Smart homes: a importância da (ciber)segurança dentro de nossa casa

dinheirovivo.pt/opiniao/smart-homes-a-importancia-da-ciberseguranca-dentro-de-nossa-casa-15123938.html

29 de agosto de 2022

"If everything is connected, everything can be hacked". Esta frase, que, em tradução livre significa "Se tudo está conectado, tudo pode ser hackeado", foi proferida pela Presidente da Comissão Europeia, Ursula von der Leyen, no discurso do Estado da Nação, em 2021, e resume na perfeição a premissa das duas faces da tecnologia e do digital: ao facilitarem a nossa vida, também nos trazem riscos acrescidos.

Ao longo dos últimos anos temos assistido à rápida evolução dos gadgets que utilizamos no nosso dia-a-dia assim como ao papel, cada vez mais preponderante, dos assistentes virtuais - dispositivos estes que estão a revolucionar o conceito de trabalho, mas também o mundo tecnológico em nossas casas. A digitalização dos objetos do nosso quotidiano permite-nos, por exemplo, poupar tempo com tarefas domésticas ou manter a nossa casa segura, contudo, existem alguns riscos associados, os quais, sem o fator da cibersegurança aliada poderão fazer com que não estejamos, nem nos sintamos tão seguros como o desejado nas nossas próprias casas.

É um facto que os ciberataques estão a aumentar com o crescimento da utilização recorrente destes dispositivos, de que são exemplo as smart TV, os sistemas de segurança inteligentes, os aspiradores "robots" ou até os monitores de bebés. De forma a contextualizar os leitores, deixo a nota de algumas estatísticas, a título de curiosidade, sobre a proliferação deste tipo de dispositivos e o consequente aumento do risco associado de ciberataques através dos mesmos. Em 2021, existiam cerca de 10 mil milhões de dispositivos smart ativos em todo o mundo, e estima-se que este número aumente para os 25.4 mil milhões até 2030; até 2025, os dados gerados por este tipo de dispositivos poderão atingir os 73.1 ZB (zettabytes). Um relatório conduzido pela The Avast 2019 Smart Home Security refere ainda que, e atendendo à data do estudo, cerca de 41% das smart homes tinham, pelo menos, um dispositivo vulnerável a ciberataques. É certo que, atualmente, este número seja superior devido ao crescimento da utilização destes dispositivos no nosso quotidiano.

Não sendo uma regra, podemos afirmar que a maioria dos ciberataques através deste tipo de dispositivos "inteligentes" seguem, por norma, o seguinte padrão: utilizando sistemas previamente comprometidos - zombies - que estão já controlados remotamente pelos criminosos (através de C&C - Comando e Controlo), são utilizados como "veículo" para procurar novas vítimas - se possível os ditos dispositivos inteligentes - nas redes, geralmente domésticas, onde residem. Posteriormente, após terem identificado o universo de potenciais vítimas - dispositivos inteligentes - utilizam malware para explorar vulnerabilidades específicas e daí controlar (também) remotamente os dispositivos. Daí em diante, tudo depende de quais dispositivos inteligentes foram comprometidos com sucesso e qual a sua função ou valor para os criminosos. Poderá ir desde roubo de

informação, por exemplo imagens de videovigilância, ou o controlo de acessos físicos às habitações (ex.: desligar o alarme, abrir portas, etc.), ou até, utilizar os dispositivos com veículos para realizar outros ciberataques.

Existem inúmeros motivos que refletem o acréscimo deste tipo de ataques e aos quais os utilizadores deverão estar bastante atentos, uma vez que podem levar à desativação de sistemas de segurança da vossa habitação ou até ao roubo de informações pessoais. Para evitar estes riscos indesejados, é fundamental que, ao decidir aderir a este novo conceito de smarthome, esteja preparado também para implementar mecanismos de segurança adequados à exposição e ao risco de segurança que passará a ter que conviver diariamente. Assim sendo, aplicam-se as boas práticas de segurança que implementamos no tecido empresarial, ou seja, a instalação de sistemas de segurança que monitorizem e controlo o comportamento da rede "doméstica", atualização - patch management - dos dispositivos inteligentes através dos próprios fabricantes, utilização de palavras-passe fortes e seguras com verificação pelo menos de dois fatores, rédea configuração (muito mais) exigente da rede de comunicação doméstica - wifi, wireless ou por ethernet - de forma a estabelecer uma arquitetura de rede adequada ao nível de exposição que passará a existir com a internet. É ainda essencial que mantenha os seus dispositivos inteligentes, tipicamente mais vulneráveis, em redes segregadas e protegidas, execute testes de segurança de forma contínua, e monitorize o comportamento da própria rede doméstica, como por exemplo, as autenticações que são efetuadas bem como o tráfego de atividade maliciosa através de sistemas de segurança inteligentes como firewalls de última geração. Por último e não menos relevante, é da máxima importância investir em dispositivos de boa qualidade onde os fabricantes tenham a cibersegurança como preocupação, e assim, não se tornem alvos fáceis de ataques que poderão comprometer a sua segurança e de todos os que habitam na sua rede doméstica.

As smart homes estão a revolucionar a forma como estamos e vivemos em casa, tornando como prioridade o pragmatismo, o conforto e o bem-estar. No entanto, no regresso pós-férias, se está a considerar tornar a sua casa mais inteligente e conectada com o mundo cibernético, aprenda também a mantê-la (ciber) segura e a protegê-la dos riscos cibernéticos que passará a ter de conviver daqui em diante. O salto para o mundo digital também obriga a uma responsabilidade maior.

Bruno Castro, Fundador e CEO da VisionWare - Sistemas de Informação SA.