1.Vulnerabilidades de Hardware

Em qualquer rede doméstica ou corporativa, diversos dispositivos estão conectados, muitos dos quais possuem sistemas operacionais internos que não são acessíveis ao usuário. Esses dispositivos podem incluir sistemas de ar-condicionado, relógios de ponto e diversos outros equipamentos que funcionam de forma autônoma. Embora o sistema operacional desses dispositivos não esteja visível, ele ainda pode apresentar riscos de segurança, já que, ao estarem conectados à rede, tornam-se potenciais alvos para ataques.

Com o avanço da Internet das Coisas (IoT), esses riscos aumentaram significativamente. Antigamente, a preocupação com a segurança digital se restringia a sistemas operacionais tradicionais como Windows, macOS e Linux. Hoje, qualquer eletrodoméstico inteligente, como fogões, geladeiras, fechaduras eletrônicas e sistemas de garagem, pode representar um ponto de vulnerabilidade caso não esteja devidamente atualizado. Esses dispositivos funcionam por meio de firmware, que é o software interno responsável pelo seu funcionamento. No entanto, a maioria dos usuários não tem controle sobre esse firmware, e a única forma de atualizá-lo depende do fabricante.

O problema é que muitas empresas que produzem esses dispositivos não priorizam a segurança cibernética como deveriam. Um exemplo disso foi o caso dos termostatos Trane Comfortlink II. Esses dispositivos automatizados, que podem ser controlados por celulares e tablets, apresentaram vulnerabilidades de segurança identificadas em abril de 2014. No entanto, o fabricante levou um ano inteiro para lançar a primeira atualização corretiva, que só foi disponibilizada em abril de 2015. Uma segunda correção ainda demorou mais um ano, sendo lançada apenas em janeiro de 2016.

Enquanto grandes empresas de software, como Microsoft e Apple, costumam lançar atualizações de segurança em menos de um mês, no mundo dos dispositivos IoT as correções podem levar anos. Durante esse período, os usuários desses termostatos estavam expostos a falhas conhecidas sem nenhuma solução disponível. Além da demora nas atualizações, existe também o problema do fim do suporte dos dispositivos. Quando um fabricante decide descontinuar um produto, ele emite um aviso chamado **EOL (End of Life)**, **indicando que o dispositivo deixará de ser vendido**. Mesmo após o EOL, ainda podem ser oferecidas atualizações de segurança por um tempo, mas isso não dura para sempre.

Quando o suporte oficial termina completamente, o dispositivo entra no status de **EOS (End of Service)**. **Nesse ponto, nenhuma nova atualização de segurança é fornecida, tornando o equipamento vulnerável**. Em alguns casos, fabricantes oferecem suporte pago para clientes empresariais, mas o custo costuma ser muito alto.

Para a maioria das pessoas, a única opção viável é substituir o equipamento por um modelo mais recente.

Em empresas com grandes infraestruturas de TI, a situação pode ser ainda mais complicada. Equipamentos antigos podem estar em uso há anos, rodando softwares desatualizados e middleware ultrapassado. Nesses casos, cabe aos administradores avaliar se o risco de continuar usando esses dispositivos supera os custos e desafios de substituí-los. Quando a substituição imediata não é possível, algumas medidas paliativas podem ser adotadas, como a criação de regras de firewall para restringir o acesso ao dispositivo ou a implementação de assinaturas de detecção de ameaças específicas para sistemas antigos.

Embora dispositivos legados nem sempre possam ser removidos rapidamente, é fundamental ter um plano para substituí-los e, ao mesmo tempo, adotar medidas que minimizem os riscos de segurança. Isso garante que a rede permaneça protegida enquanto a transição para novas tecnologias ocorre de forma planejada e segura.