CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA CURSO DE GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

ALEX CARVALHO DE SANTANA
BRUNO ANDRADE MENDES DE FRANÇA
MANNEX FERREIRA DA SILVA LIMA

ESTUDO DAS VULNERABILIDADES DOS DISPOSITIVOS RESIDENCIAIS COM IOT E POSSIBILIDADES DE COMO REDUZI-LAS.

RECIFE/2023

ALEX CARVALHO DE SANTANA
BRUNO ANDRADE MENDES DE FRANÇA
MANNEX FERREIRA DA SILVA LIMA

ESTUDO DAS VULNERABILIDADES DOS DISPOSITIVOS RESIDENCIAIS COM IOT E POSSIBILIDADES DE COMO REDUZI-LAS.

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: Msc Ameliara Freire Santos de Miranda
Professor Orientador: Msc. Luiz Sérgio Ferreira de Lima

RECIFE/2023

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

S231e Santana, Alex Carvalho de.
Estudo das vulnerabilidades dos dispositivos residenciais com iot e possibilidades de como reduzi-las / Alex Carvalho de Santana; Bruno Andrade Mendes de França; Mannex Ferreira da Silva Lima. - Recife: O Autor, 2023.
25 p.

Orientador(a): MSc. Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2023.

Inclui Referências.

1. IoT. 2. Vulnerabilidades. 3. Segurança. 4. Residências inteligentes. I. França, Bruno Andrade Mendes de. II. Lima, Mannex Ferreira da Silva. III. Centro Universitário Brasileiro. - UNIBRA. IV. Título.

CDU: 004

AGRADECIMENTOS

Primeiramente, agradeço a Deus aos meus amigos e familiares e professores que me ajudaram para obter a concretização deste TCC, e em especial a minha esposa Diane Glayce por compreender e me ajudar nos momentos em que eu estava ocupado desenvolvendo este trabalho.

ALEX CARVALHO DE SANTANA

À Deus, aos meus pais, Mendes e Nalva, minhas tias Leda, Leda, Albonize e Cleide e minha namorada Mikaela.

BRUNO ANDRADE MENDES DE FRANÇA

Agradeço a Deus, a minha família e meus amigos de faculdade por ter me dado suporte para conseguir passar por cada etapa desses dois anos e meio aos professores que fizeram parte deste processo e de uma pessoa que nos deu ajudou com este trabalho e nos orientou da melhor maneira possível, obrigado à todos.

MANNEX FERREIRA DA SILVA LIM

SUMÁRIO

ESTUDO DAS VULNERABILIDADES DOS DISPOSITIVOS RESIDENCIAIS COM IOT E POSSIBILIDADES DE COMO REDUZI-LAS.

ALEX CARVALHO DE SANTANA

BRUNO ANDRADE MENDES DE FRANÇA

MANNEX FERREIRA DA SILVA LIMA

Profº Msc Ameliara Freire Santos de Miranda - Orientadora

RESUMO:

A internet das coisas (IoT), tem como definição, uma rede de objetos físicos, contendo algum tipo de software, sensor e outras tecnologias, para se conectar na internet com algum outro dispositivo e trocar dados, trazendo muita praticidade e comodidade ao seu usuário. Contudo, as preocupações estão voltadas para a segurança dos dados de quem utiliza essa tecnologia. O objetivo deste trabalho foi identificar as vulnerabilidades em residências que utilizam dispositivos com IoT e como reduzi-las. O estudo foi qualitativo, com natureza descritiva e exploratória. Os dados foram coletados através de pesquisa bibliográfica de diversos autores na área de IoT com foco principal em ambiente residencial, a fim de buscar uma maior confiança na utilização dessa tecnologia sem receio de os dados pessoais seja exposto a vazamentos cibernéticos, onde ficou claro os dispositivos estão sendo cada vez mais atacados se tornando vulneráveis. Foram pesquisadas quais as formas e medidas de prevenção deverão ser tomadas para reduzir os ataques a dispositivos que são utilizados em ambiente residencial.

Palavras-Chaves: IoT. Vulnerabilidades. Segurança. Residências Inteligentes

STUDY OF THE VULNERABILITIES OF RESIDENTIAL DEVICES WITH IOT AND POSSIBILITIES OF HOW TO REDUCE THEM

ALEX CARVALHO DE SANTANA

BRUNO ANDRADE MENDES DE FRANÇA

MANNEX FERREIRA DA SILVA LIMA

Profº Msc Ameliara Freire Santos de Miranda – Advisor

ABSTRACT:

The internet of things (IoT) is defined as a network of physical objects, containing some kind of software, sensor and other technologies, to connect to the internet with another device and exchange data, bringing a lot of practicality and convenience to its user. However, concerns are focused on the security of the data of those who use this technology. The objective of this work was to identify vulnerabilities in homes that use IoT devices and how to reduce them. The study was qualitative, with a descriptive and exploratory nature. The data were collected through a bibliographical research of several authors in the field of IoT with a main focus on the residential environment, in order to seek greater confidence in the use of this technology without fear of personal data being exposed to cyber leaks, where it was clear that devices are being increasingly attacked, becoming vulnerable. It was researched which forms and preventive measures should be taken to reduce attacks on devices that are used in a residential environment.

Keywords: IoT. Vulnerabilities. Security. Smart Homes

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

AMQP = Advanced Message Queuing Protocol
CFTV= Circuito Fechado de Televisão
CoAP =Constrained Application Protocol
DDS = Data Distribution Service
DDoS= Distributed Denial of Service
HTTPS = Hyper Text Transfer Protocol Secure
IoT= Internet Of Things
IP= Internet Protocol
LoRaWAN= Long Range Wide Area Network
M2M= Machine-to-Machin
MITM = Man-in-the-Middle Transport
MQTT = Message Queue Telemetry
NFC= Near Field Communication
OWASP=Open Web Application Security Project
RAM= Random-Acess Memory
REST = Representational State Transfer
RFID= Radio Frequency Identification
ROM= Read-Only Memory
SSH = Secure shell
TELNET= Teletype Network
USB = Universal Serial Bus
XMPP= Extensible Messaging and Presence Protocol

1. INTRODUÇÃO

Nos dias atuais, a interação das pessoas com dispositivos eletrônicos está cada vez mais abrangente, crescendo em larga escala (CRYPTO ID, 2023). IoT "*Internet of Things*", que traduzindo para nossa língua significa: "Internet das Coisas", foi um termo criado por Kevin Ashton, em 1999 enquanto realizava uma palestra para *Procter & Gamble* (P&G), onde falava sobre uma nova ideia do sistema RFID *(Radio Frequency Identification)* para a rastreabilidade do produto na cadeia de suprimentos (MANCINI, 2019).

O IoT usa a nuvem como um dos meios de interligação com os dispositivos, tendo como finalidade de coletar e enviar dados, através de sensores, acarretando grande praticidade para aqueles que acessem tais informações (MANCINI, 2019). Com ajuda de aplicativos, como por exemplo: Google Cloud, Smart Things, Positivo casa inteligente, Mactive Pro, entre outros... é possível controlar e monitorar, em tempo real, essas informações coletadas por cada sensor, e como consequência, tomar decisões baseadas nesses resultados (PONTOTEL, 2022)

Conforme site Terra (2022), a expectativa é que até 2025, no mundo, mais de 27 bilhões de dispositivos do cotidiano da sociedade estarão conectados. Assim, com o crescimento dessa tecnologia em diversos ambientes, a IoT nas residências não podia ficar de fora. O conceito de "Casa Inteligente" está cada vez mais presente nas cidades mais desenvolvidas. Surgem dispositivos dotados de inteligência, através de sensores IoT em lâmpadas, geladeiras, tomadas, ar - condicionado, chuveiro etc. Os sensores fazem a conexão aos dispositivos de internet, para que permita a comunicação a outros sistemas computacionais. O IoT residencial melhora em grande escala na vida dos moradores da Casa Inteligente, pois os aparelhos vêm facilitando a vida das pessoas nas casas inteligentes (FISHER, 2019). Com esse novo conceito, conforme Wanzeler, Fulber e Merlin (2016), a automação residencial veio para beneficiar a vida da sociedade, se comparado com equipamentos que não possuem essa tecnologia e funcionam isoladamente.

A evolução da Internet das Coisas, vem causando grandes impactos no dia a dia das pessoas dentro de suas residências. Com avanço tecnológico foi possível ter objetos eletrônicos cada vez mais práticos, e com isso temos além dos smartphones e computadores pessoais outros dispositivos como, geladeira, termostaticos, smartwhatch, que poderão identificar padrões e assim processar informações e

executar tarefas com apenas um clique ou nenhum clique. Hoje já podemos encontrar equipamentos e soluções para automatizar uma residência conectando ou integrada à aplicativos (BIT 2000, 2021).

Contudo, vale destacar que, paralelamente ao crescimento dessa tecnologia, cresce também a vulnerabilidade na segurança, visto que, quando os aparelhos estão conectados a internet podem estar vulneráveis e serem invadidos por Hackers, por não ter uma configuração adequada de segurança, como uma senha forte, por exemplo. Isso ocasiona o vazamento de dados e dão acesso às informações confidenciais dos indivíduos para fins ilícitos (FISHER, 2019).

Sabe-se que muitos dispositivos ligados à internet não são desenvolvidos para criptografar as saídas de dados, facilitando o ataque de pessoas com intenções maliciosas. De acordo com Greene (2019), em pesquisa realizada pelo provedor de segurança baseado na nuvem Zscaler, identificou que 91,5% das transações de dados realizadas por dispositivos IoT em redes corporativas não são criptografadas, ficando suscetíveis a vários tipos de ataques. Isso ocorre devido aos dispositivos IoT ficarem, em grande parte, localizados nas extremidades da rede e fisicamente em locais de fácil acesso. Assim, é necessário ter medidas de segurança, uma vez que muitos dispositivos são desenvolvidos com pouca capacidade de processamento, já que são criados pensando no baixo consumo energético, dificultando a aplicação de técnicas de segurança.

1.1 PROBLEMA

Os dispositivos são fabricados com tamanho reduzido, tendo restrições com memória, processamento, energia, *bandwidth.* Isto conduz a uma grande preocupação, pois não é dada a atenção devida no aspecto de alcançar a segurança mínima necessária, como portas padrões alteradas, criptografias avançadas entre outras, para a utilização destes dispositivos. (NOBRE *et al.*, 2019). Assim, a coleta, a transmissão e o armazenamento dessas informações (dados) pessoais e, muitas vezes sigilosos, apontados na lei, se torna um “problema” quando estamos falando desses dispositivos. (NOBRE *et al.*, 2019). Em um ambiente residencial existem vários dispositivos com essas características, como notebooks, celulares, smart TV, micro-ondas, ar-condicionado, sistema de monitoramento, iluminação, cortinas e etc...

Diante desse contexto, surge a seguinte pergunta: Como diminuir a vulnerabilidade em residências que utilizam dispositivos com IoT?

1.2 JUSTIFICATIVA

Faz-se necessário conhecer as várias formas de vulnerabilidades como falta de mecanismo para atualização, senhas fracas, proteção de privacidades insuficientes, para se resguardar no sentido de prevenir e de como deve ser feita a prevenção nos dispositivos para o qual vai ser usada para automação residencial, diminuindo os impactos para que a presença de pessoas não autorizadas na rede diminua a cada dia.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Identificar as vulnerabilidades em residências que utilizam dispositivos com IoT e como reduzi-las.

1.3.2 OBJETIVOS ESPECÍFICOS

- Compreender os conceitos das vulnerabilidades em dispositivos com IoT;
- Identificar os dispositivos de IoT que são usados nas residências, observando os mais suscetíveis a ataques de invasores na rede.
- Apontar medidas para reduzir os ataques aos dispositivos com IoT nas residências.

1.4 ANÁLISE DAS VULNERABILIDADES DO IOT (METODOLOGIA)

Esta pesquisa realizada neste trabalho pode ser classificada como exploratória, pois busca um conhecimento mais aprofundado do problema, a fim de torná-lo mais evidente e por admitir maior flexibilidade para seu planejamento, favorecendo a uma maior abrangência do que está sendo estudado (GIL, 2017). Este trabalho objetivou

identificar as vulnerabilidades em residências que utilizam dispositivos com IoT e como reduzi-las.

Quanto ao método, foi escolhido a Pesquisa Bibliográfica, uma vez que conduz a uma aproximação direta dos pesquisadores com o que já foi publicado sobre o tema, possibilitando uma nova visão do mesmo (MARCONI; LAKATOS, 2017). A pesquisa foi dividida nas seguintes etapas:

1) Coleta de estudos em bases de dados;
2) Seleção dos estudos;
3) Análise dos estudos selecionados;
4) Síntese dos resultados encontrados.

Para a primeira etapa, foi realizado um levantamento de trabalhos publicados nos últimos 06 anos (de 2018 a 2023), sendo utilizado com base de dados na coleta: Google Acadêmico, Researchgate, Revista Brasileira de Computação Aplicada, *International Journal of Network Security & Its Applications (IJNSA)*, Revista Computação Brasil. Para localizar os trabalhos, foram usados os seguintes termos nas pesquisas: Dispositivos de IoT, Segurança da informação, Vulnerabilidade no IoT, Casas inteligentes e Protocolos de segurança do IoT. Nesta etapa foram coletados 38 trabalhos

Na segunda etapa, os trabalhos coletados passaram por uma seleção, tendo sido empregados os seguintes critérios para a escolha: a) os artigos que continham os termos utilizados na pesquisa; b) os que estavam mais relacionados com a temática estudada, sendo descartados os que aparecem repetidos em mais de uma base de dados utilizada e aqueles que focaram apenas em dispositivos muito específicos

Após a seleção dos trabalhos coletados, restaram 11 trabalhos. Assim, para concretizar as etapas 3 e 4, os trabalhos selecionados foram analisados com maior profundidade, tomando como base a literatura abordada no Referencial Teórico, associando-os aos objetivos específicos desta pesquisa. Em seguida, foi construída uma síntese dos resultados encontrados.

Figura 1 - Resumo da metodologia de pesquisa

Fonte: elaborado pelos autores

2. REFERENCIAL TEÓRICO

Esse capítulo apresenta as considerações teóricas acerca de como fundamentar o trabalho. Primeiro é abordado os conceitos da Internet das Coisas. Em seguida, são tratadas a Segurança e Vulnerabilidades no IoT, bem como os tipos de Protocolos utilizados em IoT.

2.1 Internet das Coisas (IoT)

Com a tecnologia cada vez mais avançada a conexão com a internet melhorou, devido o avanço das tecnologias como por exemplo fibra óptica FTTH, diminuindo suas limitações, com relação a largura de banda. Com isso, os objetos também evoluíram, segundo Santaella, Gala, Policarpo e Gazoni (2013), que passaram a ser mais ativos e presentes na vida das pessoas para uma maior independência.

Com o passar do tempo, com evoluções tecnológicas, novos meios de conexões foram sendo criados, deixando de existir a necessidade do uso de fios. As barreiras de espaço e outras limitações passaram a ser cada vez menores, bem como a expansão da mobilidade, usando redes sem fio, como *Wi Fi (Wireless Fidelity), Bluetooth* e o *RFID (Radio-Frequency IDentification),* sensores e chips. Assim, tem-se a seguinte linha do tempo da evolução no IoT:

Quadro 1 - Linha do Tempo da IoT

Ano	Evento
1969	A ARPANET foi a primeira rede a implementar o pacote de protocolos TCP/IP, servindo de base para a Internet
1989	Tim Berners Lee criou a rede mundial de computadores (*World Wide Web*).
1990	John Romkey inventou a Internet Toaster, uma torradeira que se conectava à internet — foi o primeiro dispositivo IoT.
1998	Foi iniciado o Projeto Intouch pelo MIT para desenvolver novas formas de comunicação interpessoal.
1999	Foi criado o Radio Frequency Identification (RFID). É uma forma de comunicação wireless usada para detectar objetos. Hoje, é muito utilizada na Logística 4.0.

2004	A Internet das Coisas começa a aparecer em várias plataformas.
2005	A ONU publicou o primeiro relatório baseado na Internet das Coisas.
2008	IoT é reconhecido pela União Europeia e a primeira conferência IoT Europeia realizada.

Fonte: adaptado do TOTVS (2022)

Atualmente, tem-se a possibilidade de atribuir uma identidade digital (IP – *Internet Protocol*) aos objetos, permitindo que a internet se faça presente em todos os locais, conforme observado por Paes (2014), a Internet das Coisas permite a interação entre humanos e objetos, ou seja, o que diferencia um objeto comum de um objeto inteligente é a capacidade de se conectar com a internet se comunicando com outros dispositivos e o fato de transmitir e enviar dados além de interagir com o ambiente no qual está conectado. Teixeira *et al.* (2014, p. 589) ratificam e ampliam esse conceito:

> "É uma infraestrutura de rede dinâmica e global com capacidades de auto configuração, baseada em protocolos de comunicação padronizados e interoperáveis, onde 'coisas' físicas e virtuais têm identidades, atributos físicos e personalidades virtuais. [...]. Na IoT, as "coisas" ou objetos devem se tornar participantes ativos em processos de negócio, informacionais e sociais, onde serão capazes de interagir e comunicar entre elas mesmas, trocar informações coletadas do ambiente, reagindo autonomamente aos eventos do mundo físico real, bem como influenciar esse contexto sem intervenção direta do ser humano."

Uma rede de dispositivos conectados trocando informações entre si é muito abrangente em aplicações diferentes que atendem pelo nome de Internet das Coisas. Os dispositivos podem enviar e receber dados ou ser apenas um emissor transmitindo informações sem receber nada, podendo ser de minuto a minuto ou com intervalos de tempo. (CARVALHO; SANTOS; GONÇALVES, 2021)

Com vários recursos tecnológicos, fazem com que a integração e a utilização da IOT em vários lugares físicos, composta de dois blocos que são a identificação e serviços, onde que a identificação serve para detectar objetos que serão utilizados para conectá-los a internet destacando o RFID, NFC (*Near Field Communication*) e endereçamento IP. Já os sensores estão com a responsabilidade de coletar informações, armazenar ou encaminhar para a base de dados dos clouds ou de data

centers. Normalmente são utilizadas *WiFi, Bluetooth e RFID* para as técnicas de conexão de objetos com o papel no consumo de energia. O *Wifi* é a tecnologia mais usada onde suas características são de baixa vazão reduzindo o consumo de energia. Também muito utilizadas na IoT, o 3G e o 4G que podem alcançar várias distâncias aproveitando a infraestrutura da telefonia celular (CARVALHO; SANTOS; GONÇALVES, 2021).

O IOT tem como principais características, segundo Wangham, Domenech e Mello (2013):

- A IoT pode ser caracterizada como uma rede mundial de coisas/objetos/dispositivos interconectados que se comportam como entidades ativas;
- As coisas (dispositivos) na IoT, muitas vezes, possuem restrições de recursos como memória RAM ou ROM, poder de processamento e energia;
- Mecanismos de comunicação de alguns dispositivos, na maioria das vezes sem fio, possuem baixa potência de transmissão e baixa taxa de dados;
- Há uma grande quantidade de coisas (dispositivos) com ciclo curto de vida, o que exige uma alta capacidade de gerenciamento;
- Integrar coisas (dispositivos) heterogêneos, o que demanda uma preocupação em relação a interoperabilidade entre estes;
- A rede possui uma topologia dinâmica, pois muitos nós entram e saem da rede com frequência;
- O ambiente de IoT culmina com a geração de enormes quantidades de dados que precisam ser armazenados, processados e apresentados de uma maneira eficiente e fácil de interpretar.

Diante do exposto, observa-se que, quanto maior essa interação, maior é o fluxo de dados e tráfego na rede. Com isso, a vulnerabilidades desses dados, que podem conter informações pessoais, serem monitorados e atacados também aumenta.

2.2 Segurança e Vulnerabilidades no IoT

O Brasil, em 2018, foi o líder em ataques a dispositivos IoT, recebendo 23% dos ataques globais. Nessa mesma época, as *Smart Tvs*, representavam cerca de

70% dos dispositivos de internet das coisas, dentro desse percentual está incluso o “TV Boxes”, a maioria vem com sistema Android desatualizadas, roteadas e vulneráveis a serem infectados (COSSETTI, 2018).

Existem, também, relógios inteligentes, que podem gerar dados sobre a saúde, trajeto, atividades realizadas, históricos do batimento cardíaco entre várias outras funções. (CAPUTO, 2016)

“O que podemos esperar é que quanto mais tivermos aparelhos IoT, mais teremos incidentes criminosos, levando em consideração o aumento de tempos em tempos, No mapa de dispositivos infectados, o Brasil já está em vermelho [junto com a china]”, apontou Thiago Marques, pesquisador de segurança da Kaspersky Lab, na 8ª conferência de analista de segurança para América Latina, que ocorreu em 2018. Se tratando de segurança física, Marques ainda citou, em uma pesquisa que 47% das pessoas que compram fechaduras inteligentes, no intuito de tornar sua residência mais segura, a realidade pode ser diferente, um ataque de *phishing* já bastaria para assumir todo controle dos IoTs (COSSETTI, 2018).

Contudo, uma das principais preocupações em relação à internet das coisas é a vulnerabilidade, uma questão que pode limitar a implementação do IoT (MIORANDI *et al*., 2012). Assim, com a enorme quantidade de objetos consumidos por clientes finais, para sua residência ou uso no dia a dia, os criminosos da internet procuram sempre explorar essas fragilidades, onde a preocupação com a segurança é mínima. A maioria dos dispositivos da Internet das Coisas, não foram projetados levando em consideração a segurança, muitos deles não possuem um sistema operacional ou até mesmo memória suficiente para implementar soluções de segurança (PHILL KEELY, 2017).

De acordo com o DEMARTINI (2023) entre os meses de janeiro e fevereiro de 2023, os ataques a dispositivos da Internet das Coisas já tiveram 41% de aumento, com mais da metade das organizações de todo mundo registrando pelo menos um incidente desse tipo por semana. Para a Checkpoint, esse é um reflexo da transformação digital causada pela pandemia da covid-19 quando se teve um crescimento de trabalho home office ou regimes híbridos, e a maioria dos dispositivos da Internet das Coisas nem sempre protegidos como deveria, e assim abrindo uma porta para a entrada de cibercriminosos. (DEMARTINI,2023)

Com as primeiras vulnerabilidades do computador surgiu a segurança da informação, com isso diversos protocolos foram implementados com a navegação

pela internet por HTTPS, firewall e soluções como antivírus e a implementação da criptografia para informações sensíveis. Nos computadores pessoais de atualmente já vem com dispositivos de segurança que já são instalados dentro do sistema operacional. Já os dispositivos como *Smartphones*, *Smart TVs* e *Smartwatches* nem sempre têm esse cuidado com a segurança, porque ficam conectados a uma rede doméstica (MOURA; D' ALKMIN NEVES, 2021).

Segundo Moura e D' Alkmin Neves (2021), as principais vulnerabilidades encontradas podem ser físicas, lógicas e em dispositivos de IoT, conforme detalham os Quadros 2, 3 e 4 a seguir:

Quadro 2 – Principais vulnerabilidades físicas

Vulnerabilidade Física	**Principais Riscos Associados**
Conexões Físicas	Reprodução automática de conteúdo (exemplo: entrada USB)
Informações Impressas	Presença de dados de conexão e informações de permissões de acesso (exemplo: nome de usuário e senha escritos próximos ao dispositivo)

Fonte: Moura e D' Alkmin Neves (2021)

As vulnerabilidades físicas, conforme demonstrado no quadro 2, as vulnerabilidades físicas podem ocorrer devido a configurações do dispositivo, onde softwares mal-intencionados podem se aproveitar para reproduzir automaticamente conteúdos ao ser conectado um novo dispositivo por uma conexão física, como por exemplo *Universal Serial Bus* (USB) e manter uma anotação com nome e senha do usuário próximo do equipamento, utilizando um malware de quebra de senha por força bruta, Ataque de Man-in-the-Middle (MITM).

Quadro 3 – Principais vulnerabilidades lógicas

Vulnerabilidade Lógica	**Principais riscos associados**
Usuário e senha padrão	Acesso indevido ao dispositivo
Ausência de *Firewall*	Ausência de filtro sobre as transmissões de dados, controle de portas e conexões e de bloqueio de potenciais ataques pela rede

Ausência de Antivírus	Não monitoramento e identificação de arquivos, páginas de rede e executáveis maliciosos ou suspeitos
Firmware desatualizado	Exploração de falhas de segurança existentes por ataques direcionados
Ausência de criptografia	Acesso a informações e dados sensíveis
Criptografia fraca	Ataques de força bruta para quebra da criptografia, ataques *man-in-the-middle*
Portas e serviços habilitados	Ataques *Ransomware,* acesso privilegiado a recursos restritos

Fonte: Moura e D' Alkmin Neves (2021)

As vulnerabilidades lógicas, como mostra no quadro 3, aborda cada tipo de vulnerabilidade com os principais riscos associados a eles.

Quadro 4 – Principais vulnerabilidades em dispositivos IoT

1	Senhas fracas
2	Serviços de redes inseguros
3	Interfaces inseguras
4	Ausência de mecanismos de atualizações seguros
5	Uso de componentes desatualizados
6	Proteção de privacidade insuficientes
7	Transferência e armazenamento de dados inseguros
8	Falta de gerenciamento de dispositivos
9	Configurações padrão inseguras
10	Falta de fortalecimento físico

Fonte: Elaborado por Moura e D' Alkmin Neves (2021) baseado em OWASP (2018)

A fundação *Open Web Application Security Project* (OWASP *Foundation*) elegeu as dez principais vulnerabilidades em dispositivos IoT em 2018, conforme apresentado no quadro 4.

2.3 Tipos de protocolos utilizados em IoT

A confiabilidade do *Internet Protocol* (IP) e sua forma de se adaptar, torna um meio de transmissão para o IOT, o modelo OSI por sua vez, traz um mapa com camadas que enviam e aprovam o recebimento dos dados. Existe vários tipos de

protocolos de IOT, que utilizam distintas camadas da rede IOT, como por exemplo: LoRaWAN, AMQP, CoAP, DDS, MQTT, REST, XMPP, WIFI, BLUETOOTH, NFC,entre outros. (LATERE, 2022).

Dentre esses os mais utilizados são os protocolos MQTT e o REST, por trazer bastante benefícios e pontos positivos como, a confiabilidade e o transporte de pacotes mais leves, o MQTT (*Message Queue Telemetry Transport)* é definido como um protocolo de comunicação IoT *Machine-to-Machine* (M2M), ou máquina a máquina, tem como característica a sua leveza no projeto de transporte de mensagens por meio da publicação e assinatura do tópico, o que é importante, em um sistema de comunicação que possuem problemas com largura de banda e latência alta, para transmissão de dados (DEAL, 2019)

Já o REST (*Representational State Transfer,* que no português é Transferência de Estado Representacional) é uma abstração da arquitetura web, com base de regra e limitações para permitir a criação do projeto com as interfaces de transmissão de dados, ele permite que exista recursos que são utilizados por meio de um identificador global onde existe a manipulação desses recursos através dos componentes da rede, a comunicação via interfaces HTTPS, possibilita que aconteça a troca de informações (DEAL, 2019).

Quadro 5 – Principais vantagens e desvantagens dos protocolos usados em IoT

PROTOCOLO	VANTAGEM	DESVANTAGEM
MQTT	Transporta pacotes leves	Não armazena mensagens no broker
COAP	Protocolo mais leve	Precisa de redes mais estáveis para funcionar bem
WIFI	Consegue lidar com grande quantidade de dados	Alto consumo de energia (para dispositivos iot)
BLUETOOTH	Baixo consumo energético	Curta distância

Fonte: adaptado de Alctel (2023)

3. RESULTADOS

Neste capítulo serão discutidos os resultados encontrados com a análise dos artigos selecionados na busca, com o propósito de atender os objetivos desta pesquisa. Para uma melhor apresentação dos resultados o capítulo foi dividido em três subtítulos: Dispositivos de IoT, Vulnerabilidades nos dispositivos de IoT e Medidas de Segurança.

3.1 Dispositivos de IoT

Após ser realizado pesquisas acadêmicas, notou-se que o crescimento de dispositivos com IOT em residências, é cada vez maior, inclusive tendem a crescer mais que outras tecnologias, mesmo com esta rapidez de expansão no mercado, a internet das coisas, ainda não chegou a seu ápice, quando se trata em automação residencial (SYMANTEC, 2017).

Objetos com a tecnologia IoT vêm auxiliando as pessoas em vários aspectos, como os relógios inteligentes, que fazem o papel de monitorar a saúde das pessoas, quando estão realizando exercícios físicos, ou quando querem saber o status do seu batimento cardíaco ou oxigenação e até mesmo pressão arterial. Nas residências, alguns outros objetos se conectam à rede como, geladeiras, torradeiras e brinquedos (MORAES *et al.*, 2022).

Os sensores em IoT junto com outros dispositivos podem controlar eletrodomésticos de qualquer lugar usando um dispositivo móvel ou a internet. Com isso o sistema pode controlar várias lâmpadas tubulares, ventiladores, eletrodomésticos, motores elétricos, condicionadores de ar e sistemas de aquecimento de ar, entre outras coisas, e é facilmente acessado por dispositivos habilitados para web ou internet (KARUNA *et al*., 2023).

Segundo a NSFOCUS Security Labs, laboratórios da empresa focados na descoberta e análise de ameaças, no Brasil em média temos 1.236 ataques por empresas no meses de Abril e Junho de 2021, representando uma alta de (57%) em relação a 2020, onde os dispositivos que foram mais pontuados pela pesquisa foram as câmeras IP (35%), os roteadores (35%) e os mídia players e assistentes virtuais (20%) sendo a principal fonte por meio de *Malwares* específicos para dispositivos IoT favorecido por senhas fracas sendo por geral os que vem de fábrica. Não ocorrendo

a criptografia correta para oferecer mais segurança ao usuário (CISCO ADVISOR, 2021).

Moraes *et al.* (2022) mencionam o crescente uso da Alexa, que é a interface de voz onde a proprietária é a empresa Amazon. É um serviço que permite comandar outros dispositivos por comando de voz dentro da residência, como, alarmes, interruptores, sensores etc. Coletando informações sobre o cotidiano do usuário, informações essas que alguns casos são pessoais.

Fornecedores como Samsung, Philips já fornecem soluções de hardware, como *smart plugs, smart TVs*, e lâmpadas inteligentes, permitindo que o usuário possa controlar o ambiente com soluções específicas, porém sem uma completa integração entre os dispositivos. Também usando um sistema IoT capaz de receber comandos por voz (STORK, 2019).

Com um smartphone você tem a possibilidade de controlar quase todo ambiente residencial, com um comando de voz, como por exemplo substituir os controles do ar-condicionado, da tv, do *home theater* etc. Quanto mais casas conectadas, mais complicado fica para os consumidores finais abrir mão de tal comodismo, o que nos levou a pensar, é confiável trazer tal tecnologia para um lugar tão importante, como nosso lar?

3.2 Vulnerabilidades nos dispositivos de IoT

Hoje em dia existem várias vulnerabilidades no nosso sistema atual, onde temos uma rede insegura com software e firmware com pouca criptografia e uma estrutura física deficiente, proporcionado o aumento de invasões criminosas de pessoas não autorizadas, coletando dados e violando a privacidade digital (MASOODI; ALAM; SIDDIQUI, 2019).

Uma falha de segurança considerável, de acordo com Candido e Pereira (2019), é a senha padrão que consta nos dispositivos IoT, pois não podem ser facilmente alteradas por seus usuários, o que facilita o ataque de um *hacker*, via DDoS *(Distributed Denial of Service)*, onde pode ser utilizado um pacote de malware, chamado Mirai, estima-se que ele já tenha atingido milhões de dispositivos IoT em todo mundo e por ser difícil seu rastreamento, é muito utilizado pelos H*ackers.*

O Girai, que é um botnet feito especificamente para atacar dispositivos IoT, como por exemplo os roteadores, câmeras CFTV (Circuito Fechado de Televisão), e impressoras que estejam conectadas a internet, ele pode fazer o escaneamento deles automaticamente, buscando por aqueles que não tiveram seus nomes e senhas padrões alterados (CANDIDO; PEREIRA, 2019)

Costa (2018) retrata em seu trabalho um resumo dos maiores riscos, que foram identificados com base nos estudos analisados, para segurança do IoT:

- Falta de atualizações ao software dos dispositivos;
- Autenticação insegura ou inexistente na aplicação web;
- Autenticação insegura ou inexistente em serviços;
- Exposição incorreta à internet;
- Protocolos de comunicação inseguros;

No capítulo do Referencial Teórico, foi mencionado que Moura e D'Alkimin Neves (2021), classificam as vulnerabilidades em físicas, lógicas e em dispositivos de IoT, conforme detalhado nos quadros 2,3 e 4, respectivamente. Já Silva (2018) cita em seus estudos uma lista da OWASP (*Open Web Application Security Project*) de problemas relacionados ao IoT que favorece ao crescimento de acessos de pessoas não autorizadas a fim de pegar informações pessoais para se apoderar de dados, causando um transtorno para os usuários. A seguir tem-se os principais problemas apontados pela autora:

1 - Interfaces Web Inseguras: O primeiro risco mencionado refere-se à falta de certas interfaces da web, tanto para ameaças quanto para usuários internos.Os invasores podem usar credenciais fracas ou criptografadas e enumeração de contas do sistema.

2 - Autenticação e Autorização Insuficientes: A fraqueza no processo de autenticação e autorização pode vir de interfaces web, móveis e de nuvem, presentes em muitas das Internet das Coisas. Senhas fracas, mecanismos fracos de recuperação de senha, credenciais fracamente protegidas e falta de controle de acesso granular são os principais pontos de ataque para esse risco.

3 - Serviços de Rede Inseguros: Os diferentes serviços que compõem a rede

em que os dispositivos IoT estão inseridos podem trazer vulnerabilidades que atacam outros dispositivos conectados à mesma rede, além de ataques de negação do serviço e perda ou corrupção de dados transmitidos.

4 - Falta de Criptografia no Transporte: Assegurar a confidencialidade, a integridade do transporte de dados, a autenticação das pessoas envolvidas e a garantia de não repúdio são os objetivos da criptografia, objetivos fundamentais para um transporte seguro de dados. Porém, muitas vezes, por uma série de motivos, abre mão dos mecanismos de criptografia no tráfego, o que é um erro, pois não tem como se livrar das ameaças internas. Configuração incorreta de uma rede sem fio, por exemplo, tornando o tráfego visível para qualquer pessoa.

5 – Privacidade: Os dados gerados pelos vários dispositivos que compõem os objetos trafegam por uma rede e frequentemente por aplicativos móveis e que são armazenados na nuvem. Existe então uma preocupação relacionada ao fato de os dados passarem por diferentes ambientes que estão fora do controle do usuário.

6 - Interfaces de Nuvem Inseguras: Muitos dados e informações de controle para dispositivos IoT são armazenados externamente na nuvem.

7 - Interfaces Móveis Inseguras: Assim como muitos dispositivos usam a nuvem, muitos também usam recursos móveis e é essencial que o celular seja usado com segurança.

8 - Configurabilidade de Segurança Insuficiente: Ocorre quando os usuários não têm recursos para modificar ou customizar os controles de segurança disponíveis. Os vetores de ataque podem se originar intencionalmente ou acidentalmente de dispositivos e usuários.

9 - Softwares e Firmwares Inseguros: Considerado um risco difícil de explorar, os vetores para software e firmware incluem captura de atualização transmitida em claro ou para invasor fornecer uma atualização própria sequestrando um servidor DNS. A impossibilidade de atualizar um software é um grande problema, em termos de segurança, pois é justamente a partir das atualizações que a segurança é corrigida.

10 - Segurança Física Fraca: por meio do acesso físico aos componentes do dispositivo, o invasor pode acessar a memória e, portanto, o sistema operacional, obtendo uma gama incontrolável de explorações e ataques.

Para Santos (2020), os ataques quando direcionados aos dispositivos são destinados, em sua grande maioria, a serviços de acessos remotos, mais especificamente os que utilizam os protocolos SSH e Telnet, utilizando tentativas em senhas padrões, que por mais que seja feito várias vezes trabalhos de conscientização, é uma das fontes de ataques a esses dispositivos assim como a exploração de “*bugs*” já conhecidas em versões desatualizadas.

Outro ponto de falha são equipamentos residenciais que têm suas interfaces de entrada, inseguras e visíveis na grande rede, exemplo desse caso é a câmera IP, outros dispositivos com falhas recorrentes são as lâmpadas de LED e DVR (COSTA, 2018).

Com relação aos protocolos, os autores Silveira e Gradvohl (2021) afirmam que um dos mais utilizados pela tecnologia, o MQTT, possui vulnerabilidades que podem ser exploradas de diversos modos, o que pode causar danos à integridade e disponibilidade de dados do sistema.

4.3 Medidas de Segurança

Com o mundo interligado e agitado do dia a dia, a forma de uma residência automatizada veio para facilitar aos usuários que já utilizam a internet para ter uma comodidade a mais, transformando sua residência mais segura e de fácil controle, através de uma rede de sensores sem fios e tecnologia biométrica aumentando a segurança com uma rede de nuvem privada, tornando isso cada vez mais comum entre os usuários que utilizam essa tecnologia.

Com o aumento dessa tecnologia surge também a preocupação de proteger os dados 2de pessoas não autorizadas para dificultar ao máximo esses invasores. A forma mais eficiente de reduzir esses ataques cibernéticos a dispositivos é através da prevenção digital, criando barreiras para complicar o acesso. No trabalho de Al-Hamarneh (2021) é descrito requisitos necessários para a segurança de uma cidade inteligente, sendo eles: autenticação, confidencialidade, disponibilidade e proteção de privacidade. O quadro abaixo detalha cada requisito:

Quadro 6 – Principais requisitos para a segurança de Cidades Inteligentes

Requisito	Descrição
Autenticação	Requisito básico para que os usuários possam se identificar e acessar o sistema de IoT com mais eficiência.
Confidencialidade	Outro requisito que serve para evitar que as informações sejam divulgadas de forma incorreta, é proteger as informações e as transferências de dados.
Disponibilidade	Fator para que os dispositivos estivessem disponíveis quando necessário, mantendo um funcionamento eficaz mesmo sob ataque. Como os dispositivos são suscetíveis a ataques, o sistema inteligente deve ser capaz de detectar quaisquer condições anormais e fazer com que seja impedido para não causar danos ao sistema, tendo a capacidade de se recuperar automaticamente das falhas causadas por ataques de grande escala. Por isso que a proteção deve ser robusta e de capacidade de aprender a lidar com ataques cada vez mais inteligentes.
Proteção da Privacidade	Está interligada com as condições citadas acima que podem ter impacto diretamente na proteção da privacidade.

Fonte: adaptado de Al-Hamarneh (2021)

Esses requisitos podem ser aplicados de maneira simples pelas empresas. Para a autenticidade, o sistema pode utilizar a autenticação em duas etapas, com o Captcha (BUGHUNT,2021). Algumas medidas preventivas como a inserção de logins, senhas, tokens, criptografia entre outros, podem garantir e proteger a confidencialidade dos dados do usuário, mantendo os sistemas seguros. De acordo com Bughunt (2021), a Disponibilidade reside na estabilidade dos sistemas e o acesso contínuo aos dados devem ser garantidos por meio de processos rápidos de manutenção, eliminação de erros de software, atualizações contínuas e planos de gerenciamento de emergência. Os sistemas são vulneráveis a desastres naturais, ataques, falta de energia e muitas outras ameaças à disponibilidade. Manter os sistemas seguros também significa garantir o máximo de segurança possível para que os dados estejam sempre disponíveis.

As grandes empresas devem tomar medidas para abordar adequadamente as

vulnerabilidades conhecidas e ter um processo para corrigir bugs de maneira eficiente e segura. Caso contrário, os consumidores perderão a confiança em seu produto, sua marca e até mesmo no próprio dispositivo IoT. É responsabilidade do líder empresarial identificar possíveis pontos fracos em seus negócios. Uma vez que isso seja entendido, os gerentes terão uma compreensão mais clara das ameaças cibernéticas e uma compreensão de como integrar a segurança em todo o processo de design, codificação, teste e avaliação do produto (HSC BRASIL, 2018).

Do mesmo modo que Silva (2018) listou os principais problemas nos dispositivos de IoT na seção anterior, apontou, para cada problema, medidas de mitigação das vulnerabilidades, conforme descreve o quadro 06:

Quadro 7 – Medidas para minimizar problemas com a segurança aos dispositivos com IoT

Vulnerabilidade	Medida de Segurança
1 – Interfaces Web Inseguras	Limitações quanto ao número de tentativas e de logins para acesso dos usuários ao sistema.
2 – Autenticação e Autorização Insuficientes	As sugestões dadas para mitigar os riscos incluem autorização de senha, autorização de acesso granular, credencial revogável, requisito permanente em aplicativos, dispositivos e servidores e gerenciamento seguro das credenciais do usuário.
3 – Serviços de Rede Inseguros	A varredura de porta é necessária usando um scanner de porta para verificar as vulnerabilidades de negação de serviço para UDP, estouro de buffer e ataques fuzzing. Além disso, é recomendável verificar se são realmente necessários e se há algum exposto usando UPnP.
4 – Falta de Criptografia no Transporte	Criação de um mecanismo para garantir que as informações sejam transmitidas apenas de forma clara e que apenas a criptografia com alto nível de confiabilidade seja usada. Além disso, os protocolos SSL e TLS devem estar ativados o tempo todo.

5 – Privacidade	O sistema deve saber quais dados são coletados, se a coleta é realmente e se é permitida. Deve também tentar evitar, tanto quanto possível, a utilização de dados sensíveis, assegurando que os dados permaneçam anônimos e protegidos por encriptação, garantindo que pessoas autorizadas terão acesso aos dados. Por fim, dar liberdade e transparência ao usuário em relação aos dados.
6 - Interfaces de Nuvem Inseguras	Deve verificar se os identificadores e senhas padrão são alterados periodicamente, se o acesso é bloqueado após um determinado número de tentativas, se as credenciais do usuário são protegidas e, finalmente, que o bloqueio de detecção de solicitações incomuns pode ocorrer.
7 - Interfaces Móveis Inseguras	É recomendado senhas e credenciais, valores padrão, aplicar técnicas de ofuscação móvel para evitar ataques de engenharia reversa. Você também deve usar mecanismos anti-adulteração para dispositivos móveis e limitar o uso de aplicativos a apenas sistemas móveis confiáveis.
8 - Configurabilidade de Segurança Insuficiente	É necessário verificar na interface de administração a possibilidade de separar usuários regulares de usuários administrativos, de criptografar dados armazenados e em trânsito, de definir políticas de senhas fortes, de atualizar Disposição de eventos e notificar os usuários sobre os eventos.
9 - Softwares e Firmwares Inseguros	Sugere-se verificar se o pode ser atualizado se necessário, se a atualização é transmitida de forma criptografada pode ter sua autenticidade verificada, com , por exemplo.
10 - Segurança Física Fraca	Para evitar que componentes sejam usados de forma maliciosa, podem ser aplicadas técnicas para dificultar, como componentes autodestrutivos que liberam uma substância que apaga a memória quando o componente é ignorado. Os dados armazenados devem sempre ser criptografados e os externos não podem ser usados para funções diferentes das pretendidas.

Fonte: adaptado de Silva (2018)

Muitos dispositivos IoT não são construídos com a segurança em mente porque seu objetivo principal é adicionar funcionalidade a um custo baixo. Nesse caso, o principal produtor desses aparelhos é o mercado chinês. Além disso, não há protocolo

padrão para comunicações e segurança de dispositivos IoT, o que pode permitir que o malware infecte a rede à qual você está conectado. O maior problema é que não está claro quais são todos os "pontos cegos" na Internet das Coisas. O fabricante deve assumir a responsabilidade de garantir a segurança desses dispositivos, mesmo que ainda não estejam regulamentados. Conexões inseguras, transmissão de dados através da nuvem e os serviços de hospedagem também podem estar sujeitos a ataques externos. Portanto, o vazamento de dados pode ocorrer na conexão entre o próprio dispositivo e o local onde os dados estão armazenados (a nuvem) ou até mesmo cada gateway (HSC BRASIL, 2018).

Ainda, Dietz *et al.* (2018), em seu estudo, sugeriram um método para que evitasse a contaminação por *malwares* na rede, dividindo-se em várias fases a aplicação, no qual consiste que um firewall que estará aplicado no roteador possa realizar uma varredura para identificar dispositivos de IoT vulneráveis. Ao término do escaneamento os dispositivos vulneráveis encontrados pelo firewall serão catalogados no qual montará uma tabela de endereçamento, a partir daí, o firewall age de forma igual ao *malware* escaneando por portas abertas e testando as combinações de credenciais que os *malwares* usam.

Posteriormente, atinge o momento onde todos os endereçamentos dos dispositivos que estão mapeados e aqueles que foram invadidos pelo firewall, colocando-os nas regras de acesso para que não seja possível o acesso externo sem passar pelo firewall. Nos testes, os autores chegaram à conclusão da eficácia de que realizando três teste com três dispositivos alternando os dispositivos na simulação. No total o firewall conseguiu identificar as vulnerabilidades, isolando os dispositivos antes da degradação originada pelo *malware* (DIETZ *et al*., 2018).

Com o grande crescimento dos dispositivos de IoT nas residências, bem como a interatividade cada vez mais abrangente, fica evidente com os resultados pesquisados que para ter um dispositivo seguro de ataques cibernéticos, se faz necessário realizar as atualizações corretas periodicamente, com a finalidade de evitar a vulnerabilidade e tornar os dispositivos mais eficientes e confiáveis para a sua utilização.

5 CONCLUSÃO

Observou-se que os autores das pesquisas analisadas entendem que existe de fato a necessidade de melhoria na vulnerabilidade dos dispositivos IoT, e continuam em busca de melhores soluções, que até o presente momento, ainda não são tão eficazes na minimização das fraquezas dos dispositivos.

Com isso é de extrema importância a busca por correções dessas falhas de segurança, quantificar as mesmas, alertar e proteger o usuário final, vimos que surgiram algumas propostas como, um sistema de automação que mitigassem qualquer tipo de problema relacionado a IoT, recorrente, buscando esses eventos em um base de dados, de diversos órgãos de pesquisas, pesquisadores acadêmicos, empresa de segurança, assim como um monitoramento a esses dispositivos em tempo real para identificar acessos malicioso isolando-os.

Como também a existência de uma lei que regulamentasse, um padrão mínimo de segurança para fabricação dos dispositivos com IoT, para que pudesse garantir uma maior confiabilidade na utilização dos mesmos, e diminuindo as vulnerabilidades existentes, citadas em todo trabalho.

Diante do exposto, entende-se que as empresas fabricantes dos dispositivos que podem ser usadas com IoT, possam fazer com que esses dispositivos estejam preparados para os tipos de ataques que acontecem frequentemente. Observou-se que os dispositivos conectados à Internet estão suscetíveis aos ataques maliciosos, e que não podem prever com antecedência esses ataques, contudo indica-se a prevenção como agente de mitigação dos ataques cibernéticos. Deste modo, a produção de dispositivos com melhores configurações, auxilia aos seus usuários a se protegerem dos invasores.

REFERÊNCIAS

AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M.; AYYASH, M. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications": in **IEEE Communications Surveys & Tutorials,** vol. 17, no. 4, p. 2347-2376, Fourthquarter 2015. Disponível em: Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications | IEEE Journals & Magazine | IEEE Xplore. Acesso em 04 mar. 2023.

AL-HAMARNEH, R. Improve Security in Smart Cities Based on IoT, Solve Cyber Electronic Attacks with Technology by using Packet Tracer. **International Journal of Network Security & Its Applications**. v. 13, n. 6, p. 55-69, 2021. Disponível em: IMPROVE SECURITY IN SMART CITIES BASED ON IOT, SOLVE CYBER ELECTRONIC ATTACKS WITH TECHNOLOGY BY USING PACKET TRACER(aircconline.com) Acesso em: 08 jun. 2023.

ALCTEL. **O que é protocolo IOT e como funciona na prática?** 2023. Disponível em: https://www.alctel.com.br/o-que-e-protocolo-iot-e-como-funciona-na-pratica/ Acesso em 25 jul. 2023.

BIT 2000 TELECOMUNICAÇÕES E INFORMATICA. **Conheça mais sobre Casa inteligente: a IoT no futuro da automação residencial.** 2021. Disponível em: https://www.bit2000.com.br/blog/casa-inteligente-a-iot-no-futuro-da-automacao-residencial. Acesso em: 04 mar. 2023.

BUGHUNT. **Quais são os 4 princípios da segurança da informação?** 2021. Disponível em: https://blog.bughunt.com.br/principios-da-seguranca-da-informacao/#Quais%20S%C3%A3o%20OS%20Princ%C3%ADpios%20Da%20Seguran%C3%A7a%20Da%20Informa%C3%A7%C3%A3o? Acesso em: 22 jul. 2023.

CANDIDO, F. A. S.; PEREIRA, F. C. DDoS em IOT: uma revisão da Literatura. **Projetos e Relatórios de Estágios**, v. 1, n. 1, p. 1-29, 2019.

CAPUTO, V. **Google indica apps para cuidar da saúde usando um *smartwatch***. 2016. Disponível em: https://exame.com/tecnologia/google-indica-apps-para-cuidar-da-saude-usando-um-smartwatch/ . Acesso em: 02 abr. 2023.

CARVALHO, A. F. A.; SANTOS, C. M. L.; GONÇALVES, L. V. Segurança em IoT. Orientador: Hélder Line Oliveira. 2021. 18f. **Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação)** - Centro Universitário do Planalto Central Apparecido dos Santos, 2021.

CIRANI, S.; FERRARI, G.; PICONE, M.; VELTRI, L. **Internet of Things: Architectures, Protocols and Standards**. John Wiley & Sons, Ltd, 2018.

CISCO ADVISOR. **Brasil é o 8º do mundo em ataques a dispositivos IoT**. 2021. Disponível em: https://www.cisoadvisor.com.br/brasil-e-o-8o-do-mundo-em-ataques-a-dispositivos-iot/#:~:text=Entre%20os%20dispositivos%20mais%20atacados%20est%C3%A3o%20as%20c%C3%A2meras,%E2%80%93%20em%20geral%20as%20que%20v%C3%

AAm%20de%20f%C3%A1brica. Acesso em 07 jun. 2023.

COSSETTI, M. C**. Brasil é líder em ataques a dispositivos IoT com 30 mil infectados em 2018.** 2018. Disponível em: https://tecnoblog.net/especiais/brasil-e-lider-em-ataques-a-dispositivos-iot-com-30-mil-infectados-em-2018/ . Acesso em: 02 abr. 2023.

COSTA, L. C. G. **Vulnerabilidades em Dispositivos IoT para Ambiente Smart Home.** 2018. 151 f. Dissertação (Mestrado) – Mestrado em Engenharia de Segurança Informática. Instituto Politecnico de Beja, Portugal. 2018. Disponível em:https://repositorio.ipbeja.pt/bitstream/20.500.12207/4827/1/Dissertacao_Luis_Costa_ PDFA.pdf

CRYPTO ID. **IoT: saiba como a Internet das Coisas já está presente no dia a dia.** 2023. Disponível em: https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/iot-saiba-como-a-internet-das-coisas-ja-esta-presente-no-dia-a-dia/ Acesso em: 10 jun. 2023.

DEAL TECHNOLOGIES. **O MQTT E O REST São Os Protocolos Mais Utilizados No Mundo Do IoT E Possuem Diversos Benefícios E Pontos Positivos**. 2019. Disponível em: https://www.deal.com.br/blog/iot-mqtt-e-rest-os-protocolos-utilizados-no-mundo-iot/. Acesso em: 30 abr. 2023.

DEMARTINI, F. **Ataques a dispositivos de Internet das Coisas crescem 41% em 2023**. 2023. Disponível em: https://canaltech.com.br/seguranca/ataques-a-dispositivos-de-internet-das-coisas-crescem-41-em-2023-247348/. Acesso em: 01 maio 2023.

DIETZ, C. *et al*., "IoT-Botnet Detection and Isolation by Access Routers," 2018. **9th International Conference on the Network of the Future (NOF)**, Poznan, Poland, 2018, p. 88-95. Disponível em: https://ieeexplore.ieee.org/document/8598138/authors#authors

FISHER, Sharon. **Riscos de segurança da Internet das Coisas**. 2019. Disponível em: https://www.avast.com/pt-br/c-iot-security-risks. Acesso em: 03 mar. 2023.

GIL, A. C. **Como elaborar Projetos de Pesquisa**. 6ª ed. São Paulo: Atlas, 2017.

GREENE. T. **Study: Most enterprise IoT transactions are unencrypted.** 2019. Disponível em: https://www.networkworld.com/article/3396647/study-most-enterprise-iot-transactions-are-unencrypted.html. Acesso em 28 fev. 2023.

HSC BRASIL. Segurança para IoT: quais os desafios e seus impactos em segurança. 2018. Disponível em: https://www.hscbrasil.com.br/seguranca-em-iot/ . Acesso em 22 jul. 2023.

KARUNA, G.; KUMAR, R.; KAPSE, R.; REVULAGADDA, S. **Home Automation Based on IoT. E3S Web of Conferences. 391**. 2023. DOI: 10.1051/e3sconf/202339101159.

LATERE**. Protocolos de Rede sem fio de IoT.** 2022. Disponível em: https://embarcados.com.br/protocolos-de-rede-sem-fio-de-iot/#Tipos-de-protocolos-IoT. Acesso em: 30 abr. 2023.

MANCINI, M. **Internet das Coisas: história, conceitos, aplicações e desafios**. Ed. Tudo sobre Iot, 2019, 24 p. Disponível em: http://monicamancini.com.br/wp-content/uploads/2019/07/Monica_Mancini-Ebook_Iot.pdf.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 8ª ed. São Paulo: Atlas, 2017.

MASOODI, F.; ALAM, S.; SIDDIQUI, S. T. Security & Privacy Threats, Attacks and Countermeasures in Internet of Things. **International Journal of Network Security & Its Applications**. v. 11, n. 1, p. 67-77, 2019. Disponível em: https://www.researchgate.net/publication/341096378_SECURITY_PRIVACY_THREATS_ATTACKS_AND_COUNTERMEASURES_IN_INTERNET_OF_THINGS Acesso em 07 jun. 2023.

MIORANDI, D. *et al*. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, v. 10, n. 7, p. 1497-1516, 2012.

MORAES, J. M.; QUIRINO, C.; ALMEIDA, R. M.; D' ALKMIN NEVES, J. E. Internet das Coisas (IoT) - casa inteligente, definições e aplicações. **RBTI - Revista Brasileira em Tecnologia da Informação**, v. 4, n. 2, p. 1-48, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/52. Acesso em: 09 jun. 2023.

MOURA, T. M.; D' ALKMIN NEVES, J. E. Análise de Segurança em Dispositivos Internet das Coisas. **Revista Interface Tecnológica**, v. 18, n. 2, p. 15–27, 2021. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1174. Acesso em: 6 abr. 2023.

NOBRE, J.; LOPES, R.; GOMES, M.; DE OLIVEIRA, N. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados. **Revista Eletrônica de Iniciação Científica em Computação**, *[S. l.]*, v. 17, n. 4, 2019. Disponível em: https://sol.sbc.org.br/journals/index.php/reic/article/view/1704. Acesso em: 6 mar. 2023.

OWASP. OWASP top10 Internet of things. 2018. Disponível em: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project. Acesso em: 6 abr. 2023.

PONTOTEL**. IoT: entenda o que é a Internet das Coisas, como funciona e a sua importância!** 2022. Disponível em: https://www.pontotel.com.br/iot/#1. Acesso em: 02 mar. 2023.

PAES, W. M. Interoperabilidade móvel: a Internet das Coisas. **Revista da Universidade Vale do Rio Verde**, v. 12, n. 1, p. 794-810, 2014.

SANTAELLA, L.; GALA, A.; POLICARPO, C.; GAZONI, R. Desvelando a Internet das Coisas. **Revista GEMInIS**, v. 1, n. 2, p. 19-32, 2013.

SANTOS, M. M. **IoT Tunnel – Uma proposta para mitigar vulnerabilidades na comunicação de elementos IoT.** 2020. 103 f. Dissertação (Mestrado) – Programa de Pós-Graduação em computação. Universidade Federal do Rio Grande, Rio Grande. 2020. Disponível em: https://sistemas.furg.br/sistemas/sab/arquivos/bdtd/1ebf7a7f15caf8aeef56ebc1959d4d64.pdf

SILVA, C. D. O. O Desafio da Segurança das Informações Digitais na Internet das Coisas**. Revista Científica Multidisciplinar Núcleo do Conhecimento**. Ano 03, Ed. 05, v. 04, p. 137-157, 2018. Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/internet-das-coisas,

SILVEIRA, M.; GRADVOHL, A. Security analysis of the message queuing telemetry transport protocol. **Revista Brasileira de Computação Aplicada**. v. 13, n. 2, p. 83-95, 2021. Disponível em: https://www.researchgate.net/publication/353527336_Security_analysis_of_the_message_queuing_telemetry_transport_protocol

STORK, E. **Smart Voice Control:** um sistema IoT para Casas Inteligentes controlado por voz. 2019. 76 f. TCC (Graduação) - Curso de Engenharia da Computação, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2019. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/11589

SYMANTEC. **Security Center Archived Publications**. Disponível em:https://www.broadcom.com/support/security-center/publications/archive#accordion- threat-reports . Acesso em: 09 jun. 2023.

TEIXEIRA, F. A. et al. Siot: defendendo a internet das coisas contra *exploits*. *In:* Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 32, 2014, Florianópolis. **Anais [...]**, Florianópolis, 2014, p. 589-602. Disponível em: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/Defendendo%20a%20Internet%20das%20Coisas%20contra%20Exploits.pdf

TERRA. Até 2025, mundo terá cerca de 27 bilhões de dispositivos IoT conectados. 2022. **Site do Terra**, 24 nov. 2022. Disponível em: https://www.terra.com.br/noticias/ate-2025-mundo-tera-cerca-de-27-bilhoes-de-dispositivos-iotconectados,ba609033b546442d18d06660dbc7bb2d709p6o4w.html

TOTVS. **Internet das Coisas: o que é, exemplos e impactos.** 2022. Disponível em: https://www.totvs.com/blog/inovacoes/aplicacoes-da-internet-das-coisas/. Acesso em: 16 abr. 2023.

WANZELER, T.; FÜLBER, H.; MERLIN, B. Desenvolvimento de um sistema de automação residencial de baixo custo aliado ao conceito de Internet das Coisas (IoT). In: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 34, 2016, Santarém. Anais eletrônicos [...]. Santarém: SBTR, 2016. Disponível em: https://biblioteca.sbrt.org.br/articles/129.