INSPIRAÇÃO PARA INOVAR

# ÉPOCA NEGÓCIOS

SET 2018

INTERNET DAS COISAS

## Mais dados,

## mais lucros,

## mais hackers

**COMO CASAS, ROUPAS E OBJETOS ULTRACONECTADOS REVOLUCIONAM OS NEGÓCIOS**

O IMPACTO DA NOVA LEI DE PROTEÇÃO DE DADOS NO DIA A DIA DAS EMPRESAS

O BRASILEIRO QUE LIDERA O AVANÇO GLOBAL DA WHIRLPOOL RUMO AO LAR INTELIGENTE

A BATALHA ENTRE AS CORPORAÇÕES E OS CRIMINOSOS DA INTERNET

MAIS DADOS, MAIS LUCROS, MAIS HACKERS

# ESTADO DE EBULIÇÃO

**Ataques recentes alertaram as empresas que a IoT vai permitir ataques em escala nunca vista antes. É melhor prevenir**

**US$ 1,5 BILHÃO**

é o investimento global em segurança de IoT previsto para 2018


é o aumento previsto nesse investimento em comparação com o ano passado

**30 MINUTOS**

foi o tempo necessário para especialistas invadirem a maior parte dos equipamentos de IoT


dos dispositivos avaliados no Brasil apresentam vulnerabilidade acima da aceitável

Fontes: Gartner, Qualcomm, Universidade Ben-Gurion

conectadas. "Com a internet das coisas, vamos ter mais explorações de brechas de segurança. Vai ser um trabalho constante diminuir a frequência e o impacto desses ataques", afirma Pedro Paulo Pérez, vice-presidente de segurança digital do Grupo Telefônica e CEO da ElevenPaths, unidade de segurança da companhia.

Parte da responsabilidade é das fabricantes de equipamentos e prestadoras de serviços de rede. Produtos e serviços não são concebidos para oferecer o máximo de segurança. Permitir a conexão e o gerenciamento remoto dos aparelhos traz comodidade ao consumidor, mas o torna vulnerável a todo tipo de larápio do mundo digital. De acordo com um estudo realizado pela Universidade Ben-Gurion do Negev, Israel, divulgado em março, dispositivos conectados, como babás eletrônicas, câmeras, portas automáticas, segurança residencial e termostatos, foram facilmente invadidos por um grupo acadêmico que se dedicou a identificar as vulnerabilidades das redes domésticas.

Para o experimento, os pesquisadores dissecaram dispositivos inteligentes conectados à internet. Usaram técnicas de engenharia reversa e simularam ataques virtuais. "É assustadora a facilidade com que um criminoso, voyeur ou pedófilo toma o controle desses aparelhos", disse, em comunicado, o professor Yossi Oren, líder do laboratório de segurança digital da Ben-Gurion — num alerta para o fato de dispositivos conectados estarem próximos também de crianças e adolescentes. Segundo Oren, em apenas 30 minutos a equipe desvendou as senhas da maioria dos dispositivos, recorrendo a recursos simples como buscas no Google e uso dos manuais dos produtos.

No Brasil, uma equipe da Qualcomm reproduziu, em menor escala, o experimento. A demanda para testar aparelhos comumente encontrados no mercado surgiu de queixas de clientes. O resultado também foi alarmante: 70% dos dispositivos avaliados apresentaram, em média, 25 diferentes pontos de vulnerabilidade. Os riscos vão da facilidade para a invasão cibernética até a adição de peças. Ao desmontar um dos roteadores, José Palazzi, diretor de IoT da Qualcomm para a América Latina, deparou com uma placa sobressalente. A função do objeto era copiar os dados processados e enviá-los aos bandidos. O roteador estava nas mãos de uma equipe de instaladores de redes domésticas, e o contratante do serviço seria incapaz de perceber a manobra. "Os equipamentos têm de ser vedados para evitar este tipo de ação. É preciso proteger o hardware, o software e a rede", afirma. Silmar Palmeira, diretor de inovação e tecnologia de rede da TIM, concorda que, diante da transformação, vamos precisar de camadas extras de proteção nos ambientes domésticos, com sistemas redundantes e cuidados especiais com os sensores que captam informações sobre a vida dos usuários.

**Jose Palazzi, diretor de IoT na Qualcomm, já topou com quadrilhas que inserem placas espiãs em roteadores**

A reação das grandes companhias tem sido mais lenta que o ideal. "As empresas buscam parcerias para produzir aparelhos mais seguros e difíceis de invadir", comenta Sudha, da Universidade Stanford. Segundo ela, a intenção é estabelecer padrões e acordos de conectividade entre os dispositivos e protegê-los desde o desenho industrial. "É possível projetar aparelhos mais seguros", comenta. Alguém se habilita?

A IoT vai exigir mais empenho das organizações porque, além de corrigir seus próprios produtos e serviços, empresas vão precisar pensar com a cabeça do usuário médio, sem tempo nem conhecimento para garantir sua própria segurança digital. Thiago Bordini, diretor de inteligência cibernética e pesquisa do Grupo New Space, explica que, até agora, não há padrões de segurança estabelecidos para os dispositivos domésticos. A maior parte das configurações é feita diretamente no equipamento e depende de ação do usuário. "Mas as pessoas não sabem que precisam configurar uma senha", explica. Durante a entrevista, Bordini acessou o site Shodan, espécie de Google da internet das coisas. Procurou, no Brasil, por um modelo específico de TV inteligente. Em segundos, obteve a lista com o endereço de internet (IP) de 22 aparelhos. "Para sair da lista, é preciso mudar as configurações do equipamento", indica. Especialistas vão ser muito trabalho educativo a fazer. Em dezembro passado, três profissionais da área — dois da IBM e um da escola politécnica de Montreal — publicaram uma sugestão de estrutura de segurança para a rede inteira, que consideram ser à prova de ignorância tecnológica dos usuários. Chamaram seu sistema de HIoT.

Silmar Palmeira, diretor de inovação e tecnologia da TIM: IoT residencial exige atenção extra dos provedores de serviços

Enquanto fabricantes de equipamentos e usuários tentam se adaptar, o setor de segurança digital anteve muito trabalho. Companhias tradicionais no ramo, como Symantec, McAfee e F-Secure, passaram a oferecer serviços específicos para IoT residencial. As estratégias englobam desde a oferta direta ao consumidor até a inclusão de recursos de segurança nos serviços de conexão, comunicação e entretenimento. "Esse modelo exige a parceria dos desenvolvedores com os provedores de serviços de internet e operadoras de telecomunicações", explica Annette, do Gartner. As startups também estão no páreo e devem chacoalhar os modelos de negócios no ramo de proteção das casas conectadas. Entre as novatas, a especialista destaca a BitDefender, da Romênia, e a Cujo, de Los Angeles.

Fundada nos Estados Unidos, a Cujo tem equipes de desenvolvimento na Lituânia — responsável pelos sistemas que rodam na nuvem — e no Brasil, que concentra a parte do software que vai embarcada nos dispositivos, o firmware.