Desafios e Soluções na Segurança da Internet das Coisas(IoT)

1st Fabrício Silva Dias
Sistemas de Informação - UFG
Senador Canedo, Brasil
fabricio_silva@discente.ufg.br

2nd Filipe Augusto Lima Silva
Sistemas de Informação - UFG
Goiânia, Brasil
filipe_augusto@discente.ufg.br

3rd Guilherme Pereira Fernandes
Sistemas de Informação - UFG
Goiânia, Brasil
guilherme_fernandes@discente.ufg.br

4th João Felipe Peres Lima
Sistemas de Informação - UFG
Goiânia, Brasil
joaofelipe2@discente.ufg.br

5th Philippe Augusto Monteiro Silva
Sistemas de Informação - UFG
Goiânia, Brasil
philippe_silva@discente.ufg.br

***Abstract*—Com grande adesão de dispostivos que usam da internet para coletar, transmitir ou trocar dados cada vez mais se faz urgente soluções para lidar com os desafios de segurança na Internet das Coisas (IoT). Assim, esse documento tem por objetivo: definir Internet das Coisas(IoT); pontuar as diferentes áreas de uso da Iot na sociedade, e ampla gama de dispositivos; principais desafios encontrados na garantia de segurança dos dados; exemplos de vulnerabilidades existentes; medidas essenciais. A IoT gera uma grande massa de dados e garantir a integridade destes é crucial.**

***Index Terms*—IoT, Vulnerabilidade, Segurança, Ataques Cibernéticos.**

I. Introdução

A Internet das Coisas(IoT) ou "Internet of Things" é um conceito abrangente, criado por Kevin Ashton, pioneiro tecnológico britânico, em 1999 e a comunicação entre objetos físicos, por meio da internet, com objetivo de coletar, transmitir ou trocar dados teve início em 1990 por meio da Internet Toaster criada por John Romkey.

A IoT é um tema emergente de importância no âmbito social e também econômico. Esses dispositivos vêm transformando as formas de viver, realizar atividades ou trabalhar. Presente em vários âmbitos sociais, como : Na saúde, possibilitando o monitoramento remoto de pacientes e gestão de medicamentos; Em cidades inteligentes, otimiza o tráfego, melhora a gestão de resíduos e promove a segurança pública; Na agricultura, sensores monitoram condições climáticas e otimizam a irrigação; Na indústria, contribui para manufatura inteligente e manutenção preditiva. Essas aplicações, entre outras, destacam a versatilidade da IoT na transformação positiva de setores e na qualidade de vida.

Entretanto, conforme cresce o uso de IoT na sociedade, os ataques cibernéticos à estes dispositivos também cresce de maneira equivalente, segundo relatórios da Check Point Software Technologies, empresa de soluções de segurança digital, no ano de 2023 mais de 50% das organizações foram alvos de ataques direcionados a dispositivos IoT, como roteadores, câmeras IP e impressoras.

Não obstante, tivemos um transformação tecnológica impulsionada pela pandemia da covid-19, onde redes de aprendizado e empresas aderiram a ambientes digitais de comunicação. Como consequência disto o uso de câmeras IP e demais dispositivos IoT tornaram-se mais comuns, aumentando as entradas possíveis para os cibercriminosos e dificultando mais as formas de garantir a integridade de informações. Entre os setores mais afetados, a educação e pesquisas estão entre os principais alvos de ataques, concentrando 131 ataques semanais.

A vasta quantidade de dispositivos conectados aumenta a exposição a ameaças, e na tentativa de mitigar esses riscos é necessário que usuários e fabricantes compartilhem da responsabilidade cabível a ambas as partes. O fabricante na garantia de um projeto seguro, atualizações de Firmware, implementação de fortes meios de autenticação e fornecer informações sobre práticas segura, as quais devem ser seguidas pelo usuários, além de seguir essas instruções devem também manter o seu dispositivo atualizado, colocar senhas fortes e monitorar atividades suspeitas.

II. Fundamentos Teóricos

Todo dispositivo conectado à internet está vulnerável a ataques cibernéticos, e existem diversas possibilidades e pontos visados em cada tipo de ataque, cada um utilizando uma vulnerabilidade diferente. Esses ataques podem ser divididos em três tipos:

- Ataques por Engenharia Social: Foco em manipular usuários para obtenção de informações confidenciais ou realizar ações prejudiciais (Phishing, Ransomware).
- Ataques ao Sistema: Foco em comprometer a integridade do sistema ou sua disponibilidade (Ataque de Negação de Serviço(DoS), Ataques de Força Bruta, Injeção de Código(SQL, XSS)).

Identify applicable funding agency here. If none, delete this.

- Ataques a Dispositivo IoT: Foco em ter acesso/controle sobre um dispositivo conectado(Exploração de vulnerabilidade em dispositivo IoT).

Para lidar com os ataques cibernéticos aliados a vulnerabilidade do sistema, têm-se os seguintes mecanismos:

A. Ataques ao Sistemas

- Firewalls
- Sistema de Detecção de Intrusões(IDS)
- Sistemas de Prevenção de Intrusões

Esses mecanismo são mais utilizados na tentativa de prevenção dos ataques, atualizações em vulnerabilidades conhecidas e monitoramento contínuo são também medidas válidas.

B. Ataques por Engenharia Social

- Filtros de e-mail
- Software Antivírus

Ressalta-se também o treinamento de usuários para reconhecer e evitar ataques de phishing

C. Ataques a dispositivos IoT

- Atualizações de firmware
- Segmentação de rede
- Políticas de Segurança

Manter os dispositivos IoT atualizados com as últimas correções de segurança e patches de firmware é de suma importância, por corrigir as vulnerabilidades e melhorar a segurança global, junto com a implementação robusta, por meio de senhas fortes ou metodos multifatores dificultando a entrada de invasores. Firewall baseado em rede é também uma técnica válida, pois protege os dados assim que os mesmo entram na rede, permitindo também monitorar e bloquear o tráfego fora de sua VPN, muito útil principalmente em dispositivos M2M que possuem capacidade de processamento limitada.

Parte dos desafios encontrados, quanto ao assunto de segurança em dispositivos IoT se deve as particularidades únicas de cada ecossistema, visto a grande variedade de dispositivos, impossibilitando a criação de uma solução de forma universal. Além disto, muitos dos dispositivos são compactos e móveis, assim têm maiores limitações quanto a utilização de energia, capacidade de processamento e também armazenamento, o que faz necessário soluções de segurança que além de eficazes sejam otimizadas, para não comprometer o desempenho.

REFERENCES

[1] DE OLIVEIRA, Nairobi Spiecker et al. Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). Revista Eletrônica de Iniciação Científica em Computação, v. 17, n. 4, 2019.

[2] CARVALHO, André Ferreira Almeida de; SANTOS, Christyan Matteus Lima; GONÇALVES, Lucas Vaz. Segurança em IoT. 2022.

[3] ABRANET. *Ataques a disposiftivos da Internet das Coisas (IoT) crescem 41%*. ABRANET. 24/04/2023. Disponível em: https://www.abranet.org.br/Noticias/Ataques-a-dispositivos-da-internet-das-coisas-(IoT)-crescem-41%25-4300.html? Acesso em: 16 jan. 2024.

[4] Carlos Campo. *O que é Segurança em IoT? Riscos, Exemplos e Soluções*. EMNIFY. Disponível em: https://www.emnify.com/pt-br/glossario-iot/seguranca-iot#:~:text=Falta%20de%20criptografia&text=Muitos%20dispositivos%20IoT%20n%C3%A3o%20criptografam,transmitidas%20para%20e%20do%20dispositivo.. Acesso em: 16 jan. 2024.

[5] DE OLIVEIRA, Nairobi Spiecker et al. Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). Revista Eletrônica de Iniciação Científica em Computação, v. 17, n. 4, 2019.