INTERNET DAS COISAS

UM MUNDO TÃO VASTO QUANTO PERIGOSO

TEXTO *Ana Tulha*

Vivemos cada vez mais rodeados de aparelhos ligados à rede, desde os smartwatches às televisões, passando por frigoríficos, placas de fogão ou até torradeiras inteligentes. Mas se a IoT nos tem trazido um admirável mundo novo, ela também está carregada de perigos, sobretudo em termos de segurança e privacidade. Perceba os riscos que corre e como se proteger.

O caso foi notícia na semana passada. Lourenço, bebé de um ano, filho do futebolista Gonçalo Guedes e de Madalena de Moura Neves, estava a dormir a sesta quando a mãe, que estava noutra divisão, começou a ouvir uma música vinda do quarto. Aproximou-se e percebeu que a música vinha da câmara, apesar de ninguém a ter ligado. Mais estranho foi o facto de se tratar de uma música de igreja, que não constava sequer da playlist do aparelho. Assustada, desligou a ficha. Mais tarde, quando foi ver o histórico, percebeu que antes do momento musical se ouviu uma voz. "Conclusão: alguém 'hackeou' a câmara e estava a tentar interagir de alguma forma com o bebé ou connosco", partilhou, numa publicação feita nas redes sociais, para sensibilizar. "Hoje aconteceu uma coisa grave aqui em casa. Faço esta partilha para que estejam alerta e para que pensem que não acontece só aos outros", escreveu a esposa do atleta ex-Benfica, que defende atualmente as cores do Wolverhampton. Admitia até que já tinha visto vídeos de pessoas a partilhar situações semelhantes, mas que nunca achou que lhes pudesse tocar a eles. E acrescentava que desde então tinham uma câmara que não estava sequer conectada à Internet.

O episódio, necessariamente mais mediático por envolver a família de um futebolista conhecido, é espelho de muitos outros que acontecem diariamente pelo Mundo fora. Serve também de alerta geral para todos os riscos que estão inerentes à Internet das Coisas (ou IoT, do inglês "Internet of Things") e ao sem-fim de possibilidades que ela abre. Yasser Al Helaly, professor na NOVA IMS (Information Management School), investigador no MagIC (Information Management Research Center) e engenheiro informático com mais de 25 anos de experiência em cibersegurança, invoca uma expressão que é um bom resumo. Refere-se à IoT como "um campo minado num mundo conectado". E avança com um exemplo prático. "Uma família senta-se na sala de jantar em Lisboa, a desfrutar de uma noite tranquila. O frigorífico inteligente rastreia em silêncio os alimentos que lá estão dentro, os relógios vão contando os passos que dão e o termóstato ajusta automaticamente a temperatura da divisão em que se encontram. Sem que eles saibam, estes aparelhos que estão ligados à rede podem também estar a comunicar com mais alguém – um cibercriminoso determinado a explorar vulnerabilidades na Internet das coisas." Como faz questão de sublinhar, este "não é só um exemplo hipotético". "À medida que a adoção da IoT dispara, disparam também os riscos."

"[A IOT] É ESTA QUESTÃO DE TORNAR ELETRÓNICOS MUITOS DISPOSITIVOS QUE ANTES NÃO ERAM. DO FRIGORÍFICO À PLACA DO FOGÃO, PASSANDO PELA CAMPAINHA DA PORTA OU PELOS CARROS, PASSÁMOS A ESTAR RODEADOS DE DISPOSITIVOS QUE SÃO PEQUENOS COMPUTADORES"

Miguel Pupo Correia
Professor do Instituto Superior Técnico e investigador no INESC-ID

K/AIREL - STOCK.ADOBE.COM

"A SOCIEDADE AINDA NÃO VÊ ESTAS QUESTÕES COM GRANDE PREOCUPAÇÃO, O UTILIZADOR FINAL NÃO TEM NOÇÃO DE QUÃO IMPORTANTES SÃO OS SEUS DADOS, ACABA POR CONSENTIR E FACILITAR"

Dalila Durães
Professora na Escola de Engenharia da Universidade do Minho

O docente aponta dois números particularmente reveladores. Um é global e data de 2020, ano em que uma equipa de investigadores concluiu que 50% dos aparelhos que se integram na IoT estavam vulneráveis a ciberataques severos. O outro diz respeito à realidade portuguesa e é da ANACOM: em 2022, dois em cada cinco portugueses dependiam da Internet das Coisas para uso pessoal ou doméstico. Não custa adivinhar que o número será hoje bem mais significativo. E que, com este crescimento, aumentam também as vulnerabilidades. Antes disso, vale a pena explicar o que é a Internet das Coisas. Miguel Pupo Correia, professor do Instituto Superior Técnico e investigador no INESC-ID, na área da cibersegurança, responde assim: "É esta questão de tornar eletrónicos muitos dispositivos que antes não eram. Desde o frigorífico à placa do fogão, passando pela campainha da porta ou pelos carros, passámos a estar rodeados de dispositivos que são pequenos computadores, colocados em sítios inesperados." Dalila Durães, professora auxiliar na Escola de Engenharia da Universidade do Minho que se tem dedicado a vários projetos na área da Inteligência Artificial, acrescenta: "A Internet das Coisas é um conjunto de sensores que vão recolher dados e que podem ou não estar centralizados."

Logo aí, levanta-se uma questão pertinente. "Onde é que vão estar guardados esses dados e quem é que vai ter acesso a eles?", questiona a docente. "As aplicações já começam a ter um regulamento que obriga a ter de aceitar dados cookies de acesso, mas muitas vezes as pessoas nem prestam grande atenção. A sociedade ainda não vê estas questões com grande preocupação, o utilizador final não tem noção de quão importantes são os seus dados, acaba por consentir e facilitar. Estamos constantemente a ceder a nossa informação." E se nestas situações está inerente um certo grau de incúria, outros casos há em que o problema é mais lato e nos foge das mãos. Nelson Escravana, diretor de cibersegurança do INOV - INESC Inovação, admite isso mesmo. "Atualmente, há um conjunto muito variado de dispositivos, com capacidades de processamento muito diferentes, desde uma lâmpada, que tem zero, a uma televisão, que tem praticamente a capacidade de um computador. Como tal, as medidas de segurança que é possível aplicar também são muito distintas. E a questão é que há hoje uma grande variedade de fabricantes, há centenas, se não milhares de fabricantes distintos, o que torna muito difícil gerir a segurança dos dispositivos." Acresce que os utilizadores não têm noção do real impacto de ligar à sua rede doméstica câmaras de vigilância, até de bebés. "Muitas ve-

zes, apesar de estes aparelhos estarem ligados em rede, estão a enviar dados para fora, até para fora do espaço europeu, e não se sabe muito bem para onde vão nem quem tem acesso." Sendo que, com o número de dispositivos crescente que temos à disposição, "aumenta o número de oportunidades para um ataque ocorrer".

PORTAS ESCANCARADAS

Fábio Gomes, principal offensive security engineer na Devoteam CyberTrust (na prática, testa os softwares das empresas que os procuram, em busca de potenciais vulnerabilidades), também enfatiza este ponto. "Hoje em dia, tudo está a ficar ligado à Internet e isso faz com que haja cada vez mais portas de entrada para a vida das pessoas. Estes dispositivos permitem obter de forma direta ou indireta informações muito concretas, desde as horas a que chegam a casa àquilo que fazem no dia a dia. Muitos dispositivos são comprados a pequenos fabricantes, que não realizam sequer testes de segurança à procura de vulnerabilidades. Um dos grandes desafios é tentar manter todos os dispositivos seguros, com testes constantes." De resto, ao longo dos últimos anos, têm-se registado inúmeros casos que atestam as vulnerabilidades. Um dos que mais deu que falar foi o Mirai botnet, em 2016. O ataque afetou o serviço de Internet nos EUA e na Europa, deixando inacessíveis algumas das principais páginas mundiais, incluindo o Twitter (hoje X), as versões online do "The Guardian" e da CNN, a Netflix, o Spotify, o Reddit, entre muitos outros. Em suma, uma rede de dispositivos infetados com software malicioso, conhecida como "botnet", foi programada para bombardear um servidor com tráfico, até que este colapsasse. A questão é que, ao contrário do que era habitual, esta "botnet" não assentava em computadores propriamente ditos, mas antes em dispositivos da Internet das Coisas, tal como câmaras digitais e leitores de DVR. "Foram acedendo a uma série de dispositivos que estavam ligados à Internet, e que tinham nomes de utilizador e passwords fracas, e foram-nos comprometendo um a um, até conseguirem criar uma grande rede de dispositivos capaz de executar o ataque."

E quais são os dispositivos mais vulneráveis? Nelson Escravana aponta desde logo as câmaras, lembrando que "há imensos casos de câmaras vulneráveis que têm sido explorados". E até partilhados online, de forma a que qualquer pessoa possa aceder às imagens. Sendo que há um outro problema. "Às vezes um único aparelho vulnerável potencia o acesso ao resto da rede, pode servir como porta de entrada para o nosso computador e para os nossos sistemas de dados." Depois, os televisores. "Muitos vêm equipados com microfones e podem captar conversas sem que o utilizador se aperceba." Já fora da esfera doméstica, há ainda "uma grande preocupação em relação aos veículos autónomos e ao setor dos dispositivos médicos". Pela mesma razão, ainda que entrem em campos bem distintos: porque uma possível intrusão pode representar "perigo para a vida humana". Basta pensar, por exemplo, nos riscos que podem estar inerentes a uma bomba de insulina que pode ser controlada remotamente. Miguel Pupo Correia lembra ainda que a IoT vem criar um paradigma distinto, que devemos ter em mente. "Por um lado, a realidade passou a ser intermediada por estes aparelhos. Pensemos, por exemplo, num frigorífico que nos diz o que tem lá dentro. Nunca sabemos se corresponde à realidade ou não, porque há uma intermediação. Por outro lado, estes dispositivos atuam sobre a realidade. Num exemplo hipotético, alguém que consiga atacar um frigorífico pode estragar a comida e, no limite, envenenar as pessoas da casa. Ou pode simplesmente tornar os dispositivos indisponíveis, desligando-os ou impedindo o utilizador de aceder."

MAXIDISIGN - STOCK.ADOBE.COM

"SE NÃO PRECISAREM DO DISPOSITIVO, NÃO O TENHAM. SERÁ QUE PRECISAMOS MESMO DE TER UMA TORRADEIRA INTELIGENTE EM CASA? TEMOS DE ASSUMIR SEMPRE QUE OS DISPOSITIVOS PODEM ESTAR COMPROMETIDOS"

Fábio Gomes
Principal offensive security engineer na Devoteam Cyber Trust

A propósito de todos estes riscos, desde os mais domésticos e mais comummente explorados, a outras áreas em que ainda não há registo de grandes ataques mas em que os danos são potencialmente fatais, o que tem sido feito é suficiente? Fábio Gomes não tem dúvidas. "Nem de perto. Muitas das vulnerabilidades que vão sendo detetadas são-no à custa de pesquisas de investigadores independentes. No geral, as empresas não investem tempo suficiente a testar os dispositivos. E temos de ter em conta que um atacante é tipicamente uma pessoa motivada, com muito tempo livre e que tem em vista um grande benefício financeiro. As empresas nunca dedicam tanto tempo a estas questões como um atacante. A balança está desequilibrada e de alguma forma vai estar sempre, porque é uma corrida do gato e do rato. O que podemos fazer é aproximar-nos ao máximo. É preciso mais pesquisa, mais testes, mais investimento." Nem tudo é mau, ainda assim. "Há ainda um longo caminho a percorrer, mas notamos que começa a haver uma maior preocupação, há cada vez mais empresas que nos trazem dispositivos e aplicações para que as testemos." Para Nelson Escravana, a "ausência de estandardização" continua a ser um dos principais problemas. "Não há regulamentação específica nesta matéria, o que leva a que cada fabricante implemente mecanismos de segurança muito distintos. O consumidor tendencialmente procura o mais barato e, regra geral, nos produtos mais baratos, a segurança não é de todo uma prioridade."

"HÁ HOJE UMA GRANDE VARIEDADE DE FABRICANTES, HÁ CENTENAS, SE NÃO MILHARES DE FABRICANTES DISTINTOS, O QUE TORNA MUITO DIFÍCIL GERIR A SEGURANÇA DOS DISPOSITIVOS"

Nelson Escravana
Diretor de cibersegurança do INOV - INESC Inovação

Mas, afinal, que legislação é que se aplica nesta área? "Estes dispositivos não são diferentes, do ponto de vista tecnológico, de um computador ou de um telemóvel. Continuam a ser dispositivos que processam dados. Portanto, a regulamentação que se aplica é a do Regulamento Geral de Proteção de Dados [RGPD]." Mais recentemente foi dado, a nível europeu, um outro passo, muito significativo. "Foi publicada na segunda-feira [dia 18] a nova diretiva da responsabilidade do produtor [Diretiva (UE) 2024/2853]. Em causa está uma diretiva que vem já do tempo da CEE e que responsabiliza o produtor e demais intervenientes pelos danos que o produto possa causar, mesmo que não haja culpa direta do produtor. A questão é que agora passa a incluir especificamente o software e a consagrar o direito de o consumidor ter uma expectativa sobre a funcionalidade e a segurança de um dado software e dos produtos com componente digital." Sendo que esta diretiva terá de ser transposta para a legislação nacional até dezembro de 2026. "Este é um passo pioneiro a nível mundial, que vai obrigar os produtores a terem cuidados adicionais com a qualidade e a segurança", realça Nelson Escravana. Lembra ainda a publicação recente do novo regulamento europeu de resiliência cibernética (2024/2847), que estabelece "requisitos de segurança obrigatórios para produtos com componentes digitais, incluindo IoT".

REGRAS DE OURO

Do nível macro para o plano individual, há algo que possamos fazer para nos protegermos de possíveis intrusões (ou pelo menos minorarmos os riscos)? Há. Desde logo, apostar na ponderação. Miguel Pupo Correia dá o mote. "A pessoa tem de pensar na sua privacidade e na cibersegurança destes dispositivos de forma séria. No caso da saúde, por exemplo, será que faz sentido enviar os meus dados para uma aplicação que não conheço? Se pensarmos numa pessoa que está politicamente exposta, por exemplo, esta questão é ainda mais premente. E no caso do GPS, será que faz sentido permitir o acesso constante à localização e deixar que os dispositivos saibam todas as nossas rotinas? Eu, por exemplo, só dou acesso mesmo quando preciso de usar o GPS." Fábio Gomes deixa um alerta no mesmo sentido. "Se não precisarem do dispositivo, não o tenham. Será que precisamos mesmo de ter uma torradeira inteligente em casa? Temos de assumir sempre que os dispositivos podem estar comprometidos."

No sentido de reduzir vulnerabilidades, avança com alguns conselhos práticos. "Manter sempre o dispositivo atualizado é uma regra fundamental. As empresas vão sendo notificadas das vulnerabilidades existentes e tratam de fazer 'updates', alterações programáticas que fazem com que dadas falhas deixem de existir. Daí que seja tão importante ter sempre as atualizações mais recentes." Outro problema, de que já se vem com falando com frequência, é o facto de muitos utilizadores ainda manterem "credenciais de origem, muito fracas". "Isso facilita muito o acesso de intrusos, que nem têm de ser muito especializados. É importante alterar as passwords de origem e escolher passwords longas e difíceis. O ideal será até usar um bom password manager, que permita guardar todas as passwords. Assim deixa de se colocar a questão de termos de as decorar, pelo que podem ser mais complexas." O especialista deixa ainda outras dicas importantes. Por um lado, procurar "comprar dispositivos de vendedores confiáveis e com boa reputação", o que, à partida, aumenta a probabilidade de haver um cuidado maior com a segurança, e, por outro, "colocar sempre que possível estes dispositivos em redes wi-fi segregadas, ou seja, em redes separadas dos restantes dispositivos". Especificamente no caso das câmaras, também há um cuidado relativamente óbvio: "Nunca as ter em locais muito privados".

Yasser Al Helaly, da Nova IMS, reconhece que a responsabilidade "recai sobretudo sobre os produtores", mas recorda que os utilizadores também "desempenham um papel crítico" no que à mitigação de riscos diz respeito. E enumera algumas ações-chave: consciencializar para a segurança nesta área, e para a importância de cuidados já referidos com a atualização de firmware e o uso de passwords fortes; adotar, sempre que possível, a autenticação de multifator (MFA), um método de autenticação eletrónica em que um utilizador apenas consegue aceder a um site, serviço ou aplicação se apresentar com sucesso duas ou mais provas a um sistema de autenticação; implementar sistemas biométricos; segmentação de redes (já referida por Fábio Gomes); e, não menos importante, "mantermo-nos informados, seguindo as diretrizes e as atualizações de fontes confiáveis como a página "IoT For All". Em suma, o especialista entende que a colaboração entre produtores, reguladores e utilizadores é "essencial para garantir que os sistemas de IoT são seguros e confiáveis". "Afinal, apostar na segurança da Internet das Coisas não tem só que ver com a proteção de dispositivos – tem que ver com a proteção de todas as vidas e indústrias que eles afetam."

"APOSTAR NA SEGURANÇA DA INTERNET DAS COISAS NÃO TEM SÓ QUE VER COM A PROTEÇÃO DE DISPOSITIVOS – TEM QUE VER COM A PROTEÇÃO DE TODAS AS VIDAS E INDÚSTRIAS QUE ELES AFETAM"

Yasser Al Helaly
Professor na NOVA IMS e investigador no MagIC