Entendendo segurança em sistemas IoT: A segurança da sua casa e dos seus dados pode estar ameaçada.

Murilo Henrique Galvão De Sousa Azevedo | murilo.hgs@aluno.ifsc.edu.br
Maykon Chagas | maykon.chagas@ifsc.edu.br
Andrei de Souza Inácio | andrei.inacio@ifsc.edu.br

Vulnerabilidades em Internet das Coisas

A Internet das Coisas (IoT) é uma tecnologia que conecta dispositivos físicos à Internet com a função de automatizar e facilitar tarefas do dia a dia. Hoje, é comum encontrar câmeras, sensores de presença e fechaduras inteligentes que se comunicam por meio do Wi-Fi. Esse tipo de tecnologia vem crescendo rapidamente no Brasil. De acordo com a Forbes (2024), o uso da assistente virtual da Amazon (Alexa) conectada a dispositivos IoT aumentou 50% no país em 2023, o que mostra o quanto essa tecnologia está se tornando comum nas residências brasileiras. Com esse crescimento, surgem também preocupações em relação à segurança desses dispositivos. Muitos deles lidam com dados pessoais e, se mal configurados ou com falhas, podem se tornar alvos fáceis para ataques. A OWASP (Open Worldwide Application Security Project), uma fundação sem fins lucrativos focada na segurança de software, criou em 2014 o projeto “OWASP IoT” para identificar as principais vulnerabilidades em dispositivos IoT. A lista mais recente, atualizada em 2018, aponta dez falhas comuns encontradas em diversos equipamentos conectados.O objetivo deste trabalho foi analisar essas vulnerabilidades com base na lista da OWASP, entender os riscos que os usuários enfrentam e mostrar como essas falhas acontecem e de que forma elas podem ser evitadas. A metodologia da pesquisa foi baseada em uma revisão bibliográfica de artigos acadêmicos e materiais técnicos recentes, cruzando informações da lista oficial da OWASP com dados atuais sobre o uso de IoT no Brasil. A análise revelou que muitas das vulnerabilidades ainda são frequentes em dispositivos vendidos atualmente. Entre elas estão o uso de senhas fracas (ou as que já vêm de fábrica), componentes desatualizados e a transferência de dados sem criptografia. Também foi observado que parte dessas falhas acontece por falta de conhecimento do próprio usuário, que muitas vezes não sabe que é possível configurar o dispositivo de forma mais segura. Essas vulnerabilidades são preocupantes, principalmente porque o Brasil é o segundo país mais afetado por ataques cibernéticos, segundo a Forbes (2025), sendo o mau uso de senhas um dos principais motivos. Por isso, além da responsabilidade dos fabricantes em melhorar a segurança dos produtos, é importante que os usuários sejam orientados a adotar práticas mais seguras, como usar senhas fortes, ativar autenticação em dois fatores, manter os dispositivos atualizados e acessar apenas sites com certificado TLS e protocolo HTTPS. Conclui-se que o avanço da IoT exige não só mais segurança nos dispositivos, mas também mais informação e conscientização para quem usa a tecnologia no dia a dia.

Palavras-chave: cibersegurança; dispositivos IoT; segurança da informação