áudio - vídeo - iluminação - automação - decoração

ÁUDIO&VÍDEO

DESIGN & TECNOLOGIA

ANO - 12
#154
Crazy Turkey Editora

CINEMAS CASEIROS

Confira uma seleção especial com os home cinemas mais modernos e charmosos criados para as edições da Casa Cor

ESPECIAL: CONDICIONADORES DE ENERGIA

Tire todas as suas dúvidas sobre os equipamentos que protegem e garantem a qualidade do seu sistema

PARA LÁ DE IRRESISTÍVEL

O novo LG G6 chega com incríveis recursos de imagem e função de reconhecimento facial

E VOCÊ? JÁ ASSISTIU?

Os bastidores da série alemã *Dark*, que se tornou um dos maiores sucessos do Netflix

O FUTURO É DOS ROBÔS?

Que funções serão substituídas pelas máquinas nos próximos anos? E que atividades não correm o risco de serem extintas?

SEGURANÇA DE DENTRO PARA FORA

A segurança cibernética de uma casa inteligente depende mais de boa informação e hábitos corretos que da própria tecnologia

››A cada dia, surgem novos eletrodomésticos e gadgets que podem dar um "upgrade" em nossas casas, tornando-as mais "inteligentes". É certo que, no Brasil, a compra desses dispositivos é um pouco mais complicada, sendo necessário recorrer a fornecedores não exatamente "autorizados" ou aproveitar viagens e trazer de fora.

O resultado é que a febre de ter esses equipamentos inteligentes ainda não pegou. Mas um número crescente de consumidores sempre acha um jeito de ter esses brinquedos em casa.

Alguns são bem conhecidos, como o Amazon Echo (também conhecido como Alexa). Mas sites de vendas online estão trazendo ao mercado brasileiro produtos "conectados" de marcas desconhecidas, vindos diretamente da Ásia e a preços muito convidativos. A oferta é grande, mas praticamente nenhum deles oferece um suporte adequado ou orientações para que o cliente consiga fazer uma instalação confiável e segura.

REDE WI-FI

Quando pensamos em ter uma casa mais moderna, com equipamentos conectados ou "inteligentes", precisamos lembrar do que está envolvido e devemos tomar algumas medidas para nos protegermos de ataques de hackers e similares. É necessário lembrar que praticamente todo equipamento "inteligente" precisa de uma conexão com a internet, sendo que a grande maioria utiliza o Wi-Fi da propriedade, enquanto outros podem, ainda, usar Bluetooth ou similares.

Portanto, você precisa planejar sua rede Wi-Fi de forma a atender todos os pontos nos quais queira instalar equipamentos "inteligentes", sejam câmeras, caixas de som, lâmpadas ou geladeiras. Esse planejamento envolve três pontos básicos: cobertura, capacidade e segurança.

Em geral, os equipamentos "inteligentes" que você pensa em adquirir oferecem a possiblidade de serem monitorados ou comandados de qualquer lugar no planeta através do seu smartphone. Isto só será possível se esses equipamentos conseguirem falar com o mundo exterior (fora da sua casa e de sua rede Wi-Fi). E eles farão isso usando sua conexão com a internet para alcançar servidores específicos, que, por sua vez, se conectarão aos aplicativos instalados no seu smartphone.

CABOS DE REDE

Quando planejar sua rede Wi-Fi, pense em todas as áreas onde quer ter alcance, tanto para seu smartphone ou tablet quanto para os dispositivos inteligentes que pretende instalar. Há muitas opções de como planejar esta rede. Mas, lembre-se: se utilizar repetidores, a velocidade de conexão cai aproximadamente 40% a cada repetidor, até chegar ao roteador principal. Assim, recomendo que cada repetidor se conecte ao roteador por cabo ao invés de fazer uma conexão Wi-Fi.

Por George Wootton Fotos Shutterstock.com

Isto irá requerer algum planejamento e a passagem de cabos de rede, mas o resultado será muito melhor, tanto em confiabilidade quanto em performance. Se tiver alguma dificuldade em fazer você mesmo, contrate um profissional e diga-lhe a cobertura que deseja, para que ele providencie a melhor solução.

Outro ponto importante é a capacidade da rede, que é medida por dois parâmetros principais: velocidade e volume. Enquanto, internamente, sua rede será de alta velocidade, o gargalo realmente está na conexão do roteador à internet, que está diretamente relacionado com a velocidade que você contrata das operadoras (normalmente medida em dezenas de megabits por segundo).

Já o volume se refere à quantidade de dados (bytes) que foram transferidos ao longo de um determinado tempo, normalmente ao longo de um mês. As operadoras podem limitar esse volume e, ao estourar sua cota, diminuir sua velocidade ou lhe oferecer a compra de uma franquia de volume adicional. Este parâmetro é normalmente medido em Gigabytes. Seu consumo de velocidade e volume depende do número máximo de usuários conectados ao mesmo tempo e do tipo de utilização.

NOVOS PERIGOS

Os equipamentos inteligentes não costumam utilizar muito da rede, passando poucas informações e em momentos espaçados. Mas é importante verificar se algum desses equipamentos tem uma funcionalidade ou necessidade de

um acesso mais rápido para que opere corretamente. Um caso típico são as TVs Smart, que podem oferecer serviços como YouTube ou Netflix, os quais consomem uma razoável parte da velocidade e do volume que você contratou.

Já o capítulo segurança merece uma atenção especial, principalmente com a inclusão de dispositivos inteligentes à sua rede doméstica.

Antes da inclusão desses dispositivos, os cuidados com a segurança já eram necessários. Mas a diversidade de equipamentos era muito limitada. Você tinha o roteador propriamente dito, alguns micros e smartphones. Os principais cuidados envolviam o uso de senhas para acesso à rede e de programas de firewall e antivírus nos micros. Ninguém se preocupava com medidas adicionais, como configuração do roteador, fechamento de portas de acesso não utilizadas, alteração periódica de senhas etc. E os danos, no caso de uma invasão por hackers, se bem que extremamente nocivos, eram conhecidos: perda de acesso aos equipamentos, roubo de informações pessoais e utilização de seus equipamentos para operações escusas, sem seu conhecimento.

A chegada dos dispositivos inteligentes trouxe duas novas preocupações para a segurança de sua rede (e, indiretamente, de sua casa): agora, são equipamentos novos e diferentes a serem protegidos, e a ação de hackers sobre esses aparelhos traz novos perigos, alguns, ainda desconhecidos do público em geral.

Então, precisamos aumentar nossos cuidados com a segurança do sistema, principalmente de nossa conexão com a internet. Algumas medidas de proteção são bastante simples e eficazes, enquanto outras podem exigir a ajuda de especialistas.

REVISITE SUA SEGURANÇA

Reveja o que você tem configurado atualmente no seu roteador. Se preocupe com pontos como:

• Você trocou a senha de fábrica do roteador por alguma mais complexa? Pode caprichar na complexidade, pois os equipamentos de sua casa somente precisarão ser configurados uma vez. Guarde sua senha com cuidado e segurança.

• Não use a mesma senha para todos os equipamentos. Troque suas senhas regularmente.

• Você costuma deixar seus convidados usarem seu Wi-Fi? Em muitos roteadores, é possível criar uma segunda rede, onde você pode mudar as senhas com facilidade e periodicamente. Assim, você libera o acesso e sabe que este será temporário, bastando mudar a senha.

• Se você não conhece a fundo a parte técnica, peça a um especialista para verificar as configurações do roteador. Os provedores não costumam proteger adequadamente este equipamento.

• Busque um conjunto de proteções que sejam ótimas, mas sem dificultarem seu uso e o gerenciamento do sistema. Do contrário, abandonando os cuidados, deixando o sistema vulnerável.

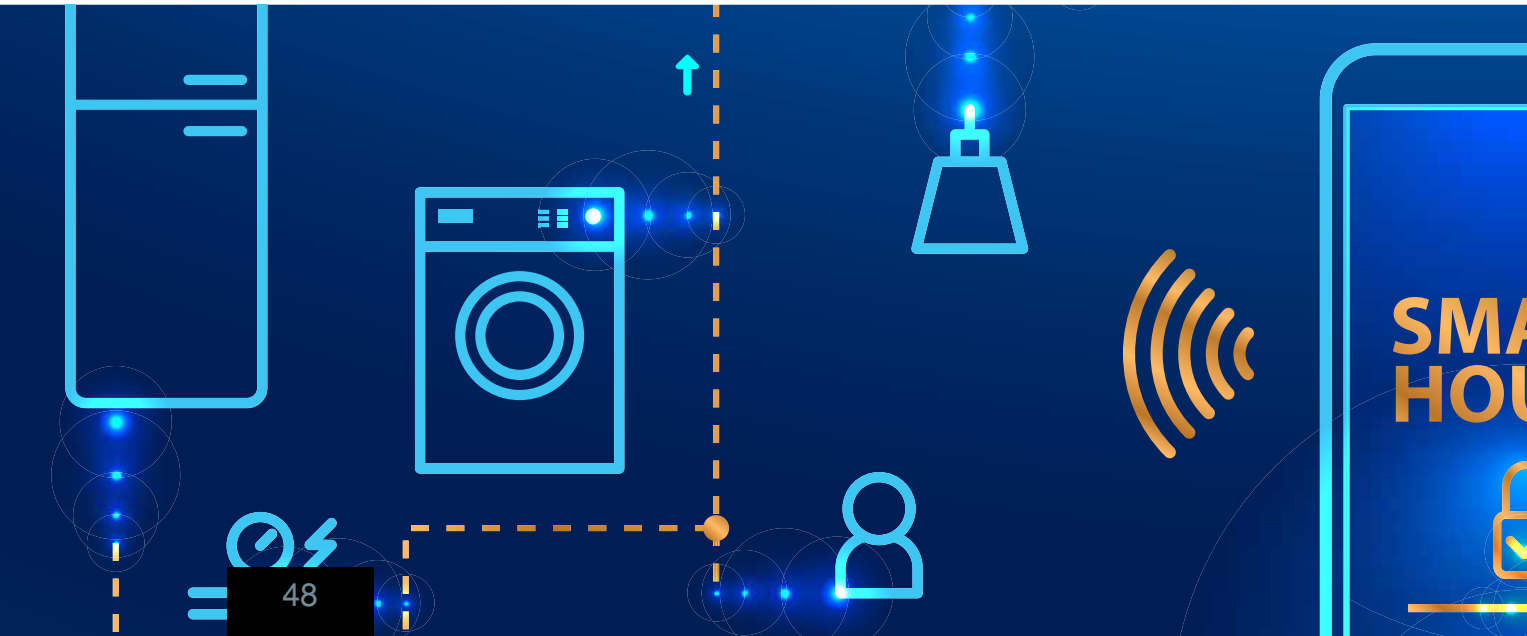
CONHEÇA SEUS NOVOS "BRINQUEDOS"

Antes de instalar algum novo dispositivo inteligente que precise de sua rede doméstica, tome alguns cuidados básicos:

• Verifique, na internet, comentários e avaliações do dispositivo, principalmente quanto à segurança.

• Informe-se sobre como o fabricante oferece as atualizações do firmware do produto. O ideal é que seja via internet e de forma automática. Assim, qualquer atualização de segurança será feita assim que disponível.

• Lembre-se de trocar a senha padrão do dispositivo. Muitas pessoas deixam a senha de fábrica, e qualquer um poderia acessar seu dispositivo se conseguisse



entrar em sua rede doméstica.

Porém, o mais importante é você verificar seu uso, para que não coloque em risco a segurança no caso de falha ou hackeamento do dispositivo. Essa recomendação é especialmente importante para dispositivos como fechaduras inteligentes ou controladores de equipamentos elétricos, como bombas de piscina.

Saiba como abrir uma fechadura inteligente quando a sua "inteligência" falhar e instale uma chave geral para o motor da bomba da piscina, para que ela não seja acionada enquanto estiver fazendo alguma manutenção.

CUIDADOS COM SEUS SMARTPHONES E TABLETS

Muitos dispositivos inteligentes possuem aplicativos que devem ser instalados em smartphones ou tablets para que possam ser usados em sua totalidade. Então, considere isso como inevitável. E muitas vezes, será mais de um smartphone ou tablet, pois outros moradores também podem querer interagir com os equipamentos.

Estes dispositivos são um dos elos frágeis da sua corrente de segurança. Em muitos casos, se alguém se apossar do seu celular, poderá controlar seus equipamentos inteligentes à distância. É obrigatório, portanto, que você verifique o grau de segurança dos próprios aplicativos e do seu telefone. Algumas perguntas que você deve se fazer:

• O aplicativo precisa de senha sempre? Ou, pelo menos, tem uma opção para que precise sempre?

• Esta proteção está "casada" com a proteção do celular? Ou seja: se seu celular tem biometria, você pode usar a mesma biometria para liberar o acesso ao aplicativo? Isso não é obrigatório, mas facilita muito o uso sem colocar em risco a segurança.

• Todos os moradores que podem acessar os aplicativos têm proteção nos celulares? Senhas de desbloqueio ou biometrias?

• Eu realmente quero funções automáticas oferecidas pelos fabricantes dos dispositivos, como destrancar automaticamente uma porta com a aproximação do celular?

O FATOR HUMANO

Em geral, o elemento mais fraco desta corrente de segurança é o ser humano, principalmente, quando temos um conjunto deles formando uma família. Diferentes idades, interesses, prioridades e conhecimentos tornam difícil criar comportamentos seguros que sejam obedecidos por todos.

Adolescentes podem liberar o acesso a aplicativos para seus amigos, confiando neles. Mas estes amigos podem ter seus celulares roubados sem que tenham se protegido adequadamente. Crianças podem acionar elementos de segurança, como destravar portas sem a capacidade de avaliar os riscos.

Pessoas de mais idade terão dificuldade em entender tudo o que está envolvido e podem não saber comandar um determinado equipamento importante para sua segurança o conforto. A doutrinação contínua de todos é necessária, assim como o treinamento para uso adequado dos dispositivos.

EM RESUMO...

A segurança cibernética de uma casa inteligente vem muito mais de dentro para fora, do que dos fabricantes e provedores. Começa com todos compreendendo que o assunto é sério! Passa por conhecimento e doutrinação. Envolve planejamento e escolhas bem feitas.

Especialistas podem ajudar a determinar a melhor solução, mas a manutenção da segurança deve ser uma responsabilidade de seus usuários. Terceirizar a segurança é como pedir a um estranho que guarde a chave de sua casa. Ele pode ser honesto e não fazer nada de errado, mas pode não saber o valor que esta chave tem e não cuidar dela adequadamente. •

GEORGE WOOTTON

é Diretor Comercial da DomóticaBR Automação Ltda. e se dedica à automação há mais de 30 anos, tendo trabalhado em grandes projetos inovadores no Brasil, em empresas nacionais e multinacionais. Ele também é Diretor Técnico da Aureside – Associação Brasileira de Automação Residencial e Predial.