

Casas inteligentes têm falhas de segurança que poderiam ser exploradas por vírus e hackers.

Versões conectadas à internet de câmeras de vigilância, lâmpadas, eletrodomésticos e outros objetos são mais vulneráveis a ataques de hackers do que se imaginava e podem causar grandes dores de cabeça aos donos de aparelhos do incipiente setor de "internet das coisas", segundo estudos e especialistas.

Cerca de 70% dos aparelhos do tipo têm brechas que permitiriam a ação de um criminoso, segundo um relatório de uma divisão de cibersegurança da HP, que analisou os dez dispositivos do tipo mais populares nos Estados Unidos.

tipo de aparelho se tornará ainda menos seguro", diz Daniel Miessler, especialista em segurança da informação, que foi um dos responsáveis pelo trabalho.

Com o levantamento, segundo Miessler, "ficou claro que existem vulnerabilidades capazes de comprometer sistemas caseiros e também corporativos". Foi encontrado um total de 250 itens problemáticos, como falta de criptografia de dados, autenticação com senhas fracas, registro de informações pessoais do usuário e atualizações automáticas inseguras.

Segundo Ilya Lopes, especialista de

pesquisa da empresa de segurança ESET no Brasil, quanto mais novo um segmento tecnológico, maior sua potencial vulnerabilidade. Por isso, é melhor evitar inserir dados pessoais em aparelhos recentes. "Se você tem um computador, um celular, por que faria um pagamento usando a TV, ou a geladeira?", questiona.

Fabricantes.

Miessler e Lopes dizem que é possível que um hacker acesse dados de um computador ou outro dispositivo ligado à rede por meio de uma brecha no

software de, por exemplo, um termostato inteligente. Por enquanto, não há software que funcione como um firewall ou um antivírus contra tais ameaças – o usuário está à mercê das fabricantes dos dispositivos.

As companhias Apple, Google e Samsung recentemente fizeram aquisições de empresas do segmento e anunciaram iniciativas para integrar seus aparelhos a casas inteligentes.

A Apple, por exemplo, anunciou o software HomeKit, que permitirá que os novos iPhones controlem objetos da "internet das coisas". (Folhapress)

ARTE/FOLHAPRESS

DADOS PRIVADOS
Cerca de 90% dos aparelhos estudados durante uma pesquisa da HP registram informações pessoais dos usuários, como e-mail, telefone e endereço, que poderiam ser exploradas no caso de um eventual ataque

REDE INVADIDA
Como a maior parte dos aparelhos de "internet das coisas" usa o Wi-Fi do usuário, um hacker poderia se valer de uma falha em um aparelho do tipo para tentar acessar PCs ou celulares

CÂMERAS "ESPIÃS"
Nos EUA, em 2012, babás eletrônicas da marca TrendNet expuseram as imagens das casas de centenas de usuários por causa de uma brecha no software de transmissão – e o caso não é isolado, segundo um relatório da Symantec

CONTROLE REMOTO
Um hacker poderia assumir o comando de uma casa conectada de maneira remota, segundo Daniel Miessler, da HP. Ele diz que empresas também podem ser alvo de ataques

FRAGILIDADE
70% dos aparelhos de "internet das coisas" estudados pela HP não tinham dados criptografados, o que simplifica a leitura de informações pessoais por hackers, enquanto 80% deles não exigiam senhas complexas

SENHA COMPLEXA
Usar uma palavra-passe longa para a rede Wi-Fi é mais importante que uma "difícil" (com símbolos, numerais, maiúsculas), segundo Ilya Lopes, especialista da ESET

BOAS ESCOLHAS
Na hora de comprar, o consumidor pode optar por produtos cujas fabricantes não tenham sido alvo de ataque anterior

NÃO COMPARTILHAR DADOS
Se o aparelho oferece a opção de não compartilhar dados pessoais, é melhor escolhê-la para protegê-los, segundo Kevin Haley da empresa de segurança Symantec

DESCONECTÁ-LO
Se não há necessidade de o dispositivo estar ligado à internet (como no caso de algumas impressoras ou aparelhos de som, por exemplo), é melhor desligá-lo da rede, segundo Haley

REDE PARALELA
Alguns roteadores permitem a criação de mais de uma rede de Wi-Fi. Uma boa ideia é separar em espaços virtuais diferentes os computadores e celulares dos aparelhos de casa