# Avaliação de segurança em dispositivos IoT

Gustavo Araujo[1], Roben Castagna Lunardi[1*]

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - *Campus* Restinga. Porto Alegre, RS.
*Orientador(a)

Nos últimos anos tivemos um crescimento na área da tecnologia, ao combinar Hardware e Software desenvolvendo dispositivos que permitem efetuar coleta de dados entre objetos e sistemas, Dispositivos Iot (Internet das Coisas) estão se tornando cada vez recorrente na vida do cidadão brasileiro, revolucionando setores como saúde, indústrias e automação residencial. Atualmente os dispositivos IoT mais conhecidos que podemos encontrar em algumas residências são a Alexa (Amazon) e o Google Nest (Google). Os Dispositivos IoT na atualidade possuem diversos padrões de segurança para melhor confiabilidade ao usuário, tendo como principal o atual Protocolo Matter (Sucessor do Projeto CHIP), desenvolvido para a melhorar a interoperabilidade, segurança e usabilidade desses dispositivos, porém, muitos destes dispositivos são mantidos sem uma avaliação de segurança necessárias para a melhor confiabilidade ao usuário, tornando assim, suscetíveis a ataques, podendo ocorrer vazamentos de dados privados. Portanto, realizar avaliações de segurança é uma prática importante para encontrar possíveis vulnerabilidades nos serviços. Uma das principais metodologias e técnicas para essas avaliações é o Teste de Intrusão (Pentest), utilizado para detectar vulnerabilidades por meio de ataques simulados (ou até mesmo em ambientes de produção), tendo diversas maneiras para realizar testes, utilizando frameworks para: organizar a execução dos testes, executar ferramentas, fornecer estimativas, fornecer relatórios e documentar um Pentest[4]. Foi divulgado em 2022 pela empresa Cynerio, uma pesquisa a qual aponta que mais de 50% dos dispositivos IoT médicos possuem vulnerabilidades críticas e 53% dos dispositivos médicos conectados à Internet analisados apresentavam vulnerabilidades já conhecidas. A avaliação de segurança em cima dos dispositivos com plataformas abertas e dispositivos comerciais compatíveis com os assistentes virtuais, sendo aplicadas técnicas de Pentest de acordo com metodologias recomendadas, como Tramonto e OWASP. Os testes visam o encontro dessas vulnerabilidades que possam comprometer os dispositivos, assim como a documentação dessas vulnerabilidades, metodologias e melhorias a serem realizadas. A divulgação deste material por meio de relatórios e tutoriais para destacar a importância dos Pentests. Resultados serão publicados em eventos científicos, contribuindo para a conscientização e aprimoramento da segurança em dispositivos IoT.

Palavras-chave: Segurança da Informação; Internet das Coisas; Testes de Intrusão; Ethical Hacking.




CNPq FAPERGS