dispositivo permite configurar opções de privacidade, limite a quantidade de informações que ele coleta ou compartilha. Uma opção é simplesmente desabilitar qualquer recurso de compartilhamento de informações;



Fabricante: Compre seus dispositivos de uma empresa que conhece e confia. Procure produtos que têm recursos de segurança, como a opção de atualização automática, mudança de senha padrão e mudança de configurações de privacidade;



Sempre ouvindo: Se um dispositivo pode responder a comandos de voz, significa que ele está constantemente ouvindo. Pense nisso quando escolher o lugar onde colocá-los em sua casa e revise as opções de privacidade;

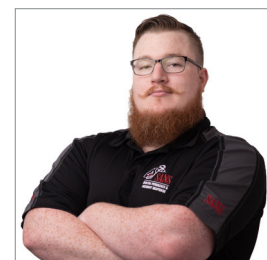


Rede de convidados: Considere a possibilidade de colocar seus dispositivos residenciais inteligentes em uma rede de “Convidados” separada, ao invés da rede primária que usa para seus computadores e dispositivos móveis. Assim, no caso de algum dispositivo inteligente ser infectado, seus computadores e dispositivos móveis da rede principal permanecerão seguros.

Não há motivo para ter medo de tecnologias novas, mas entenda os riscos que vêm com elas. Ao seguir esses passos simples você pode ajudar a criar uma casa inteligente bem mais segura.

Editor Convidado

Robert M. Lee (@RobertMLee) é um instrutor certificado SANS e autor dos cursos “FOR578 - Cyber Threat Intelligence” e “ICS515 - ICS Active Defense and Incident Response”. Robert também é CEO e fundador da empresa de segurança industrial Dragos.



Recursos

Frases de Acesso: <https://www.sans.org/u/GEB>

Gerenciamento de Senha: <https://www.sans.org/u/GEG>

Protegendo sua rede doméstica: <https://www.sans.org/u/GEL>

OUCH! é publicado pelo “SANS Security Awareness” e distribuído sob o licenciamento [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). 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 www.sans.org/security-awareness/ouch-newsletter. Board Editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduzida por: Homero Palheta Michelin, Michel Girardias, Rodrigo Gularte, Marta Visser