CASA INTELIGENTE. E SEGURA.

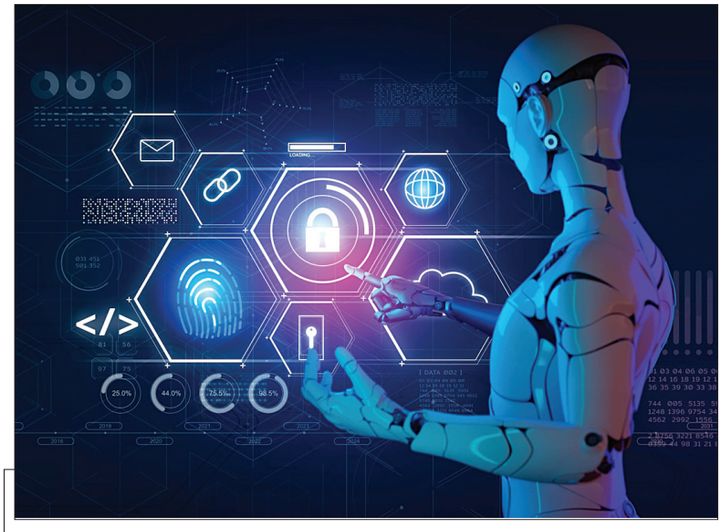
Dicas práticas para proteger sua rede doméstica e evitar ataques através dos dispositivos smart

Relatório divulgado em novembro pela consultoria internacional Frost & Sullivan indicou que já existem mais de 1 bilhão de dispositivos conectados na América Latina (no mundo inteiro, a estimativa é de 15 bilhões).

Certamente alguns deles estão em sua casa, escritório e outros locais que você frequenta: TVs, smartphones, caixas acústicas Bluetooth, assistentes de voz, consoles de videogame, relógios smart, webcams, fechaduras, lâmpadas, rastreadores fitness, GPS, dispositivos de saúde, controles de portões eletrônicos, óculos VR, monitores de bebês...

"Conectados", entenda-se, são todos os aparelhos capazes de se comunicar com outros e/ou de acessar a internet. Isso, é claro, inclui todo tipo de produto usado em monitoramento remoto, cujos dados obrigatoriamente passam por uma central de vigilância. Alguns são chamados "inteligentes", mas raros são aqueles que contêm proteção cibernética contra a segurança dos usuários.

A consequência disso é que, conforme aumenta a quantidade de produtos smart, crescem também os perigos rondando as pessoas e os espaços que utilizam. Exemplos: acesso não autorizado aos dispositivos, que passam a ser controlados por hackers; roubo de dados pessoais, que acabam sendo usados para atividades criminosas; contaminação por vírus que afetam as funções do aparelho.



COMANDANDO A CASA PELA TV

A sigla IoT (Internet das Coisas) foi saudada anos atrás como uma espécie de nirvana das redes de comunicação e dados. Cada aparelho – de uma TV de 98" a um micromódulo de iluminação – seria dotado de um sensor para se comunicar com outros aparelhos, permitindo uma integração total. Não demorou muito para os especialistas perceberem que essa interoperabilidade, ainda que possível, viria recheada de riscos à segurança dos usuários.

Os tais sensores de fato passaram a vir embutidos em quase todos os aparelhos, até mesmo as TVs que todos temos em casa. Com processadores cada vez mais potentes, as telas ganharam poderes para se comunicar com outros dispositivos da casa – e, em alguns casos, até comandá-los.

Só que, considerando a dinâmica das redes e a velocidade da evolução tecnológica, a prática de usar a TV como um item da automação na casa exige uma série de cuidados. A começar da configuração básica: a TV conectada a um modem fornecido pelo provedor de internet. Em muitas residências, a operadora instala um modem que também faz as vezes de roteador sem fio. E aí moram vários perigos.

Esse modem oferece pouca ou nenhuma proteção contra invasões, deixando a casa vulnerável. Os especialistas em segurança recomendam evitar ao máximo essa solução. Melhor conectar o modem a um ***roteador Wi-Fi*** *separado, de marca confiável e homologado pela Anatel, que venha com todos os protocolos de segurança instalados.*

Para maior proteção, há quem use dois roteadores separando o Wi-Fi: um para os computadores, smartphones e demais dispositivos que carregam informações mais sensíveis (dados bancários e de cartões de crédito, por exemplo); e outro para TVs, itens de automação e de uso eventual (para as visitas). São duas redes independentes, cada uma com sua senha: se houver problema em uma, a outra não será afetada.

Todo mundo que tem em casa uma rede Wi-Fi está vulnerável a ataques externos, que às vezes acontecem sem que a pessoa perceba. Todos os aparelhos conectados ao roteador ficam sob risco, inclusive a TV smart com acesso a centenas de aplicativos online. O que pode tornar uma rede mais segura é adotar medidas preventivas, como as sugeridas pelas grandes empresas de segurança de redes.

A primeira delas é escolher com cuidado os dispositivos que você compra. Como se sabe, a internet está infestada de produtos suspeitos que acabam atraindo pelo preço. No caso da automação, são lâmpadas, sensores, adaptadores, keypads etc. que prometem tornar sua casa "mais inteligente", mas na prática funcionam - quando funcionam - por tempo limitado. Pior: são facilmente hackeados.

Há ainda fabricantes nacionais que importam produtos da Ásia apenas para colocar suas marcas, sem qualquer preocupação com segurança. Alguns até homologam seus produtos na Anatel e no Inmetro, mas o problema é que não têm controle

DICAS PRÁTICAS DE SEGURANÇA

- *Escolha marcas de boa reputação, especialmente aquelas que oferecem regularmente updates de software e de firmware.*
- *Verifique se o produto é homologado pela Anatel e o Inmetro*
- *Altere a senha-padrão que vem de fábrica no seu produto. E acostume-se a atualizá-la de tempos em tempos.*
- *Importante: aparelhos específicos de automação normalmente não têm senha; mas os bons fabricantes mantêm servidores que monitoram esses produtos. Uma boa forma de proteção é manter atualizado seu cadastro no servidor da marca.*
- *Cuidado ao compartilhar a senha de sua rede: jamais o faça com pessoas que você não conheça bem.*
- *E acostume-se com a dupla autenticação da senha. Pode ser mais trabalhoso, mas no mínimo dobra o seu nível de proteção.*

sobre o firmware do aparelho, do qual depende a proteção contra violações. Os bons fabricantes tomam essas precauções, além de escolherem seus fornecedores com mais critério.

Uma dificuldade é que certos itens de automação são tão frágeis, em termos de segurança, que podem ser "sequestrados". Isso mesmo: de posse da senha Wi-Fi e do aplicativo usado para comandar uma lâmpada, por exemplo, um invasor pode acioná-la. E, através dela, chegar a outros dispositivos da rede.

Ao contrário do que estamos acostumados em nossos celulares e computadores, ninguém quer instalar em casa um sistema de automação para ter que ficar digitando senhas a toda hora. É por isso que os melhores fabricantes mantêm serviços em nuvem para proteger as instalações. Através de licenças e protocolos específicos, os instaladores são treinados para resolver problemas de segurança até mesmo online.

Cabe também ao usuário uma tarefa que, na prática, poucos adotam: verificar periodicamente as atualizações de seus aparelhos. Se é cômodo acionar as luzes, cortinas e o ar-condicionado pelo celular, nada mais lógico do que manter protegido o celular (e os apps nele instalados). E isso, no mundo smart, se faz com atualizações regulares.

**Colaborou George Wootton, do Instituto da Automação*

EUA QUEREM SELOS NOS DISPOSITIVOS

A preocupação com a segurança das redes existe no mundo inteiro. Mas alguns países estão mais avançados na adoção de medidas preventivas, caso dos EUA. A FCC, agência de telecomunicações, divulgou a ideia do CTM (Cyber Trust Mark), um programa voluntário para rotular os dispositivos conforme seu grau de segurança.

A proposta é fornecer aos consumidores, antes da compra, informações claras sobre os riscos cibernéticos do uso de cada produto. "Assim como o selo Energy Star indica ao consumidor que aquele aparelho consome menos energia, o selo CTM o ajudará a cuidar melhor de sua segurança e privacidade", diz Jessica Rosenworcel, diretora da FCC.

No material distribuído em agosto, a Agência diz que a identificação irá estimular os fabricantes a aprimorar seus padrões de segurança, já que essa será uma demanda cada vez mais comum dos usuários.

SOBRA: