INSTITUTO FEDERAL
SANTA CATARINA

CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TI

RODRIGO GRANDO BERLANDA

Guia de segurança da informação para a conectividade de dispositivos IoT

Florianópolis - SC
2021

Ficha de identificação da obra elaborada pelo autor.

Berlanda, Rodrigo
Guia de segurança da informação para a conectividade de dispositivos IoT / Rodrigo Berlanda; orientação de Hamilcar Boing. - Florianópolis, SC, 2021.
93 p.

Trabalho de Conclusão de Curso (TCC) - Instituto Federal de Santa Catarina, Câmpus Florianópolis. CST em Gestão da Tecnologia da Informação. Departamento Acadêmico de Saúde e Serviços.
Inclui Referências.

1. Internet of Things. 2. Segurança da Informação. 3. Indústria 4.0. 4. Dispositivos IoT. I. Boing, Hamilcar. II. Instituto Federal de Santa Catarina. III. Guia de segurança da informação para a conectividade de dispositivos IoT.

INSTITUTO FEDERAL DE SANTA CATARINA
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

RODRIGO GRANDO BERLANDA

GUIA DE SEGURANÇA DA INFORMAÇÃO PARA A CONECTIVIDADE DE DISPOSITIVOS IOT

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Professor Orientador:
Prof. Hamilcar Boing

FLORIANÓPOLIS - SC
AGOSTO/2021

GUIA DE SEGURANÇA DA INFORMAÇÃO PARA A CONECTIVIDADE DE DISPOSITIVOS IOT

RODRIGO GRANDO BERLANDA

Este trabalho foi julgado adequado para obtenção do Título de Tecnólogo em Gestão da Tecnologia da Informação e aprovado na sua forma final pela banca examinadora do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis-SC, 10 de agosto de 2021.

Documento assinado digitalmente
FELIPE CANTORIO SOARES
Data: 09/09/2021 18:27:45-0300
CPF: 398.713.399-68

Prof. Felipe Cantório Soares, M.Eng.
Coordenador do CST em Gestão da Tecnologia da Informação
Instituto Federal de Santa Catarina

Banca Examinadora:

Documento assinado digitalmente
HAMILCAR BOING
Data: 10/09/2021 14:32:45-0300
CPF: 743.217.229-34

Prof. Hamilcar Boing, Dr.
Orientador

Documento assinado digitalmente
ADRIANO HEIS
Data: 10/09/2021 14:50:58-0300
CPF: 955.690.149-34

Prof. Adriano Heis, M.Sc.

Documento assinado digitalmente
EGON SEWALD JUNIOR
Data: 10/09/2021 14:21:32-0300
CPF: 007.730.849-24

Prof. Egon Sewald Junior, Dr.

RESUMO

O avanço da Indústria 4.0 e a utilização de dispositivos *Internet Of Things* (IoT) em diversos pontos dentro das organizações trouxe diversos benefícios como otimizar as tarefas do dia a dia e melhorar a eficiência dos processos. Porém, a aplicação em larga escala destes dispositivos sem as devidas camadas de segurança pode trazer riscos e causar prejuízos inestimáveis, uma vez que estes dispositivos, em grande parte, são desenvolvidos com pouca capacidade computacional, não possibilitando a aplicação de técnicas de segurança mais complexas. Além disso, como qualquer outro dispositivo conectado a uma rede, também estão vulneráveis aos riscos dos demais *softwares* e *peopleware* da organização, que podem ser utilizadas por invasores para acessar/modificar dados confidenciais ou até mesmo, controlar/parar serviços importantes das organizações. Com o intuito de compreender o impacto que os ataques podem causar à uma rede corporativa, a presente pesquisa realiza simulações de redes/dispositivos IoT sofrendo invasões e ataques utilizando o software Contiki, onde observou-se que os ataques podem afetar de forma significativa seus alvos ao utilizarem os IoTs para este fim. Portanto, esta pesquisa poderá auxiliar gestores e empresas na utilização/adoção dos dispositivos IoT na Indústria 4.0 de forma mais segura, uma vez que tem como objetivo apresentar um guia, em formato de documento, de recomendações de segurança da informação para dispositivos IoT e para isso, realiza uma classificação dos principais tipos de vulnerabilidades e ataques realizados contra dispositivos IoT, levando em conta seu *hardware*, *software* e *peopleware*. Além disso, também identifica diretrizes, políticas e boas práticas para mitigar os riscos de segurança da informação.

Palavras-chave: Indústria 4.0. Dispositivos IoT. Segurança da Informação.

ABSTRACT

The advancement of Industry 4.0 and the use of Internet Of Things (IoT) devices at various points within organizations has brought several benefits such as optimizing day-to-day tasks and improving processes efficiency. However, the large-scale application of these devices without the proper security layers can bring risks and cause valuable losses, since these devices, in large part, are developed with low computational capacity, not allowing the application of more complex security techniques. In addition, like any other device connected to a network, they are also vulnerable to the risks of other software and peopleware in the organization, which can be used by intruders to access/modify confidential data or even control/stop important services of the organizations. In order to understand the impact that attacks can have on a corporate network, the present study performs simulations of IoT network/devices suffering invasions and attacks using Contiki software, where it was observed that attacks can significantly affect their targets when using IoTs for this purpose. Therefore, this research can help managers and companies in the usage/adoption of IoT devices in Industry 4.0 in a safer way, since it aims to present a guide of information security recommendations for IoT devices and, for this, performs a classification of the main types of vulnerabilities and attacks against IoT devices, considering their hardware, software and peopleware. In addition, it also identifies guidelines, policies and best practices to mitigate information security risks.

Key-words: Industry 4.0. IoT Devices. Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

CERT.br *Computer Emergency Response Team Brazil* (Equipe de Resposta Emergencial em Computação (tradução nossa), chamada no Brasil de Comitê Gestor da Internet no Brasil)

CROND Cyber Range Organization and Design (Cyber Range Organização e Design) (Tradução nossa)

DDoS Distributed Denial of Service ((Ataque) Distribuído de Negação de Serviço)

DoS Denial of Service ((Ataque de) Negação de Serviço)

HIDS Host Based Intrusion Detection System (Sistemas de Detecção de Intrusão baseado em Host)

IDS Intrusion Detection System (Sistemas de Detecção de Intrusão)

IFSC Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina

IIoT Industrial Internet of Things (Internet das Coisas Industrial)

IOT Internet of Things (Internet das Coisas)

IoTrain-Sim IoT Training System Using the Cooja Network Simulator (Sistema de Treinamento IoT Utilizando o Simulador de Redes Cooja) (Tradução nossa)

ISO International Organization for Standardization (Organização Internacional para Padronização)

LAN Local Area Network (Rede de área local)

LGPD Lei Geral de Proteção de Dados Pessoais

LoRaWan Long Range Wide Area Network (Rede de área ampla de longo alcance)

NIDS Network Intrusion Detection System (Sistemas de Detecção de Intrusão em Redes de Computadores)

PSI Políticas de Segurança da Informação

RTOS Real Time Operating System (Sistema Operacional em Tempo Real)

SI Segurança da Informação

SO Operating System (Sistema Operacional)

TCP/IP Transmission Control Protocol / Internet Protocol (Protocolo de Controle de Transmissão / Protocolo de Internet)

TI Tecnologia da Informação

UFSC Universidade Federal de Santa Catarina

WAN Wide Area Network (Rede de área ampla)

SUMÁRIO

1. INTRODUÇÃO

Atualmente, não são apenas computadores e smartphones que estão conectados à internet, mas qualquer outro dispositivo que se tem em casa. Desde um eletrodoméstico, com programação e controle à distância por aplicativo até mesmo carros com sensores e inteligência artificial provendo dados ao motorista enquanto dirige. Estes dispositivos inteligentes facilitam o dia a dia das pessoas e trazem possibilidades para diversos setores, inclusive para a indústria.

Esse cenário descrito anteriormente é conhecido como Indústria 4.0 ou Manufatura Avançada, que faz parte da sociedade da informação, como o novo estágio de desenvolvimento da produção industrial no mundo. Na Indústria 4.0, muitos dados são gerados ao longo das diversas etapas dos processos de produção, que são armazenados e, quando possível, analisados para a identificação de possíveis melhorias nos métodos e procedimentos do próprio processo de produção.

O principal diferencial da indústria 4.0 é a conectividade em qualquer uma das etapas e a possibilidade de adequar essa conectividade para diversos dispositivos. Dessa forma, temos dispositivos inteligentes que são chamados de dispositivos da Internet das Coisas (em inglês, *Internet of The Things* (IoT)). Segundo Davis (2008, apud ISOTANI *et al.*, 2008), a internet é dividida em quatro estágios de evolução:

1. Web 1.0: focada na conexão e aquisição de informações na rede;
2. Web 2.0 ou Web Social: focada na preocupação com a experiência de usuário e redes sociais;
3. Web 3.0 ou Web Semântica: focada na atribuição de significado e contexto às informações;
4. Web Ubíqua (atual): integrada à Internet das Coisas, constituída pela conectividade e interatividade entre pessoas, informações, processos e objetos, por qualquer pessoa, de qualquer lugar e a qualquer tempo (apud LACERDA; LIMA-MARQUES, 2015).

Considerando a definição de Davis, neste cenário em que diversos pontos da

cadeia produtiva da indústria podem ser equipamentos inteligentes e que captam informações em tempo real, é de extrema importância avaliar o armazenamento da grande quantidade de informações que são geradas para análise posterior, pois com elas é possível identificar lacunas na cadeia produtiva e levantar informações vitais para a melhoria contínua do processo. Essas informações geradas em grande volume, variedade e em alta velocidade são chamadas de *Big Data* e pode ser um aliado muito importante importante para a indústria, pois o processamento destas informações podem permitir uma melhor percepção, tomada de decisão e automação de processos (GARTNER, 2019).

O armazenamento desse grande volume de dados pode ser efetuado em data centers da organização ou na Computação em Nuvem (*Cloud Computing*), no qual os dados são armazenados de forma descentralizada, podendo ser acessados de qualquer local, facilitando assim o seu manuseio.

A nova realidade na indústria 4.0 junto com a IoT trouxe desafios consigo. Por ser uma nova tecnologia em fase de expansão e com o aumento considerável de dispositivos inteligentes e conectados, a segurança da rede tende a diminuir, já que o número de possíveis alvos aumenta. Em uma pesquisa apresentada por Constantin (2019), foi descoberto 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, pois os dispositivos IoT ficam em grande parte localizados nas extremidades da rede, e fisicamente em locais de fácil acesso para qualquer pessoa mal intencionada. Por isso, é necessário pensar muito bem nas medidas de segurança destes dispositivos, uma vez que muitos dispositivos IoT são desenvolvidos com pouca capacidade de processamento, já que são criados pensando no baixo consumo energético, o que pode dificultar a aplicação de técnicas de segurança.

Para que a segurança destes dispositivos seja feita, é necessário que as empresas façam uma análise, avaliando os requisitos de segurança, isto é, identificar e classificar os pontos de risco presentes nos equipamentos IoT. Os resultados dessa análise irão auxiliar na apuração dos pontos que demandam mais atenção, e ajudar na

implementação das soluções escolhidas.

Um dos métodos que pode ser utilizado é a auditoria de segurança de TI, que consiste no processo que verifica se padrões de segurança são cumpridos. É um processo que deve ser refeito periodicamente, pois qualquer mudança no cenário pode influenciar nos resultados, e consequentemente, na segurança da rede. Sempre pensando em respeitar e manter os três pilares da segurança da informação, a confidencialidade, integridade e disponibilidade.

No Brasil, estes cuidados com a segurança dos dados terão ainda mais importância com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2020. Com esta lei, todas as empresas que fazem tratamento de dados pessoais deverão tomar uma série de medidas para garantir o cumprimento da nova legislação, para que a privacidade, transparência, desenvolvimento, padronização, proteção do mercado e a concorrência sejam asseguradas.

Nesse cenário, a presente pesquisa propõe analisar os dispositivos Internet das Coisas, tendo em vista seu hardware, software e o peopleware em seu entorno, na perspectiva da segurança da informação, para que haja o desenvolvimento de um guia de segurança da informação para IoT.

1.1. JUSTIFICATIVA

O novo cenário apresentado pela Indústria 4.0 junto com a Internet das Coisas vem acompanhado de desafios que podem ser potencialmente perigosos para as empresas. Por isso, é importante que a segurança da informação seja levada em consideração na hora de utilizar estas tecnologias.

Em uma pesquisa feita pela empresa Gemalto (2018), empresa internacional de segurança digital, descobriu-se que 94% dos tomadores de decisão das empresas entrevistadas viam desafios em implementar a segurança na IoT. Ainda na mesma pesquisa, o autor trata que para algumas empresas, o desafio de evitar as armadilhas de segurança da IoT pode parecer assustador. Os desafios impostos pela IoT se devem, no

geral, à complexidade e a falta de práticas comuns estabelecidas pela indústria.

Ainda, a pesquisa aponta que 48% das empresas de TI não conseguem detectar violações em seus dispositivos IoT. Além dos gastos com segurança em IoT terem aumentado. Em 2017, 11% do orçamento do setor de TI era reservado para segurança, e em 2018, este número subiu para 13%.

Outro fato alarmante é que em 2017, de acordo com Menezes (2017), mais de 160 países possuíam dispositivos controlados pela botnet Mirai[1], que contaminava câmeras de segurança IP, gravadores digitais de vídeo, roteadores e outros dispositivos IoT. O tráfego gerado pela netbot Mirai chegou a 1,2 terabit por segundo (Tbps) em 2016, até então o maior volume registrado. Sendo que o Brasil está entre um dos países que sofrem mais ataques desta *botnet*.

Neste cenário, foi regulamentada no Brasil, em 2018, a Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), que visa estabelecer normas rígidas para a proteção de dados pessoais, portanto, empresas que fazem tratamento destes dados deverão tomar medidas a fim de garantir o cumprimeiro desta nova legislação (MACHADO MEYER SENDACZ OPICE ADVOGADOS, 2018).

Portanto, pensando na Indústria 4.0, Segurança da Informação e LGPD, temos um cenário onde os dispositivos IoT podem trazer diversas vantagens para as empresas e indústrias, porém, podem apresentar diversos riscos, e cuidar de sua segurança é essencial para o funcionamento e preservação das organizações.

Em relação a presente pesquisa, ele está em consonância com os objetivos do curso de Gestão da Tecnologia da Informação pois, uma vez que o profissional esteja formado e atuando na área de Segurança da Informação, deverá analisar, avaliar e gerenciar cenários e situações potencialmente perigosas para a segurança da informação, bem como buscar soluções eficazes para eles.

Sendo assim, ao consultarmos o Projeto Pedagógico do Curso (PPC) Superior de Tecnologia em Gestão da Tecnologia da Informação (CST GTI) do IFSC (2014), são apresentadas algumas competências esperadas do profissional de TI e que estão alinhadas com o tema:

[1] Os botnets se baseiam no conceito de diversos dispositivos infectados, conectados à internet, que permitem com que o hacker possa realizar ataques DDoS. O botnet Mirai tem como foco invadir dispositivos IoT para este fim.

- Desenvolver visão e raciocínio estratégico para a definição e implementação dos princípios de gestão das tecnologias da informação;
- Desenvolver competências para a tomada de decisões estratégicas sobre a adoção de tecnologias da informação de modo alinhado às necessidades do negócio;
- Disseminar conhecimentos tecnológicos e gerenciais que possibilitem ao aluno conduzir projetos, programas e atividades de aplicação das tecnologias da informação com qualidade e segurança.

1.2. PROBLEMA

No cenário da Indústria 4.0 onde a conectividade e a integrabilidade são de suma importância, surge um novo cenário, composto pela IoT (ASSAD NETO et al., 2017). Neste contexto, objetos antes simples, se tornam inteligentes e conectados, gerando dados em massa, valiosos para as organizações.

Para as empresas e indústrias, isto quer dizer sensores integrados, câmeras e demais dispositivos entregando informações em tempo real, o tempo todo. Isto pode trazer inúmeras vantagens para a organização, pois a análise desses dados podem revelar informações que podem ser de suma importância para que haja uma melhora em seus produtos ou processos.

Entretanto, este cenário também traz riscos. Um dos problemas destes dispositivos é que eles são geralmente fabricados de forma simples, sem muito poder de processamento ou armazenamento, o que torna a utilização de técnicas de segurança da informação mais difíceis de serem aplicadas.

Outro risco vem em decorrência de uma das vantagem dos IoTs, a sua grande gama de tipos de dispositivos e a diversidade de ambientes em que são inseridos, pois existem dispositivos IoTs que são dispostos em locais de fácil acesso, como corredores de uma empresa (como câmeras) e outros perto ou dentro da linha de produção, em maquinários ou tanques (como sensores). No primeiro caso, o dispositivo pode ficar

facilmente ao alcance de indivíduos mal intencionados, enquanto que no segundo podem ficar em locais de difícil acesso, o que torna mais complicado realizar tarefas como atualizar, configurar e checar estes dispositivos. Portanto a utilização de dispositivos IoT deve ser pensada a fim de trazer as vantagens deste tipo de tecnologia sem deixar de cuidar dos riscos que a acompanham.

Sendo assim, neste cenário conflituoso em que as indústrias anseiam a automação em larga escala integrada aos dispositivos IoT, que possuem requisitos mínimos de *hardware* e que consequentemente, impactam no desempenho e na utilização de ferramentas que visem a segurança dos mesmos, esta pesquisa visa responder a seguinte pergunta de pesquisa: como avaliar a conectividade, boas práticas e políticas que devem ser seguidas para minimizar os riscos de segurança da informação e seus efeitos nos dispositivos IoT adotados na indústria 4.0?

1.3. OBJETIVOS

1.3.1. OBJETIVO GERAL

Desenvolver um guia de segurança da informação para dispositivos IoT utilizados na Indústria 4.0.

1.3.2. OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são:

1. Investigar o funcionamento e requisitos dos dispositivos IoT adotados na Indústria 4.0, levando em conta seu *hardware*, *software* e *peopleware*;
2. Analisar e classificar os principais tipos de falhas e riscos em segurança da informação correlacionados com dispositivos IoT.
3. Realizar experimentos para avaliar o impacto dos ataques nos dispositivos IoT;
4. Identificar diretrizes, políticas e boas práticas para mitigar os riscos de segurança da informação introduzidos pelos dispositivos IoT;
5. Documentar as recomendações sobre boas práticas e procedimentos de segurança da informação para a adoção de dispositivos IoT na indústria 4.0.

2. REFERENCIAL TEÓRICO

Nesta seção será apresentado o referencial teórico utilizado nesta pesquisa. A apresentação do referencial será dividida em cinco tópicos principais: Indústria 4.0, *Internet of Things* (IoT), Infraestrutura da Indústria 4.0 no Brasil, Cloud Computing, Segurança da Informação.

2.1 INDÚSTRIA 4.0

A indústria que conhecemos atualmente com robôs, maquinários e até produtos interagindo uns com os outros não surgiu de repente, foram necessárias muitas evoluções, inovações e consequentemente revoluções até chegarmos no estado atual.

A primeira revolução industrial teve origem na Inglaterra, entre os séculos 18 e 19. Nesta época, os meios de fabricação mudaram, passando de métodos artesanais para máquinas movidas a vapor. Ainda no século 19 e se estendendo até o século 20 ocorreu a segunda revolução industrial, onde aconteceram evoluções em diversas áreas, e a mais impactante, a criação e utilização de máquinas industriais movidas a energia elétrica (FEIMEC, 2020).

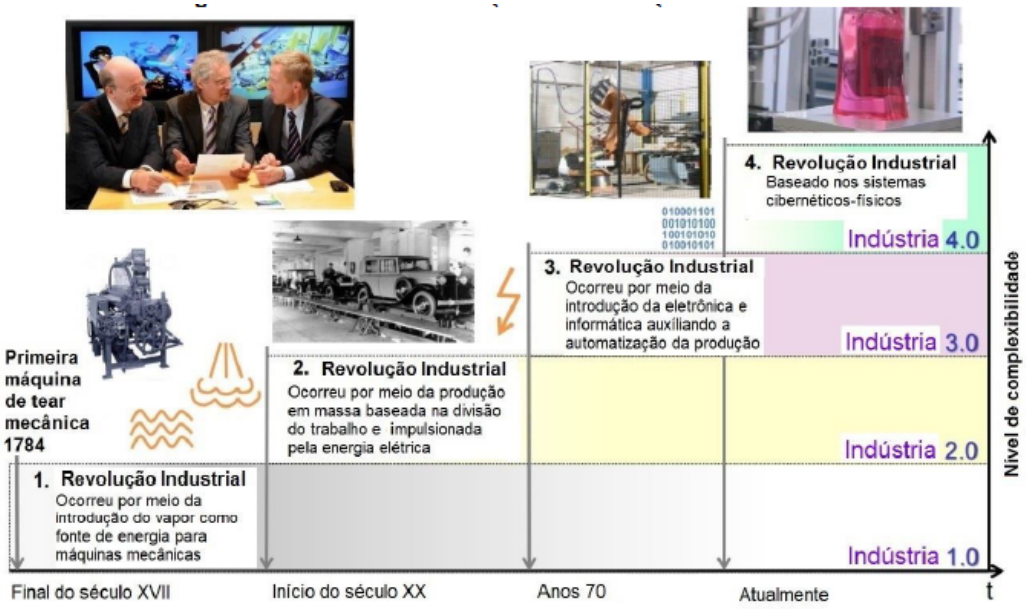
Na década de 70 a terceira revolução industrial teve início, onde se disseminou o uso de computadores, automação e robotização da linha de produção. Nessa época,o processamento e armazenamento das informações eram em meio digital, otimizando assim os meios de comunicação (FEIMEC, 2020).

> Em 2010 foi lançado na Alemanha o plano de desenvolvimento tecnológico High-Tech Strategy 2020, visando à fortificação da parceria entre indústria e ciência e a melhoria das condições para inovação tecnológica no país. Dentro do plano de ação dessa iniciativa, em março de 2012, a Indústria 4.0 foi adotada pelo governo federal como um projeto futuro. O objetivo estratégico é explorar o alto potencial econômico e de inovação resultante do impacto das tecnologias de informação e comunicação na indústria. (GTAI, 2014 apud ASSAD NETO et al., 2017, p. 2)

A quarta revolução industrial é segundo Rüßmann et al. (2015), conforme citado por Silva (2017) baseada em nove pilares que gerarão oportunidades de desenvolvimento tecnológico, sendo eles:

1. Big data;
2. Computação em nuvem;
3. Integração de sistemas vertical e horizontal;
4. Inteligência artificial;
5. Internet industrial das coisas;
6. Realidade virtual;
7. Robôs autônomos;
8. Segurança cibernética;
9. Simulação e impressão 3D.

Gráfico 1 - Revoluções industriais



Fonte: Silva, 2017, p. 11

No gráfico 1 pode-se observar uma linha do tempo mostrando a evolução da indústria e de seu nível de complexidade com o decorrer das revoluções. Por este assunto tratar de diversas dimensões e tópicos que por si só são amplos, esta pesquisa irá abordar as tecnologias computação em nuvem e a Internet das Coisas (IoT).

2.2 *INTERNET OF THINGS* (IoT)

O termo Internet das Coisas (*Internet of Things*) ainda não possui uma definição clara e padronizada e ainda está sujeita a debates (RAIWANI, 2013). Por isso, é possível encontrar diversas definições de Internet das Coisas. Uma definição apresentada por Evans (2011) diz que a IoT é o momento exato no qual o número de coisas ou objetos conectados à internet passa o número de pessoas conectadas. Outra definição é a de Gartner (2017) que define a IoT como a rede de objetos físicos que têm tecnologia embutida para que possam se comunicar, sentir e interagir com o ambiente externo ou interno.

Uma terceira definição da Internet das Coisas é dada por Lacerda e Lima-Marques (2015) onde para eles ela é um acontecimento complexo, podendo ser analisada de diversos pontos de vista, como social, cultural, econômico, organizacional, tecnológico, informacional, entre outros. E seu efeito é a criação de ambientes permeados com informação.

Ao falarmos de dispositivos IoT devemos levar em conta a sua divisão entre IoT doméstico e IoT industrial (também chamado de IIoT, de Industrial). Os dispositivos domésticos podem ser desde câmeras e lâmpadas inteligentes até fogões, geladeiras e TVs. Enquanto que os dispositivos industriais têm uma natureza voltada a automatização e coleta de dados em torno da cadeia produtiva da indústria, como por exemplo sensores que captam pressão, temperatura e umidade ou dispositivos elétricos inteligentes que distribuem energia de forma eficiente.

2.2.1 ESTRUTURA DOS DISPOSITIVOS IOT

A estrutura dos dispositivos IoT busca a simplicidade e a otimização de recursos como energia, processamento e espaço físico (RIBEIRO, 2018). Para melhor compreensão das partes que compõem a arquitetura destes dispositivos podemos dividir em três grandes tópicos que abrangem todo o entorno destes dispositivo: *Hardware*, que cuida de toda a estrutura física, sendo responsável pelo processamento, aquisição e armazenamento das informações; *Software*, que é o elemento que possui toda a lógica

que controla o hardware para que ele exerça as funções devidas; *Peopleware*, que são os agentes humanos envolvidos com aqueles dispositivos, com seu uso e configuração.

2.2.1.1 Hardware

Associado à parte física dos dispositivos temos os elementos que interagem com o mundo real, sendo este um dos principais objetivos dos IoTs industriais. Dentre estes, os hardwares que se destacam são os sensores, que ajudam a coletar os dados do ambiente em que ele estiver inserido, existindo diversos sensores que captam desde simples faixas de temperaturas até feeds de vídeo completos.

Um outro exemplo de hardware são IoTs de gestão de energia, que tornam as redes elétricas mais eficientes e confiáveis, onde os dados coletados pelo hardware dos dispositivos podem ajudar empresas a reduzir desperdícios, podendo encontrar onde e quando na rede a energia é necessária e redirecionando-a para estes lugares quando necessário (OTÁVIO, 2019).

Na cadeia de suprimentos e logística os dispositivos podem ser integrados as cargas para melhorar a visibilidade e rastreabilidades delas em tempo real, e analisando estes dados é possível identificar e trabalhar nas ineficiências e otimizar todo o processo (OTÁVIO, 2019).

Pensando nestes dispositivos e em todos os demais, criados para os mais variados fins, algo que todos têm em comum é sua arquitetura. Analisando a arquitetura de um objeto inteligente, temos 4 unidades que o compõe, apresentadas por Zabadal e Castro (2017):

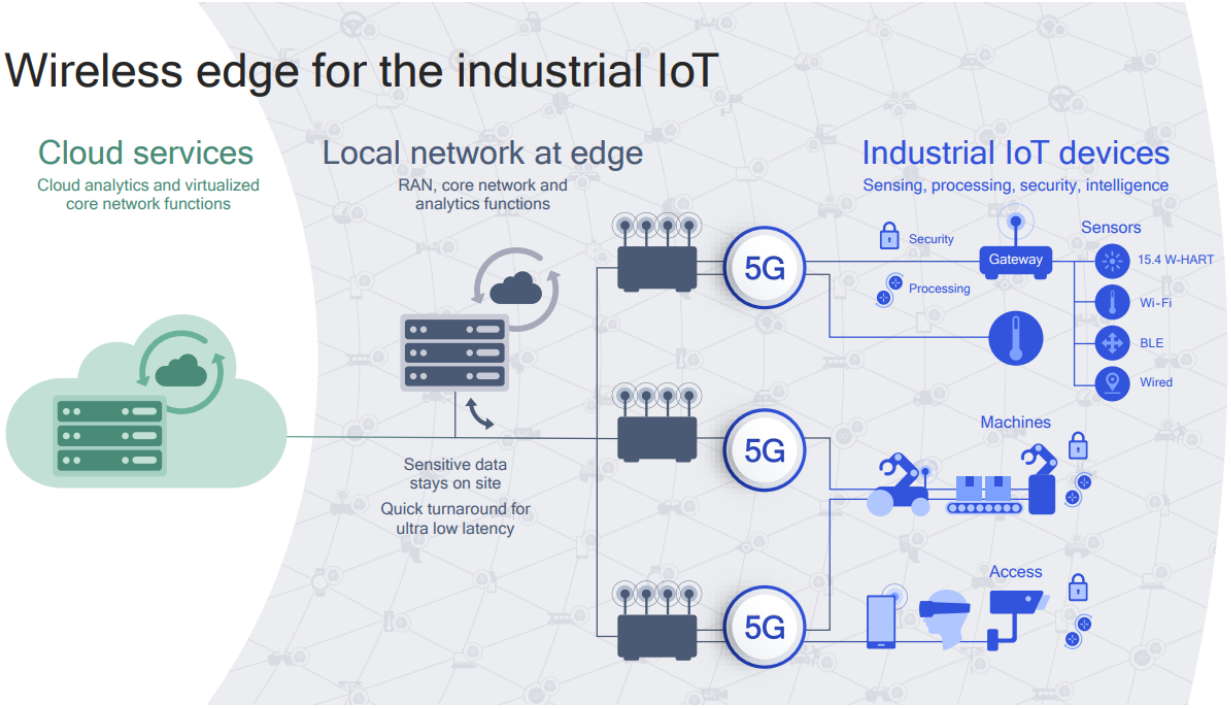
- Fonte de energia, que alimenta a energia do dispositivo, podendo ser na forma de baterias (recarregáveis ou não) ou energia elétrica;
- Sensores/Atuadores: monitoram o ambiente em que o objetivo está inserido (sensores) ou então produzindo movimentos obedecendo a comandos (atuadores);
- Processamento/memória: para armazenar dados e programas, e também um microcontrolador e conversor analógico para receber o sinal dos sensores, porém sem alto poder computacional;
- Comunicação: um meio de comunicação com ou sem fio.

Após a coleta dos dados, uma etapa é essencial, a de transmissão destes

dados para que possam ser tratados. Esta transmissão pode ser feita através de diversos tipos de conexões como redes celulares, de satélite, Wi-Fi, Bluetooth, WAN (Redes de área ampla), LAN (Redes de área local), LoRaWan, dentre outras.

E após a transmissão eles chegam em outro ponto da estrutura de hardware relacionada aos IoTs, os servidores. Muitas vezes na nuvem, os servidores compõem “uma rede que disponibiliza ou armazena recursos para com seus integrantes” (Bug Busters, 2018). São neles onde os dados que os dispositivos IoT captam são armazenados.

Figura 1 - Infográfico da infraestrutura de uma indústria utilizando dispositivos IoT



Fonte: Qualcomm, 2019, p. 23

Na figura 1 pode-se observar a infraestrutura de uma indústria utilizando dispositivos IoT, onde neste caso é utilizada a rede 5G para transmissão dos dados gerados localmente. Neste cenário, temos sensores, máquinas e demais dispositivos como câmeras IoT atuando na “ponta” da rede, onde os mesmos enviam seus dados para a rede local, de onde são redirecionados para a computação em nuvem.

2.2.1.2 Software

Os *softwares* presentes nos dispositivos IoT buscam ser compactos em decorrência da sua simplicidade física. São feitos com o mínimo possível de funções desnecessárias e configurados pensando em seu objetivo final, variando de acordo com cada dispositivo.

Dentre os *softwares* que compõem as funcionalidades dos IoT, os Sistemas Operacionais (SO) são vitais, pois ficam ativos durante todo o tempo de operação dos dispositivos (AL-FUQAHA et al., 2015). Dentre os SOs, uma de suas categorias são os Sistemas Operacionais de Tempo Real (RTOS) que segundo LI e YAO (2003), são programas que prezam pela execução em tempo hábil através do agendamento destas execuções, além disso, gerenciam os recursos do sistema e fornecem uma base consistente para o desenvolvimento do código do aplicativo. Este código pode ser muito diversificado, indo de um simples cronômetro digital até aplicações complexas para navegação aérea:

> Existem vários sistemas operacionais em tempo real (RTOS) que são bons candidatos para o desenvolvimento de aplicativos IoT baseados em RTOS. Por exemplo, o Contiki RTOS tem sido amplamente usado em cenários de IoT. A Contiki tem um simulador chamado Cooja que permite ao pesquisador e desenvolvedores simular e emular IoT e aplicativos de rede de sensores sem fio (RSSF). TinyOS, LiteOS e Riot OS também oferecem um sistema operacional leve projetado para ambientes IoT (AL-FUQAHA et al., 2015, p. 2351, tradução nossa).

Outra parte importante que pode atuar em conjunto com os RTOSs são as plataformas de nuvem. Estas plataformas oferecem facilidades para que os IoTs enviem seus dados para a nuvem, para que o *big data* seja processado em tempo real. Exemplos de *software* de plataforma em nuvem de código aberto são o Hadoop e o Nimbits (AL-FUQAHA et al., 2015).

2.2.1.3 Peopleware

São todas as pessoas envolvidas com a TI e seus dispositivos e sistemas, seja desde o desenvolvedor, analista de sistemas, cliente ou usuário final que faz uma consulta no sistema.

Dentro do *peopleware* no cenário dos IoTs um ponto para preocupação é a

formação dos profissionais que desenvolvem, criam e mantêm estes dispositivos e seus softwares.

Pegando como exemplo as matrizes curriculares dos cursos de mecatrônica, análise e desenvolvimento de sistemas e ciências da computação, ou seja, profissionais que constroem e desenvolvem estes dispositivos, vemos que no curso de análise e desenvolvimento de sistemas do Instituto Federal de Santa Catarina (IFSC) há uma disciplina de Segurança da Informação com carga horária de 40 horas. No curso de ciências da computação da Universidade Federal de Santa Catarina (UFSC) há uma disciplina de Segurança em Computação com carga horária de 72 horas. Porém ao olharmos as matrizes curriculares do curso de mecatrônica de ambas as instituições, ambos não possuem nenhuma disciplina para falar de segurança da informação.

Neste cenário, podemos notar que os futuros profissionais que cuidarão principalmente do *hardware* de dispositivos IoT não possuem noções básicas de segurança, enquanto que os profissionais de software já possuem um certo conhecimento básico. Isto reflete na arquitetura dos dispositivos, muitas vezes construídos de forma compacta para otimizar espaço e consumo de energia, mas que acabam não possuindo recursos para aplicarmos técnicas de segurança mais complexas.

- **Programação e Segurança da Informação (SI)**

Quando pensamos no desenvolvimento de dispositivos IoT e em sua segurança não podemos só pensar nas fragilidades externas ao dispositivo, devemos dar também, a devida atenção ao funcionamento interno do mesmo, ou seja, ao software que dá vida ao hardware do IoT (o cérebro lógico que deixa o objeto “inteligente”), portanto o *peopleware* desenvolvedor também é importante para a segurança da informação. Uma fragilidade em qualquer parte do código do dispositivo pode abrir brechas para potenciais invasores, e no caso dos IoTs, como dito anteriormente, onde o sistema busca ser compacto, não podemos comprometer a segurança em seu desenvolvimento em busca dessa simplicidade.

> Em determinadas situações, a programação é tão importante quanto a própria definição da cultura de proteção de dados. Quanto mais conhecimento sobre os dados e a informação de seus fluxos, melhor será o acompanhamento para a

pessoa gestora de TI e sua equipe (Noleto, 2020).

Além de nos certificarmos quanto aos pilares da segurança da informação, algumas formas de programação são grandes aliadas na busca pela segurança dos dados. A programação pode nos auxiliar desde o mapeamento de movimentações anormais até alertas sobre possíveis riscos, ou seja, a pessoa programadora tem papel fundamental (Noleto, 2020).

- **Senhas fracas:**

Um ponto de atenção que deve ser levado em conta quando pensamos em todo o peopleware de uma empresa é a utilização de senhas fracas. Um artigo escrito por Harán (2020) da empresa *WeLiveSecurity* mostra que em uma análise feita em mais de um bilhão de senhas vazadas em diversas violações sofridas por empresas, a senha "123456" é a senha mais comum e utilizada nos últimos cinco anos, sendo repetida mais de sete milhões de vezes.

Em pesquisa online feita pela empresa Avast em 2019, descobriram que:

> "95% dos brasileiros não consideram números, caracteres especiais, letras maiúsculas e minúsculas ao criar senhas. Também não criam senhas que tenham pelo menos 10 caracteres. A pesquisa constatou ainda que mais metade dos brasileiros (51%) usa a mesma senha para proteger várias contas, colocando-as em risco de serem violadas."

A mesma pesquisa revelou ainda que muitos brasileiros incluem dados pessoais na senha, até mesmo informações que podem ser encontradas facilmente em mídias sociais, como:

- Seu nome ou o nome de um membro da família (23%);
- Nome do seu animal de estimação (8%);
- Aniversário (14%);
- Palavras relacionadas ao seu hobby (9%);
- Dados do endereço residencial (3%);
- O nome do seu livro ou filme favorito (6%);
- Nomes de celebridades (5%);

- O nome do site, no qual usa a senha (4%).

A utilização de senhas fracas e que contenham dados pessoais em sua composição acaba abrindo uma brecha para que pessoas mal intencionadas possam atuar. Uma das técnicas que estas pessoas podem utilizar é a engenharia social para obter estes dados.

- **Ataques com engenharia social:**

O termo engenharia social caracteriza práticas que são utilizadas para obter informações sigilosas ou importantes do alvo, se utilizando da confiança das pessoas para enganá-las. Como outra definição temos que ela é a arte de contornar mecanismos de segurança por meio da manipulação de pessoas, construindo métodos e estratégias para ludibriá-las se utilizando de informações cedidas por elas mesmas, desta forma ganhando a confiança delas para obter informações (SILVA, 2008).

"A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação." (PEIXOTO, 2006, p. 36). Portanto não podemos esquecer da engenharia social quando estamos pensando em segurança da informação.

Algumas características tornam o ser humano passível a ataques de engenharia social conforme Junior (2006, apud ALVES, 2010, p. 43):

- Vontade de se tornar útil, pois o ser humano procura ser gentil e ajudar outros;
- Buscar amizades, humanos acabam se abrindo ao receber elogios pois se sentem bem com isso;
- Prorrogar responsabilidades, pois o ser humano não considera as responsabilidades como algo individual;
- Persuasão, ou capacidade de convencimento, pois o ser humano possui características que o tornam suscetível a manipulação.

2.2.2 SEGURANÇA DOS DISPOSITIVOS IOT

Cada um dos múltiplos dispositivos IoT presentes nas casas e empresas são um potencial ponto de vulnerabilidade e estes dispositivos conectados podem ser usados como uma forma de entrada para a rede e assim dar início a um grande ataque.

2.2.2.1 Riscos/Ameaças

No cenário da IoT, todos os aparelhos estão interconectados e isto pode gerar diversos problemas, pois se um único dispositivo estiver mal protegido e conectado a rede, ele pode consequentemente afetar toda a segurança da mesma (FIGUEIRA, 2016).

Uma característica destes dispositivos que acaba contribuindo para o problema anterior é que diversos tipos destes aparelhos são implantados em massa, como é o caso de sensores, o que aumenta a chance de um deles estar desprotegido.

Além disso, as particularidades da IoT geram outros problemas, pois nela, comunicações podem ser realizadas através de redes sem fio, que podem ser colocados em locais públicos onde estão ao alcance de qualquer indivíduo e muitos dispositivos contam com recursos limitados, onde medidas de segurança que demandam processamento poderiam acarretar em impactos como redução das funcionalidades do dispositivo, por exemplo (FIGUEIRA, 2016).

Lidando com dispositivos IoT, diversos desafios estão presentes, uma vez que em uma implantação de conjuntos de dispositivos, muitos tendem a ser idênticos ou quase idênticos, o que faz com que brechas descobertas em um deles possam ser exploradas nos demais. E dependendo da utilização do dispositivo, ele pode ser posicionado em locais ou ambientes de difícil acesso, o que torna a sua atualização ou configuração mais complicada. Na figura 2 pode-se observar a relação entre o nível de conexão de um dispositivo com o nível de proteção do mesmo.

Figura 2 - Principais ciclos da Internet das Coisas

Fonte: Aruba (2016). Adaptado por Zabadal, et al. (2017), p. 7

Nesse cenário, pessoas mal intencionadas podem utilizar estas brechas para realizar diversos tipos de ataques, sendo eles ativos ou passivos, como um ataque *man-in-the-middle*, DDoS, *sniffing* entre outros. Estes ataques podem ter como objetivo apenas a captura dos dados que correm na rede, a alteração deles ou até mesmo deixar a rede fora do ar.

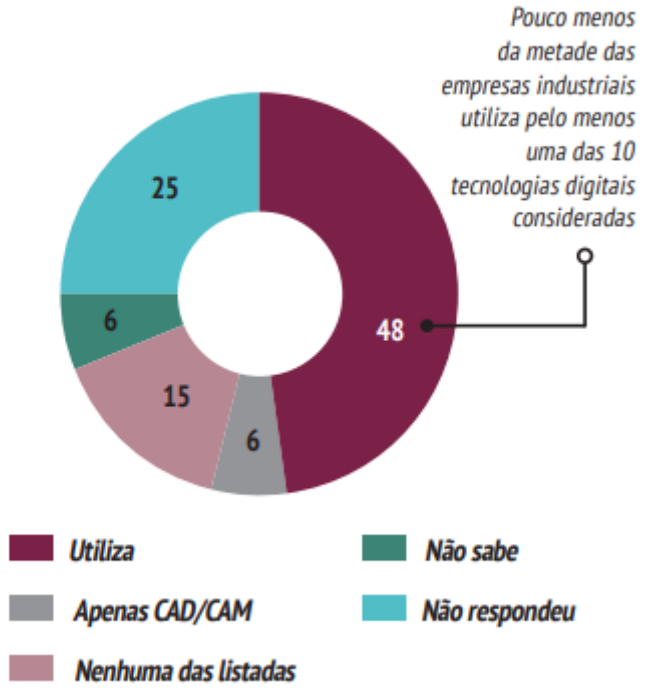
2.3 INFRAESTRUTURA DA INDÚSTRIA 4.0 NO BRASIL

No cenário atual a evolução e adoção das tecnologias da indústria 4.0 pelas empresas se torna algo natural, pois sem elas a competição e concorrência do mercado pode acabar deixando as organizações para trás.

Mas no Brasil, o estágio de difusão dessas tecnologias ainda está pouco desenvolvido, como atesta uma pesquisa da Confederação Nacional da Indústria (2016). “Do total das indústrias, 58% conhecem a importância dessas tecnologias para a competitividade da indústria e menos da metade as utiliza” (CONFEDERAÇÃO NACIONAL DA INDÚSTRIA, 2016).

No gráfico 2 podemos observar os resultados de uma pesquisa realizada pela Confederação Nacional Da Indústria (2016), onde foi levantado que mais da metade das indústrias que compõem a pesquisa conhecem a importância das tecnologias da indústria 4.0, porém menos da metade as utiliza.

Gráfico 2 - Utilização de pelo menos uma das tecnologias digitais listadas na pesquisa



Fonte: Confederação Nacional Da Indústria, 2016, p. 1

> Uma das constatações mais relevantes do levantamento foi o baixo conhecimento das empresas da importância das tecnologias digitais para a competitividade: "43% não identificaram quais tecnologias digitais, em uma lista com 10 opções, têm o maior potencial para impulsionar a competitividade da indústria. O desconhecimento é significativamente maior entre as pequenas empresas (57%). Entre as grandes empresas, o percentual de empresas que não identificaram alguma das 10 tecnologias digitais apresentadas como importantes para a competitividade cai para 32%"3. Esses dados demonstram o distanciamento da indústria brasileira das tecnologias digitais (VERMULM, 2018).

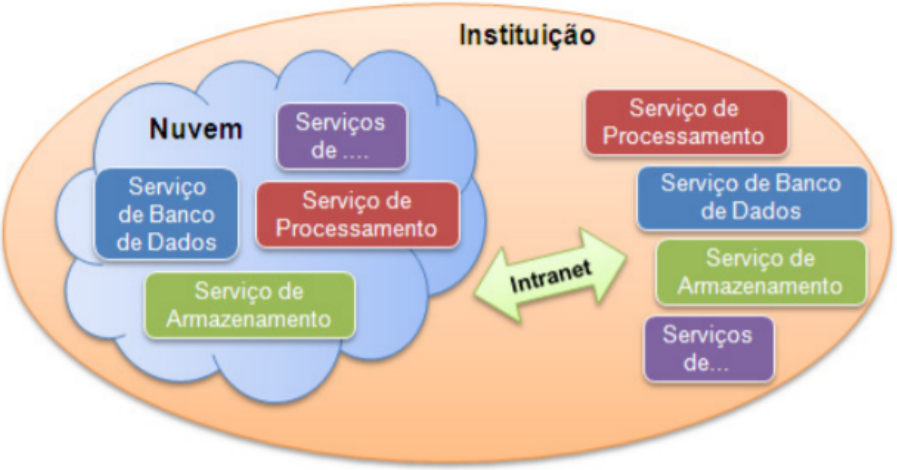
Porém, o tema da Indústria 4.0 está cada vez mais presente em agendas de instituições públicas, entidades empresariais, academias e de agências de fomento. Algumas dessas instituições têm implementado ações de promoção enquanto que outras têm proposto políticas públicas. Mas a predominância da difusão e adoção dessas tecnologias se dá por empresas industriais instaladas no país (VERMULM, 2018).

2.4 *CLOUD COMPUTING*

Na *Cloud Computing* (Computação em Nuvem), as informações são guardadas

na nuvem e podem ser acessadas de qualquer lugar. Ela tem como objetivo facilitar o acesso às informações de forma mais descentralizada, ajudando nas decisões estratégicas. A sua infraestrutura possui desde recursos físicos como servidores, redes de armazenamento, computadores e etc, até recursos abstratos como softwares e soluções integradas (YEN et al., 2014 apud SOUZA; CAVALLARI JUNIOR; DELGADO NETO, 2017). Na figura 3 pode-se observar um esquema demonstrando uma nuvem privada de uma instituição, com seus serviços locais ligados à nuvem pela intranet.

Figura 3 - Nuvem privada de uma instituição



Fonte: BORGES et al., 2011, p. 11

2.5 SEGURANÇA DA INFORMAÇÃO

A segurança da informação se baseia nos pilares da preservação da confidencialidade, integridade e disponibilidade, podendo ter outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade também englobadas na definição.

Para que haja uma segurança da informação eficaz, é necessário o levantamento dos requisitos de segurança. Os requisitos de segurança são identificados através de uma avaliação dos riscos de segurança. Esta avaliação ajuda a determinar as ações apropriadas de gestão, além das prioridades dos riscos de segurança. A avaliação deve ser refeita periodicamente para que possíveis mudanças, que podem mudar o resultado da análise, sejam identificadas.

“A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.” (HINTZBERGEN et al., 2018)

Os passos que a ISO 27002 (ABNT, 2013), o “Código de prática para a segurança da informação” (*Code of practice for information security*), aborda como mais importantes são:

1. Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação.
2. Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócio da organização.
3. Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (Information Security Management System – ISMS).
4. Melhoria contínua baseada em medições objetivas.

A segurança da informação tem como base a proteção das informações contra qualquer tipo de ameaça, para que assim a organização possa ter uma continuidade dos negócios. A segurança é basicamente feita com uma análise e identificação das potenciais ameaças, sendo elaboradas soluções para conter ou bloqueá-las, sempre monitorando-as. Este trabalho é contínuo, para que novos riscos possam ser identificados e controlados.

2.5.1 PRINCIPAIS TIPOS DE ATAQUES

Indo contra os pilares da segurança da informação, indivíduos mal intencionados podem querer quebrar a confidencialidade, integridade e disponibilidade de serviços e/ou informações. Para esse intuito ataques são utilizados, visando diversos tipos de alvos e usando diversas técnicas diferentes.

Nesse cenário, qualquer serviço, computador, dispositivo ou rede pode ser um alvo em potencial para um ataque. Assim como qualquer computador ou dispositivo inteligente, como os IoTs, podem participar de um ataque como um integrante do mesmo

(CERT, 2016).

Podemos classificar os diversos tipos de ataques em quatro tipos: Ataques passivos, ativos, de senha e de peopleware. Nos ataques passivos, as informações ou seu fluxo normal não são alterados.

> Baseados em escutas e monitoramento de transmissões, com o intuito de obter informações que estão sendo transmitidas. A escuta de uma conversa telefônica é um exemplo dessa categoria. Ataques dessa categoria são difíceis de detectar porque não envolvem alterações de dados, todavia podem ser prevenidos com a utilização de criptografia. (NETO e ARAÚJO, 2019, p.40).

Nos ataques ativos, há uma alteração no fluxo normal da informação, seja uma modificação no conteúdo ou produção de informação falsa, para desta forma tentar infringir a segurança de um sistema.

> Envolvem modificação de dados, criação de objetos falsificados ou negação de serviço e têm propriedades opostas às dos ataques passivos. São difíceis de ser prevenidos, por causa da necessidade de proteger completamente todas as facilidades de comunicação e processamento, durante o tempo todo. Assim, é possível detectá-los e aplicar uma medida para recuperar prejuízos causados. (NETO e ARAÚJO, 2019, p.40).

Já os ataques dos tipos senha e *peopleware* não se encaixam como ataques passivos ou ativos, porém possuem o mesmo objetivo, adquirir certas informações. Mesmo que estes ataques não alterem a informação ou seu fluxo, eles podem não ser realizados de dentro do sistema ou rede alvo, por isso possuem classificações próprias.

2.5.1.1 Ataques passivos

Dentre os tipos de ataques passivos que pessoas mal intencionadas podem utilizar e que não alteram o fluxo ou a informação em si, podemos citar como mais relevante para o contexto dos IoTs:

***Sniffing*:** A Interceptação de Tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados pelas redes de computadores, por meio de programas chamados Sniffers. Estes softwares são utilizados com frequência para monitorar redes a fim de detectar problemas de tráfego e manter o fluxo de dados eficiente (CERT, 2016).

Estes softwares podem ser utilizados de forma legítima por administradores de

redes, para detectar problemas ou gargalos no desempenho em computadores ou redes em que ele atua. Porém podem ser utilizados de forma ilegítima por intrusos, para capturar tudo o que passa por eles, inclusive senhas e nomes de usuários. Os *sniffers* exploram o fato dos pacotes *TCP/IP* não serem criptografados. Contudo, para a sua utilização, é necessário que ele esteja instalado em um ponto da rede onde estes pacotes com informações interessantes para o invasor ou administrador estejam passando (FUKUDA, 2019).

2.5.1.2 Ataques ativos

Além dos ataques citados acima, temos também os tipos de ataques ativos que pessoas mal intencionadas podem utilizar e que alteram o fluxo ou a informação em si, podemos citar como mais relevantes para o contexto dos IoTs:

Man-in-the-Middle: O ataque “Homem no Meio” tem como objetivo fazer com que o *host* do atacante entre como um intermediador entre a conexão de dois dispositivos, transformando-o em um *proxy* anônimo. Uma vez que o atacante está servindo como intermediador na conexão, ele pode “ouvir” o que trafega nela e espera por algo relevante, como *login*, senhas ou outros dados sensíveis. Porém, além de ouvir, o atacante pode adulterar informações que saem ou chegam em um determinado *host*, sem ser detectado (ANDRADE e SANTOS, 2018).

Este ataque pode ser classificado como um ataque passivo caso o atacante não interfira no fluxo da informação, ou seja, se o ataque só tiver o intuito de “ouvir” o que trafega na rede.

> Dentro da Internet das Coisas, podemos imaginar um cenário em que uma parte mal-intencionada pode querer falsificar dados de temperatura de um dispositivo de monitoramento para forçar um equipamento a superaquecer, interrompendo a produção. Além de inconveniente para os negócios, isso também pode levar a danos físicos e financeiros para a operação da organização. (SIMKO, 2016, tradução nossa)

DoS/DDoS: Ataques de Negação de Serviço, ou *Denial of Service*, tem como objetivo impedir que usuários consigam utilizar determinado serviço, computador ou rede,

tirando os mesmos de operação. Um ataque de DoS busca derrubar o alvo realizando inúmeras requisições a ele, até que o mesmo saia do ar. Quando o ataque for de forma coletiva, utilizando-se diversos dispositivos, é chamado de DDoS (*Distributed Denial of Service*) (FUKUDA, 2019).

Os ataques DDoS têm um impacto muito grande quando os relacionamos com o cenário dos dispositivos IoT. Como os IoT são feitos e usados em grande quantidade, isto também aumenta o número de dispositivos que podem ser usados para realizar ataques DDoS. Um exemplo do impacto dos IoTs para este tipo de ataque é que, em 2016, segundo matéria do site NetworkWorld, houve o maior ataque DDoS até então e este foi causado por dispositivos Internet das Coisas sequestrados para este fim.

"Proteger a Internet das coisas deve se tornar uma grande prioridade agora que um exército de dispositivos comprometidos - com talvez um milhão deles - invadiu um dos principais serviços de proteção de negação de serviço distribuídos do setor." (GREENE, 2016, tradução nossa)

2.5.1.3 Ataque de Senha

Para conseguir um acesso é necessário conhecer a senha, e para isso invasores tentam descobri-la através de técnicas de quebra de senhas, como tentar senhas padrões ou senhas simples, como nomes pessoais, nome da empresa, datas, entre outros. Porém, atualmente existem ferramentas que auxiliam essa descoberta da senha e estas utilizam diferentes técnicas para tal finalidade (FUKUDA, 2019). Dentre os ataques de quebra de senha, destacam-se:

- Força bruta: Um ataque de força bruta, ou *brute force*, é o método mais simples, porém demorado, para obter acesso a um dispositivo ou sistema (que esteja protegido por senha). Ele consiste em simplesmente adivinhar, por tentativa e erro, nomes de usuário e senhas. Atualmente muitas ferramentas automatizam esta técnica de quebra de senha (JESUS, 2016).

- Dicionário: Ao invés da força bruta, que testa todas as combinações possíveis de caracteres, o ataque de dicionário utiliza um dicionário de senhas possíveis e tenta todas as combinações contidas nele que podem eventualmente fazer parte da composição de uma senha. A mistura deste ataque com o de *brute force* recebe o nome de *Syllabe* (JESUS, 2016).

- Rainbow Tables: Este método é destinado à quebra de senhas com criptografia e consiste em comparar os *hashs* da criptografia da senha desejada com *hashs* já calculados e armazenados em uma tabela até descobrir o correspondente (JESUS, 2016).

> Rainbow Table é um método para descobrir senhas a partir de hashes, de forma rápida. A ideia básica é pré-computar uma longa lista de senhas, com seus respectivos hashes gerados por algum algoritmo específico, e armazenar essa lista em um arquivo, no formato de uma tabela. Assim, é possível reverter uma função de hash criptográfico. (REIS, 2019)

2.5.1.4 Ataque de Peopleware

Dentre os tipos de ataques de *peopleware* que pessoas mal intencionadas podem utilizar para adquirir informações confidenciais tendo como ponto central e alvos as pessoas que fazem parte da organização, podemos citar como mais relevante para o contexto dos IoTs:

Engenharia Social: Este ataque ocorre com foco no fator humano, sendo pouco baseado em ferramentas computacionais. Na Engenharia Social, os invasores tentam extrair o máximo de informações que conseguirem do *peopleware*, ou seja, das pessoas que têm contato com o sistema alvo (MACHADO, 2009).

> Serão pessoas que buscarão extrair informações do sistema das mais diferentes formas – através de conversas pessoais com operadores do sistema ou pessoas com dados de acesso ao sistema corporativo, através de ligações telefônicas fingindo ser outras pessoas, será através de e-mail pedindo dados sensíveis ou até mesmo verificando lixeiras físicas da instituição. (MACHADO, 2009)

2.5.2 PRINCIPAIS TIPOS DE DEFESAS

Para ajudar a manter a Segurança da Informação e seus pilares, técnicas e diretrizes podem ser aplicadas para mitigar os riscos que indivíduos mal intencionados podem utilizar para causar impactos severos na rede e nos serviços das organizações. Uma rede que utiliza técnicas de proteção se torna um alvo mais complexo, por possuir menos vulnerabilidades que podem ser exploradas e as que existirem serem mais difíceis de se explorar.

Existem técnicas e diretrizes que ajudam a aumentar a proteção contra todos os tipos de ataques. Manter os sistemas e dispositivos atualizados e realizar checagens periódicas dos mesmos e da própria rede auxilia contra ataques ativos e passivos. Instruir os colaboradores a utilizarem senhas fortes ou até mesmo outros tipos de validações de acesso auxilia contra ataques de senha e mesmo de *peopleware*.

As defesas em relação a ataques ativos e passivos são métodos técnicos, que incluem novas barreiras e realizam monitoramentos na rede. Enquanto que as defesas em relação a ataques de senha e de *peopleware* são mais direcionais para orientações e normas sobre o dia a dia dos colaboradores.

2.5.2.1 CRIPTOGRAFIA

Em uma rede corporativa, diversos dispositivos (sendo dispositivos IoT ou não) transmitem dados para a rede a todo o momento, sendo que alguns desses dados podem ser confidenciais. Transmitir esses dados diretamente pela rede acaba se tornando uma forma insegura de transmissão, visto que se um atacante já obteve acesso à rede, ele tem em seu alcance todos os dados sendo trafegados.

Para melhorar a proteção dos dados dispomos da técnica da criptografia para dificultar o acesso à informação, onde mesmo que o atacante consiga adquirir os dados, precisará decifrá-los para obter o real conteúdo.

Segundo Albarello (2019), para que um algoritmo de criptografia seja considerado seguro, ele deve embaralhar suficientemente o conteúdo original para que

seja computacionalmente inviável descobrir o teor original da mensagem, tendo o conteúdo criptografado e o algoritmo usado.

Os algoritmos de criptografia utilizam uma chave para que o emissor da mensagem consiga criptografá-la e o receptor consiga descriptografá-la e acessar seu conteúdo. Estas chaves podem ser utilizadas de duas formas diferentes, separando os algoritmos em algoritmos simétricos e assimétricos, baseado na forma de utilização da chave, cada um com suas vantagens e desvantagens.

O algoritmo simétrico utiliza uma chave privada para criptografar e descriptografar as informações. Para que as informações possam ser compreendidas, tanto o emissor da mensagem quanto o receptor devem possuir a chave. O algoritmo simétrico é relativamente eficiente quanto à velocidade e processamento necessários, porém a segurança é um grande ponto de atenção, pois a chave tem que ser compartilhada com o destinatário.

Já o algoritmo assimétrico consiste em duas chaves, uma privada e outra pública, que são utilizadas juntas para que as informações sejam criptografadas e descriptografadas. Nesse algoritmo, somente a chave pública precisa ser compartilhada, onde ela é utilizada para criptografar as mensagens, enquanto que a chave privada é usada para descriptografar. Isso auxilia para uma melhor segurança das chaves, porém necessitam de mais processamento computacional.

No quadro 1 pode-se observar a relação entre os algoritmos simétrico e assimétrico, levando em conta as vantagens e desvantagens de cada tipo.

Quadro 1 - Algoritmos Simétrico e Assimétrico

Algoritmos Simétrico e Assimétrico		
	Vantagens	Desvantagens
Simétrico	Boa segurança	Segurança do compartilhamento de chave
	Melhor performance	Gerenciamento de chaves
	Menor processamento computacional	
Assimétrico	Boa segurança do compartilhamento de chave	Requer chaves mais complexas para segurança equivalente aos simétricos
	Altamente escalável	Menor performance
	Usos múltiplos (autenticação, controle de acesso, confidencialidade e privacidade, integridade de dados, não repúdio)	Maior processamento computacional

Fonte: Miller, 2016, p. 26, tradução nossa

Tanto o algoritmo simétrico como o assimétrico possuem vantagens e desvantagens, portanto a utilização de uma das opções irá depender do cenário da organização, levando em consideração as informações que serão protegidas, a capacidade de processamento disponível e como os dados serão transmitidos.

2.5.2.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Um dos recursos para ajudar a mitigar riscos relacionados ao *peopleware* e ataques de Engenharia Social é ter uma boa política de segurança. As políticas de segurança da informação (PSIs) são instruções claras que fornecem orientações de comportamento aos colaboradores ao manipular as informações, sendo um elemento fundamental para combater possíveis ameaças à segurança.

Segundo Fonseca (2009), um programa de segurança da informação amplo se inicia com uma avaliação de risco para determinar três pontos:

- Quais são as informações da empresa que precisam ser protegidas?
- Quais ameaças específicas existem contra os ativos?
- Qual dano seria causado às empresas se essas ameaças em potencial se materializassem?

Ao pensarmos nas informações que precisam de proteção, se faz necessária uma classificação e a realização de uma análise de custo/benefício de cada grupo, para determinar qual proteção será eficaz em termos de custo. Basicamente, quais as informações que serão protegidas em primeiro lugar e qual será o custo dessa proteção.

Outro ponto importante para que a política seja efetiva, é que os colaboradores entendam a sua importância, para que sejam motivados a segui-la. Para isso, é essencial que a alta gerência suporte o desenvolvimento das políticas e as adote, para que o exemplo venha de cima, mostrando que a proteção das informações da empresa é fundamental para que ela continue funcionando.

Para que todos os colaboradores consigam entender as políticas, é vital que elas sejam escritas sem uso de jargões técnicos, para que possam ser compreendidas pelos empregados não técnicos. Além disso, as consequências do descumprimento das políticas e procedimentos de segurança devem ser amplamente divulgadas para os colaboradores, assim como reconhecimentos e recompensas de boas práticas, quando um funcionário relatar ou ajudar a impedir um incidente, por exemplo.

Um ponto importante sobre a política de segurança é que ela deve ser adaptável. Uma empresa pode mudar em decorrência do surgimento de novas tecnologias de segurança, e simultaneamente, a política deve ser revisada e alterada se necessário, à medida que vulnerabilidades evoluam ou novas se apresentem.

Para isso, testes periódicos de penetração (*pentest*) e avaliações de vulnerabilidade usando métodos da engenharia social devem ser realizados para identificar os pontos fracos dos treinamentos ou falhas nas políticas e procedimentos de segurança da empresa. No entanto, antes de realizar qualquer teste de penetração simulado, os colaboradores devem ser avisados de que testes podem ocorrer de forma

periódica (Fonseca, 2009).

Os redatores das políticas de segurança da informação de uma organização devem analisar o ambiente e os objetivos de negócio da empresa para que possam elaborar as políticas. Elas serão estabelecidas de acordo com os requisitos, necessidades, cultura, sistemas de informação e tamanho de cada organização. Na figura 4 pode-se observar a pirâmide PSI, com as ações classificadas pelo seu nível.

Figura 4 - Pirâmide PSI

Fonte: Aurélio, 2015

Ao analisarmos o PSI (Política de Segurança da Informação) do Instituto Federal de Amazonas (IFAM) (2012), temos os seguintes tópicos abordados como exemplo: Membros; Regulamentação; Composição e Atribuições; Fundamentos; Recomendações Gerais (Usos aceitáveis dos recursos de TI, uso seguro dos recursos, atividades permitidas, atividades não permitidas); Recomendações Específicas (Controle de acesso, utilização do correio eletrônico corporativo, utilização de aplicações corporativas e softwares de terceiros, manipulações das informações).

2.5.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Um fator importante que irá afetar as empresas brasileiras a partir de 2020 é a

Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece normas rigorosas para a proteção dos dados pessoais. Com ela entrando em vigor, todas as empresas que fazem tratamento de dados pessoais deverão tomar uma série de medidas para garantir o cumprimento da nova legislação (MACHADO MEYER SENDACZ OPICE ADVOGADOS, 2018).

A LGPD tem como principais objetivos a privacidade, transparência, desenvolvimento, padronização, proteção do mercado e a concorrência. Estes objetivos visam assegurar direitos, estabelecer regras, fomentar o desenvolvimento, fortalecer a segurança e promover a concorrência.

Alguns dos artigos da LGPD no quesito de segurança e sigilo dos dados diz que:

- Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (art. 46).

- As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (art. 46, § 2º).

- Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares (art. 49). (BRASIL, 2018)

A Lei Geral de Proteção de Dados Pessoais atua para que as organizações que manipulam dados se preocupem com a segurança dos mesmos. As empresas e indústrias terão que implementar políticas corporativas adequadas, além de realizar treinamentos de pessoal para respeitar os dados pessoais de clientes, empregados e demais contratados (MACHADO MEYER SENDACZ OPICE ADVOGADOS, 2018).

3. PROCEDIMENTOS METODOLÓGICOS

Nesta seção serão apresentados os procedimentos metodológicos utilizados na elaboração desta pesquisa. Primeiro será mostrada a caracterização da pesquisa, e em seguida serão explicitadas as etapas que compõem o desenvolvimento desta pesquisa.

3.1. CARACTERIZAÇÃO DA PESQUISA

A presente pesquisa pode ser classificada quanto à sua natureza como uma pesquisa científica aplicada, onde o objetivo é fazer uso das informações e conhecimento já apontados, buscando resolver problemas organizacionais (ALMEIDA, 2010).

Quanto a sua caracterização em relação aos objetivos, a pesquisa pode ser classificada como descritiva e explicativa. Pesquisa descritiva porque tem como intuito descrever o objeto de estudo, analisando as suas características e problemas relacionados. E como pesquisa explicativa, pois tem foco na identificação dos fatores que colaboram para que certos fenômenos ocorram, com suas causas e efeitos, explicando a razão de tal ocorrência, levando em consideração a contextualização quanto ao tempo e espaço, ou seja, o ambiente social onde o fato está inserido (ALMEIDA, 2010).

Em relação a abordagem, a pesquisa pode ser classificada como qualitativa, utilizando o enfoque indutivo na análise dos dados e dando foco para os significados dados pelas pessoas às coisas, não sendo necessário o uso de ferramentas estatísticas de análise de dados. A presente pesquisa tem como intuito analisar as falhas de segurança existentes nos dispositivos IoT, considerando o cenário que estão inseridos e a partir disso, efetuar testes e avaliar práticas para mitigar os problemas encontrados.

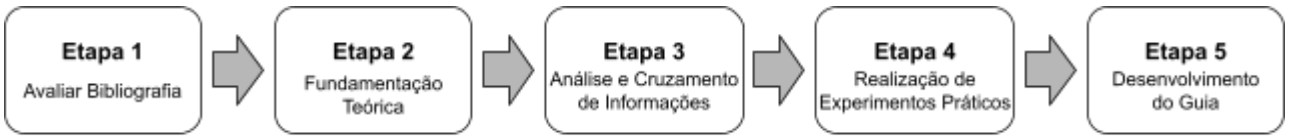
Em relação às características de pesquisa, caracteriza-se como uma pesquisa bibliográfica e experimental. Na pesquisa bibliográfica o estudo se baseia em livros e artigos científicos, com a finalidade de buscar relações entre conceitos, características e ideias, ocasionalmente unindo dois ou mais temas. Na pesquisa experimental, segundo Almeida (2010), “[...] algumas variáveis são avaliadas quanto à influência que exercem

sobre outras. Normalmente utiliza-se um grupo de controle, que não receba a influência da variável em questão, para avaliar as diferenças em relação a outro grupo que receba.”

3.2. ETAPAS DA PESQUISA

Realizada a devida caracterização da pesquisa, é importante mencionar as etapas em que a pesquisa foi dividida. Os passos que foram seguidos para a realização da pesquisa seguem abaixo, em ordem e podem ser vistos na figura 3.

Figura 3 - Etapas da pesquisa



Fonte: Elaborado pelo autor

Na etapa 1, a bibliografia sobre o tema será avaliada a fim de nortear a pesquisa, identificando os pontos que entrarão na fundamentação teórica. Os principais pontos que irão ser analisados para identificar os tópicos que também estão no ambiente da pesquisa e que merecem ser incluídos na fundamentação teórica serão: Dispositivos Internet das Coisas; Segurança da Informação; Brechas de Segurança; e Indústria 4.0.

Na etapa 2, a fundamentação teórica se dará através de livros, revistas científicas digitais, sites e teses sobre o tema Internet das Coisas, segurança da informação, indústria 4.0 e demais áreas associadas identificadas na etapa 1.

A etapa 3, análise e cruzamento de informações, consistirá na união dos dados adquiridos nas etapas 1 e 2 e cruzamento dos mesmos para correlacionar o funcionamento e os requisitos de dispositivos IoT com as brechas de segurança presentes nos dispositivos e em seu ambiente.

A etapa 4, realização de experimentos práticos, será executada utilizando o sistema operacional ContikiOS com o simulador Cooja para simular uma rede IoT e o software Wireshark para analisarmos o tráfego da rede.

A última etapa, a 5, consistirá na identificação das diretrizes, políticas e boas

práticas para mitigar os riscos de segurança da informação e no desenvolvimento do guia de segurança para dispositivos IoT contendo as recomendações de orientações e diretrizes para a segurança destes dispositivos a partir dos conhecimentos adquiridos nas 4 etapas anteriores desta pesquisa. O desenvolvimento deste documento buscará despertar a atenção de gestores e profissionais da área de segurança para os aspectos da SI na Indústria 4.0.

4. DESENVOLVIMENTO DO TRABALHO

Este capítulo tem como objetivo expor os resultados obtidos durante a fundamentação teórica e cruzamento de informações, bem como a apresentação das simulações e orientações e diretrizes de segurança da informação. A apresentação das informações será dividida em três tópicos principais: Dispositivos IoT, Testes práticos e Técnicas para mitigar riscos.

4.1 DISPOSITIVOS IOT

Para a segurança da informação no cenário dos dispositivos IoT, um ponto importante a ser analisado é o desenvolvimento e construção destes dispositivos, além de sua aplicação e da análise do ambiente em que são inseridos. Com isso, é possível identificar os possíveis riscos referentes aos pontos analisados e levantar possíveis soluções para mitigar estes riscos.

4.1.1 REQUISITOS DOS DISPOSITIVOS IOT

Os dispositivos IoT são tipicamente desenvolvidos e construídos pensando no baixo custo e simplicidade. Pelo seu tamanho físico, são desenhados para realizar somente o necessário para o objetivo final, seja ele medir temperaturas, controlar a disponibilidade de energia para a rede ou mesmo rastrear encomendas para melhorar a logística.

Na figura 5 pode-se ver as medidas de um sensor de temperatura IoT da empresa Advantech (2021). A construção de baixo custo e pensando na simplicidade dos dispositivos IoT afeta tanto o *hardware* quanto o *software* dos mesmos. Sua arquitetura se baseia em uma fonte de energia, sensores/atuadores, processamento/memória e comunicação. Neste cenário, eles podem não possuir recursos remanescentes para que soluções de segurança possam ser aplicadas nos dispositivos. Esta construção de baixo

custo levou aos testes de simulação dos ataques na rede IoT, como o ataque DDoS, com os resultados sendo visualizados através das medições no consumo de energia dos dispositivos antes e durante o ataque e o ataque de *sniffing*, impactado pela falta de recursos para aplicação de técnicas de proteção dos dados, onde os pacotes são transmitidos sem proteção para a rede.

Figura 5 - Medidas de um sensor de temperatura IoT em milímetros

Fonte: Advantech, 2021, p. 2

Outro ponto de sua aplicação é que muitos dispositivos podem ficar localizados em locais de fácil acesso (como câmeras IoT em corredores) ou então em locais de difícil acesso (como sensores de temperatura IoT). No caso dos dispositivos localizados em áreas de fácil acesso, eles ficam ao alcance de pessoas mal intencionadas. Enquanto que os dispositivos que ficam em locais de difícil acesso podem possuir uma atualização e configuração mais complicada de ser realizada.

Em relação ao *peopleware*, temos os desenvolvedores do hardware e software dos dispositivos, pois se não possuírem a segurança da informação em mente ao realizarem a construção ou codificação dos dispositivos, podem originar vulnerabilidades nos mesmos. Além disso, todos os colaboradores com acesso aos dispositivos ou qualquer outro sistema da organização também podem influenciar na segurança da rede.

4.1.2 FALHAS E RISCOS DOS DISPOSITIVOS IOT

Pensando na construção simplista e de baixo custo dos dispositivos IoT, o cuidado com a segurança destes dispositivos é importante, pois eles podem ser a porta de entrada do atacante para toda a rede da organização. Porém não são somente os dispositivos IoT que podem possuir vulnerabilidades em segurança da informação, os demais sistemas da empresa ou mesmo o peopleware em torno deles podem abrir brechas para que atacantes consigam concluir seu objetivo.

Para que consigam acesso às informações ou aos serviços da organização, os invasores aplicam ataques, utilizando vulnerabilidades encontradas na rede. Estes ataques podem ser divididos em ataques ativos, passivos, de senha ou *peopleware*. Dentre os ataques passivos mais utilizados contra dispositivos IoT temos o ataque *Sniffing* e o ataque *man-in-the-middle* (caso não o atacante não altere as informações) onde o invasor ganha acesso às informações que estão sendo trafegadas pela rede no ponto onde ele estiver “ouvindo”. Dentre os principais ataques ativos temos o *man-in-the-middle*, onde o atacante pode alterar informações sigilosas que estão sendo trafegadas na rede e o ataque DDoS, onde o invasor pode derrubar serviços da organização, realizando inúmeras requisições a ele em um curto período de tempo.

Já como ataques de senha temos o força bruta, dicionário e *rainbow tables*, onde o objetivo do invasor é conseguir a senha de acesso ao dispositivo ou sistema. Dentre os ataques contra o *peopleware* se destaca a engenharia social, onde o atacante busca extrair informações utilizando o fator humano.

Estas formas de invasão acabam sendo mais preocupantes dentro do cenário da indústria 4.0 e dispositivos IoT devido a grande quantidade de dispositivos (muitas vezes iguais) instalados na organização. Se um dispositivo da rede possuir uma falha descoberta por um invasor, ele pode utilizá-la para infectar todos os outros dispositivos iguais da rede e neste cenário os ataques ativos e passivos ganham um impacto muito maior, por isso é importante pensar na segurança da informação na utilização de dispositivos IoT.

4.2 TESTES PRÁTICOS

O sistema operacional Contiki possibilita a simulação de redes de dispositivos IoT, desde redes simples a complexas, com dezenas de nós diferentes interagindo entre si. O próprio Cooja já possui diversos *motes*, ou nós, diferentes para compilarmos e usarmos. Porém existem variados tipos de complementos, desde nós a funcionalidades na própria ferramenta, desenvolvidos pela comunidade que podem ser utilizados.

Nesta pesquisa foram utilizados alguns nós complementares para realizar as simulações de ataques, pois foram desenvolvidos para efetuar somente determinadas ações. A utilização de nós programados especificamente para realizar uma ação, como por exemplo executar um ataque DoS, se faz vantajosa pois são otimizados para este fim e não necessitam de configurações ou modificações adicionais.
Portanto, para as simulações serão utilizados os seguintes elementos:

- Nós de tipo *udp-sender* (simulando os sensores) representados pela cor verde;
- Nós do tipo *udp-sink* (simulando o nó raiz, que recebe os dados) representados pela cor amarela;
- Nós do tipo *udp-sender-flooding_attack* (simulando sensores) representados pela cor roxa, sendo estes os nós maliciosos.

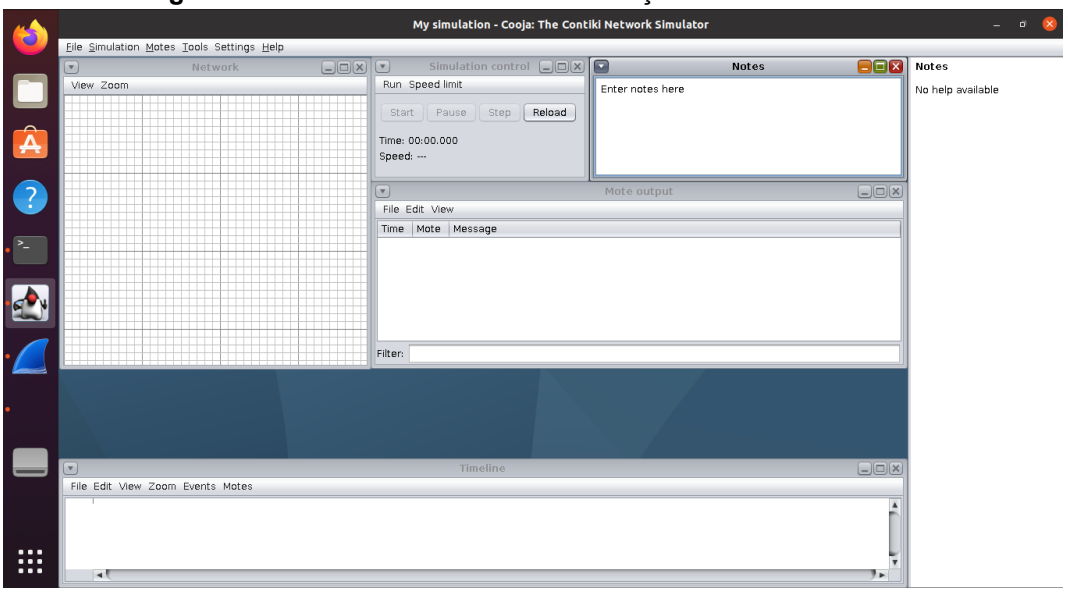
4.2.1 AMBIENTE DOS TESTES

Para a produção dos testes práticos, foi realizada a instalação de uma máquina virtual Linux Ubuntu (versão 20.04.2.0 LTS, disponível no site oficial https://ubuntu.com/download/desktop) através do aplicativo VirtualBox, em uma máquina virtual configurada com 4 gigabytes de memória (para uma melhor performance da simulação, é aconselhado que seja configurado mais gigabytes para a máquina virtual).

Dentro do sistema Linux, o ContikiOS foi instalado através do site oficial do software (https://www.contiki-ng.org/). Além disso, para as simulações de ataques, foram utilizados os *motes*, ou nós (que representam os dispositivos IoT dentro do Cooja) do

IoTrain-Sim (*IoT Training System Using the Cooja Network Simulator*), disponibilizado na página GitHub do CROND (*Cyber Range Organization and Design*) (https://github.com/crond-jaist/iotrain-sim). Na figura 6 podemos observar a tela inicial de uma nova simulação no *Software* Contiki.

Figura 6 - Tela inicial de uma nova simulação no *Software* Contiki



Fonte: Software Contiki

4.2.1.1 Construindo o ambiente de testes

Para construir o ambiente de testes, em um sistema operacional (SO) Linux (nesta pesquisa foi utilizado o SO Ubuntu 20.04.2.0 LTS), primeiramente foi executado o comando abaixo, para baixar o Contiki OS para a máquina virtual:

- *wget https://github.com/contiki-os/contiki/archive/3.0.zip*

A seguir, para extrair o arquivo baixado foi executado o comando abaixo, onde "/DiretorioDestino" se refere ao local onde o arquivo é extraído:

- *unzip 3.0.zip -d /DiretorioDestino*

Para que o Contiki e o Cooja sejam executados corretamente, foi necessário instalar os seguintes pacotes adicionais, cuja instalação foi realizada pelo comando abaixo:

- *sudo apt-get install build-essential binutils-msp430 gcc-msp430 msp430-libc msp430mcu mspdebug gcc-arm-none-eabi gdb-arm-none-eabi openjdk-8-jdk openjdk-8-jre ant libncurses5-dev lib32ncurses5*

A seguir, foi necessário acessar o diretório onde o arquivo compactado do Contiki foi extraído com o comando abaixo:

- *cd ~/contiki-3.0/tools/cooja*

E por último, para compilar e inicializar o simulador Cooja, foi executado o comando abaixo, dentro da pasta Cooja, presente no caminho “/contiki-3.0/tools/cooja”:

- *ant run*

Com isso, a tela inicial do Cooja é apresentada em tela. Em relação ao IoTrain-Sim foram utilizados somente os nós presentes na pasta do arquivo, portanto não foram realizadas instalações adicionais para o seu uso. Neste caso, foi efetuado somente o *download* do arquivo compactado de seu site oficial, extraído com o mesmo comando utilizado para o contiki e seus *motes* foram abertos pelo Cooja instalado anteriormente.

4.2.1.2 Simulação de ataques a dispositivos IoT

Após a instalação do ambiente, foram executados três testes principais. O primeiro foi feito simulando uma rede simples, onde foram adicionados 10 nós do tipo *udp-sender* (que agem como sensores normais, enviando dados para a rede) e 1 nó do tipo *udp-sink* (que age como o roteador) e posteriormente um node do tipo

udp-sender-flooding_attack, que será a representação de um dispositivo malicioso, para demonstrar o alcance de conectividade entre os nós e as suas relações.

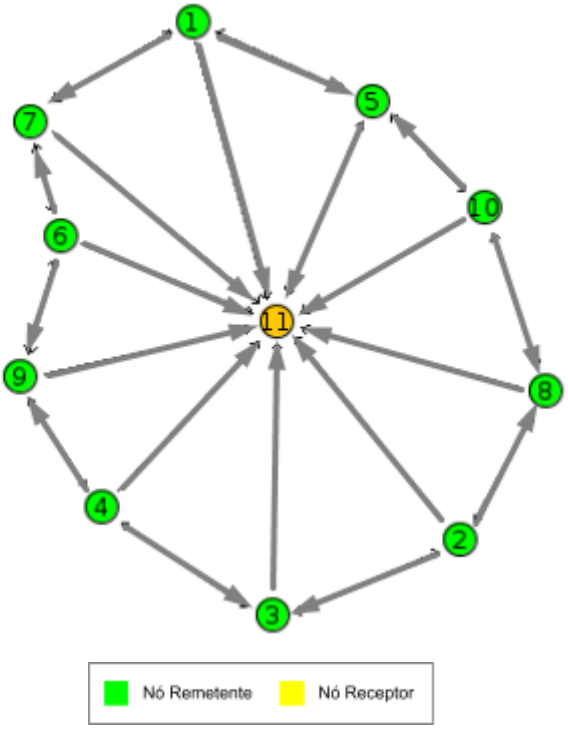
A segunda simulação foi de um ataque DoS, onde o nó malicioso realiza uma inundação de requisições (*Flooding Attack*) para os demais dispositivos. Para isso foram utilizados os mesmos nós da simulação anterior e foram apresentados os dados obtidos através do Cooja referentes ao consumo de energia dos nós, em uma rede sem o nó malicioso e outra com o mesmo, para exibir o impacto do nó malicioso na rede.

A terceira simulação foi realizada com uma rede mais simples, com 2 nós do tipo *example-broadcast* e 1 nó do tipo *example-collect*, ambos os nós são da pasta *Rime* de exemplos do Cooja, que trazem alguns nós para simulação de transmissão de dados. Nesta rede foi feita a coleta dos dados que trafegam pela rede através da funcionalidade *Radio Messages* do Cooja. O arquivo gerado com os dados foi aberto no Wireshark para análise, desta forma demonstrando como uma pessoa mal intencionada, após ganhar acesso a rede, consegue visualizar os dados trafegados por ela (*Sniffing*).

4.2.2 SIMULAÇÃO DE UMA REDE SIMPLES

Nesta rede inicial serão dispostos 10 nós sensores e 1 nó raiz, sem a presença de um nó malicioso. Os nós se comunicam com todos os outros nós ao seu alcance, como mostrado na figura 7.

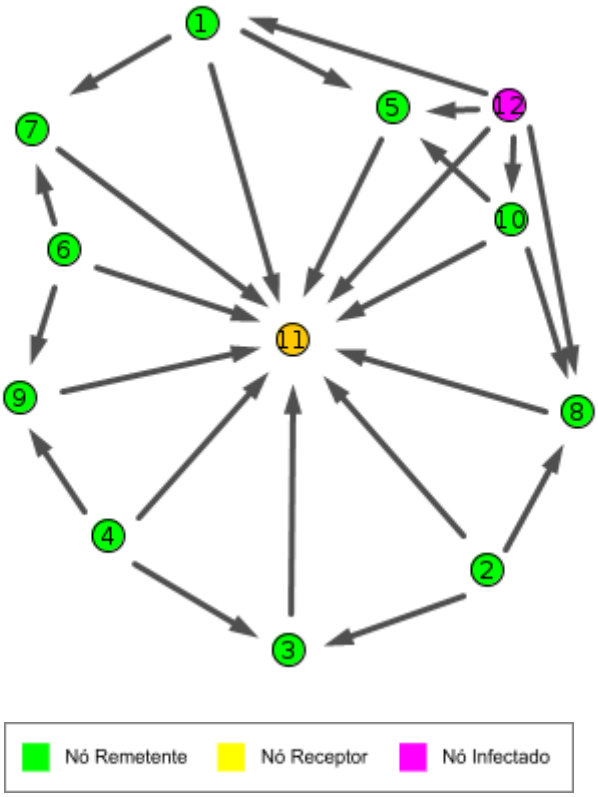
Figura 7 - Topologia com 10 nós sensores IoT sem nó malicioso



Fonte: Adaptado do Software Contiki

A seguir, adicionamos um nó malicioso, que representa a simulação de um ataque bem sucedido, na mesma topologia, desta forma totalizando 12 nós, como mostrado na figura 8. O nó malicioso detém em seu alcance os nós 1, 5, 10, 8 e o nó raiz.

Figura 8 - Topologia com 10 nós sensores com nó malicioso



Fonte: Adaptado do Software Contiki

Nesta representação, simulamos uma rede onde um dispositivo atacante é introduzido no cenário. O dispositivo malicioso está na “beirada” da rede, tendo em seu alcance somente alguns dos dispositivos presentes nela. Em um paralelo com um cenário real, podemos imaginar uma linha de produção com diversos dispositivos IoT, onde um dos dispositivos tenha sido invadido por um indivíduo mal intencionado.

4.2.3 SIMULAÇÃO DE ATAQUE DDOS (*FLOODING ATTACK*)

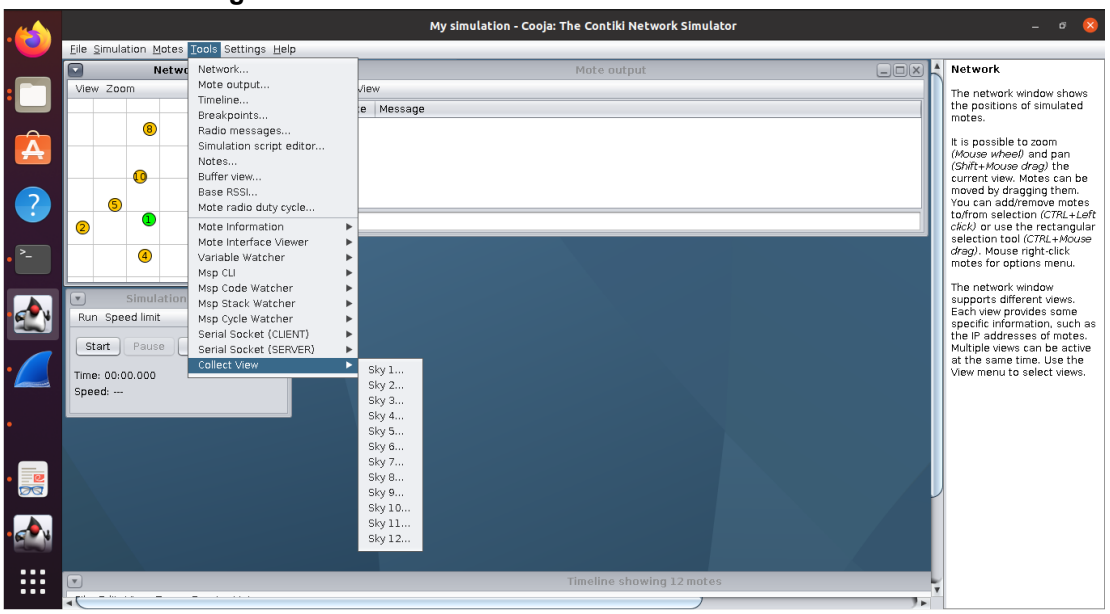
Para simularmos uma rede de dispositivos IoT sofrendo um ataque do tipo DDoS, foi utilizada a rede com o nó malicioso mostrada anteriormente, onde o nó irá realizar uma inundação de requisições (Flooding Attack) para os demais dispositivos.

Este nó malicioso foi desenvolvido para este propósito, onde intencionalmente dispara diversas requisições aos nós em seu alcance. Para que possamos ver o impacto

do ataque na rede e nos dispositivos, podemos observar os gráficos de informações coletadas nos nós sobre seu consumo de energia.

Para realizarmos a coleta dos dados dos nós em uma simulação no Cooja basta ir no menu “*Tools*”, submenu “*Collect View*” e clicar sobre um dos nós apresentados, como mostrado na figura 9.

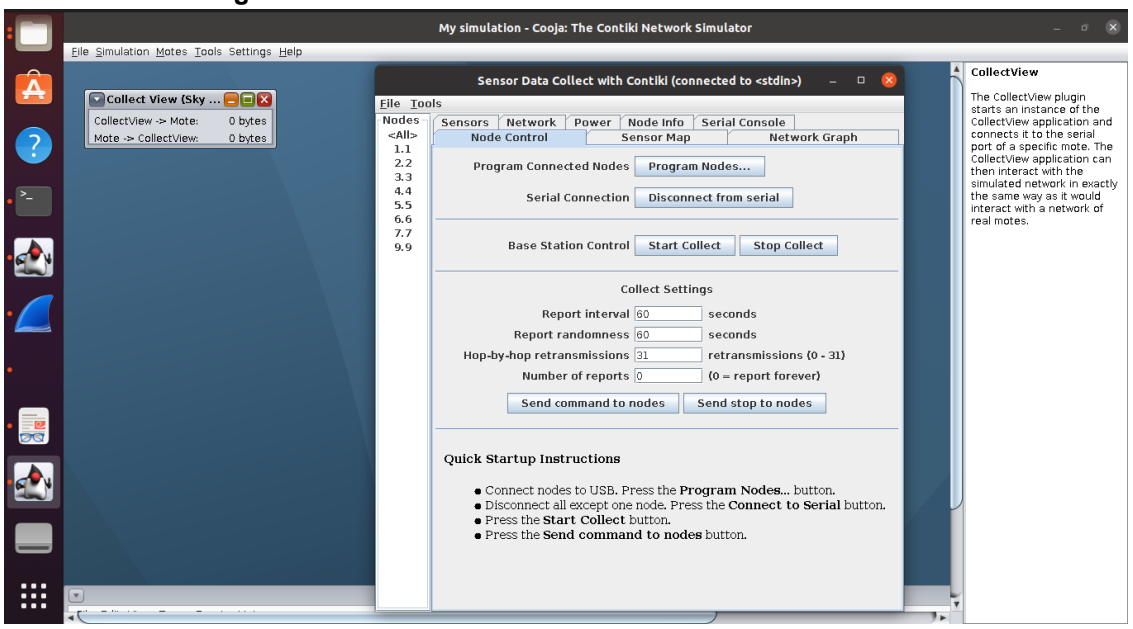
Figura 9 - Tela do menu “*Collect View*” no Software Contiki



Fonte: Software Contiki

Uma pequena janela mostrando os dados coletados irá ser apresentada e após alguns segundos, uma nova janela de controle irá abrir. Nesta janela basta clicar em “*Start Collect*” e depois em “*Send command to nodes*” para que o sistema colete os dados de todos os nós, como mostrado na figura 10.

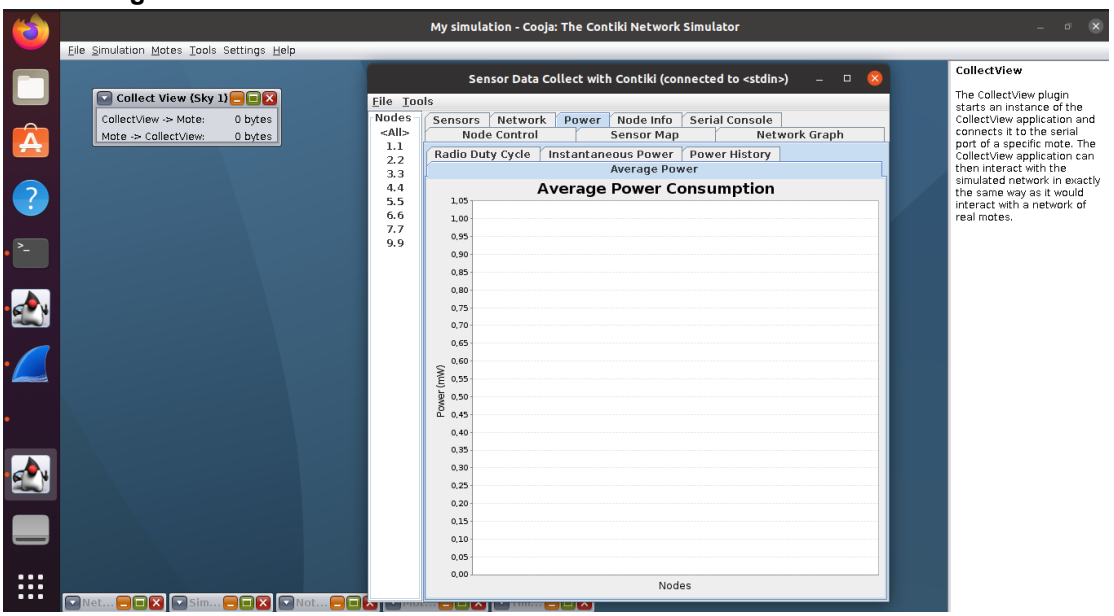
Figura 10 - Tela do menu "*Collect View*" no Software Contiki



Fonte: Software Contiki

Após mandar o comando para que o sistema colete os dados, deve-se clicar em "*Start*" no menu de controle da simulação para que a simulação se inicie. Após alguns minutos de tempo de simulação, os resultados já podem ser consultados na tela de "controle e coleta de dados" aberta anteriormente, na aba "*Power*", no formato de gráficos como mostrado na figura 11.

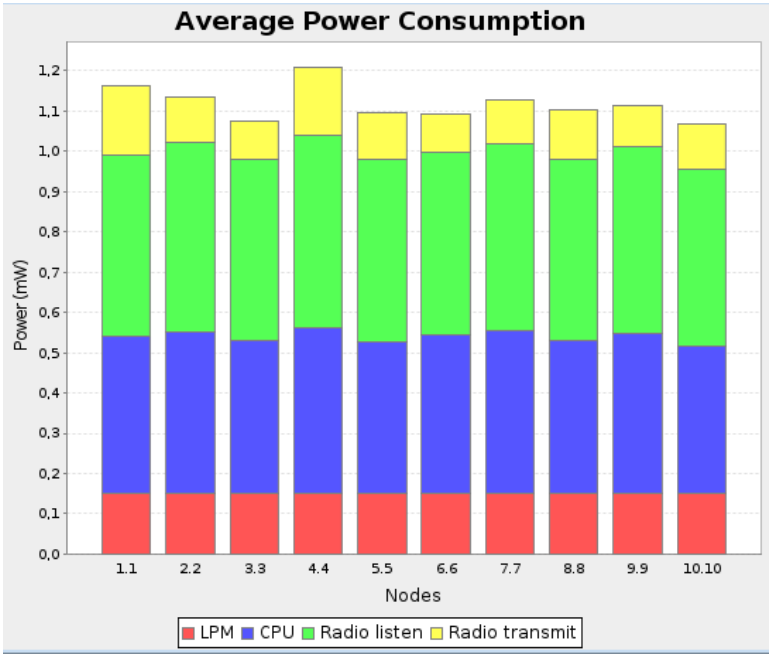
Figura 11 - Tela da aba "*Power*" do menu "*Collect View*" no Software Contiki



Fonte: Software Contiki

No gráfico 3 é possível visualizar o consumo de energia dos dispositivos na rede sem o nó malicioso:

Gráfico 3 - Média de consumo de energia por nó em uma simulação de situação normal de uso de uma rede IoT

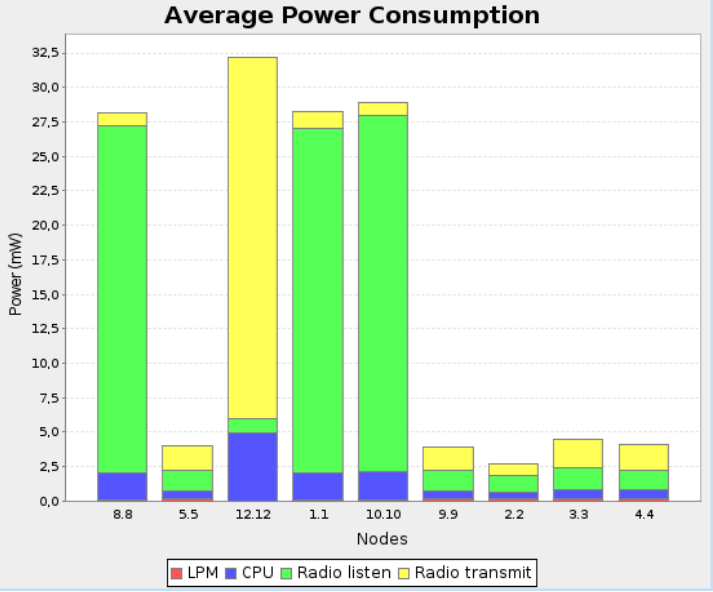


Fonte: Software Contiki

Neste primeiro gráfico, pode-se observar que o consumo médio de todos os nós na rede varia entre 1.1 e 1.2 miliwatts no total. Para estes resultados, a simulação foi executada durante 2 minutos de tempo de simulação.

A seguir pode-se ver no gráfico 4 o consumo de energia dos dispositivos em uma rede afetada pelo ataque do nó malicioso:

Gráfico 4 - Média de consumo de energia com nó malicioso em uma simulação de uso de uma rede IoT



Fonte: Software Contiki

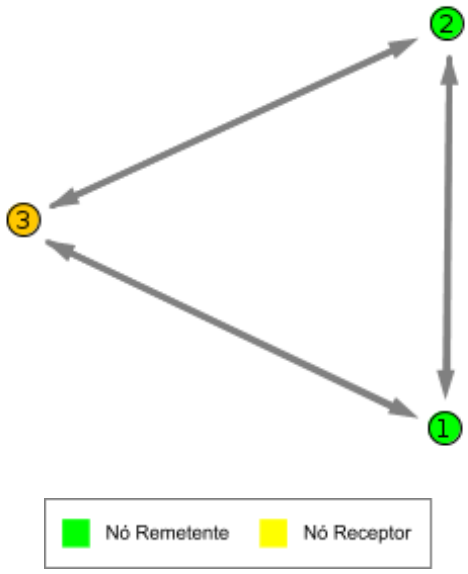
No segundo cenário, o consumo de energia dos nós em seu raio de alcance aumenta drasticamente, passando para uma média que varia entre 28 e 32 miliwatts. Para os nós 8, 1 e 10, o consumo aumentou cerca de 2566%. Para estes resultados, a simulação foi executada novamente durante 2 minutos de tempo de simulação.

Nesta rede básica, com somente 10 nós e um nó atacante, tivemos um aumento considerável no consumo de energia dos dispositivos. Em redes organizacionais com dezenas de dispositivos que podem ser alvo de outros inúmeros dispositivos invadidos, o potencial impacto é significativo.

4.2.4 SIMULAÇÃO DE SNIFFING

Para simularmos um ataque de *Sniffing* em uma rede IoT foi utilizada a seguinte topologia, mais simples que as anteriores, para que possamos ver os dados trafegados pela rede (figura 12).

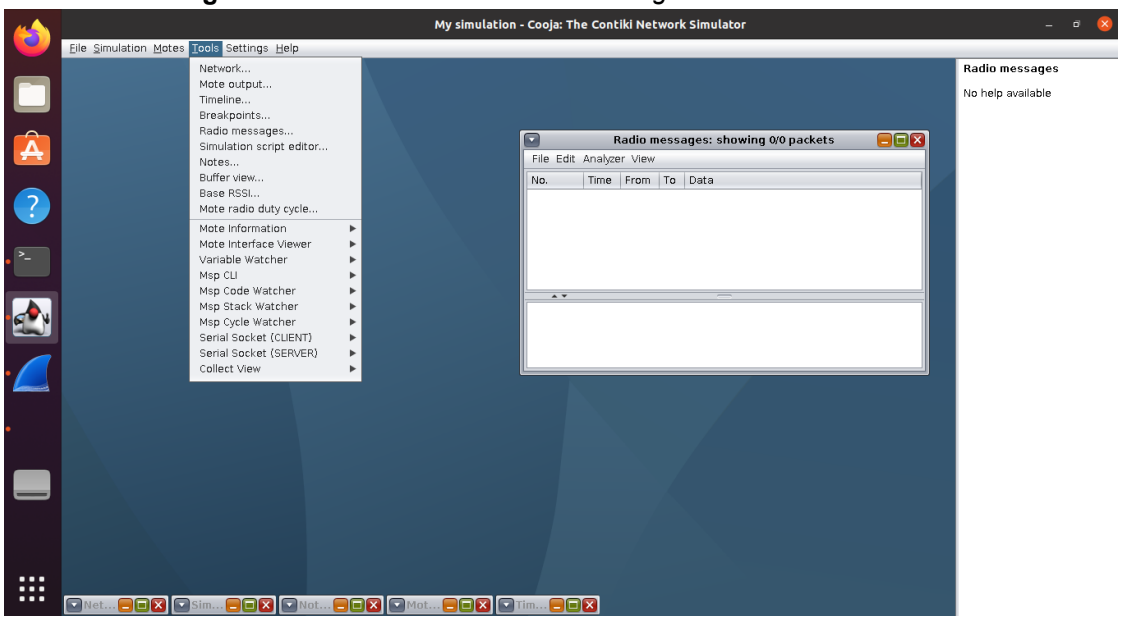
Figura 12 - Topologia da rede simulada para teste de *Sniffing*



Fonte: Adaptado do Software Contiki

Para realizarmos a captura dos dados trafegados, assim como o atacante faria em um ataque real, utilizamos a ferramenta do Cooja chamada de "*Radio Messages*", disponível no menu "*Tools*". Na tela da funcionalidade "*Radio Messages*", selecionamos a opção do menu "*Analyzer*" como "*6LoWPAN Analyzer with PCAP*" e iniciamos a simulação, como mostrado na figura 13.

Figura 13 - Tela do menu "*Radio Messages*" no Software Contiki

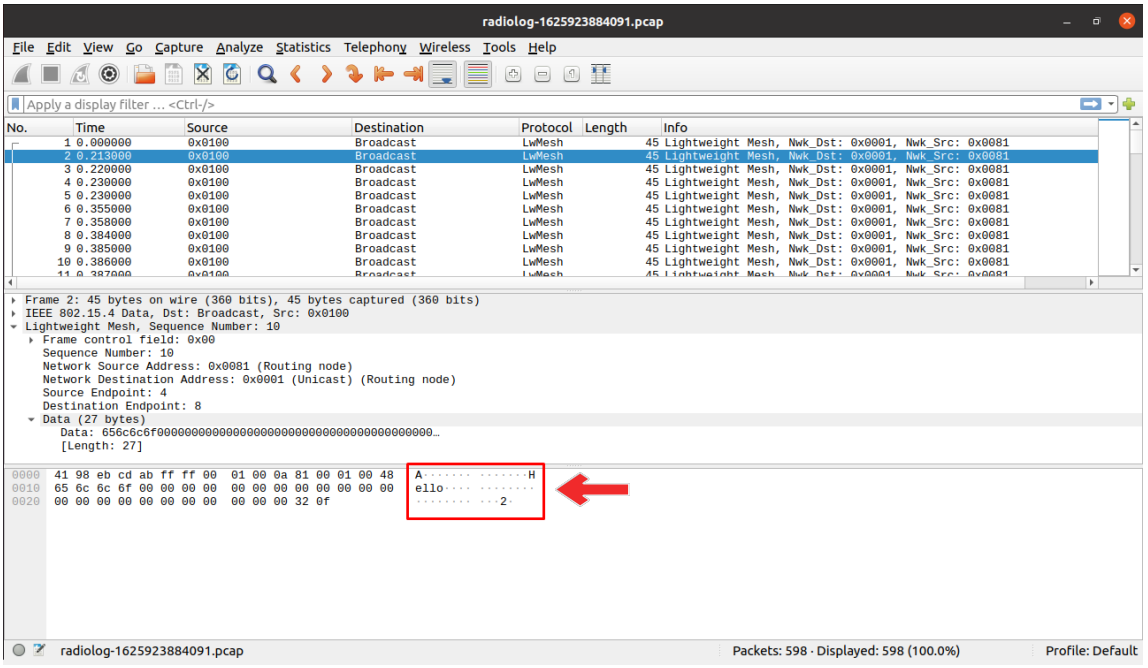


Fonte: Software Contiki

Após alguns segundos de simulação executada, um arquivo será gerado no diretório "/contiki/tools/cooja/build" com título como padrão "radiolog-[código].pcap" que pode ser aberto no software Wireshark para que a análise possa ser realizada.

Uma vez aberto no software Wireshark, é apresentado a visualização dos pacotes trafegados pela rede. A mensagem em texto que um nó enviou para outro é apresentada na Figura 14 na cor vermelha.

Figura 14 - Arquivo .PCAP aberto no software Wireshark com mensagem transmitida entre nós

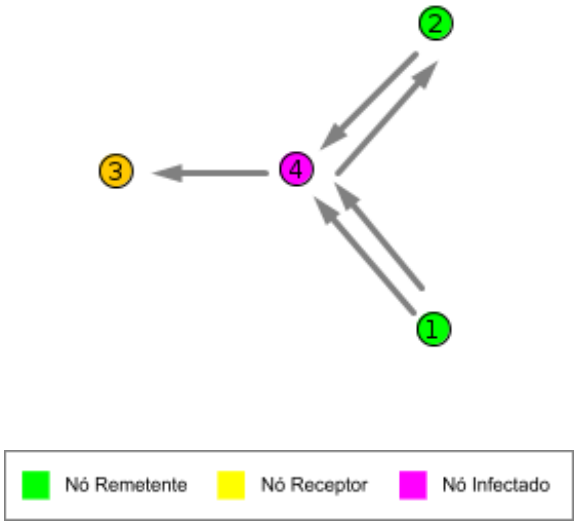


Fonte: Adaptado do Software Wireshark

Como resultado, fica demonstrado que, em uma rede sem proteções como a realizada na simulação, os dados são transmitidos sem segurança. Nesse cenário, se um atacante conseguisse acesso à rede, ele teria todas as informações que os dispositivos em seu alcance estão transmitindo entre si ou para a rede. Além disso, o atacante sabe exatamente qual dispositivo está enviando aqueles dados e qual o destinatário.

Em um cenário de uma rede sofrendo um ataque do tipo *man-in-the-middle*, o atacante se posiciona como o intermediador dos pacotes, tendo acesso a tudo que está sendo trafegado naquele ponto. Na topologia mostrada na figura 15, o atacante (representado pelo nó 4, de cor roxa) tem acesso a todos os dados que os nós 1 e 2 trocam entre si e que enviam para o nó 3.

Figura 15 - Topologia de uma rede sofrendo um ataque do tipo *man-in-the-middle*



Fonte: Adaptado do Software Wireshark

Neste cenário de ataque *man-in-the-middle*, o impacto seria semelhante ao ataque de *Sniffing*, pois o atacante das duas formas consegue capturar os pacotes sendo transmitidos pela rede.

Quando aplicamos proteções na transmissão dos dados, mesmo que o atacante tenha acesso à rede, ele não terá acesso direto às informações que estão sendo transmitidas. Mesmo após conseguir os dados trafegados, ele ainda teria mais uma etapa para ter acesso, como quando aplicamos criptografia aos dados, por exemplo.

4.3 TÉCNICAS PARA MITIGAR RISCOS

Quando pensamos na segurança da informação em uma rede com centenas de dispositivos e usuários, existem diversos pontos que precisam de atenção constante. Com a intenção de mitigar os riscos em torno de toda a estrutura dos dispositivos IoTs, olhando para o hardware, software e peopleware, temos, em especial, as seguintes técnicas que podem ser implementadas.

4.3.1 SOLUÇÕES PARA EVITAR RISCOS DE ATAQUES PASSIVOS

Os ataques passivos tem como intuito obter informações que estão sendo transmitidas pela rede e são difíceis de detectar pois não realizam alterações de dados. Neste cenário, as técnicas para mitigar riscos dos ataques passivos e ativos acabam se complementando, onde atuam para proteção em ambos os ataques. Contudo, focando em ataques passivos, podemos usar a seguinte técnica para mitigar os riscos do atacante obter os dados e proteger o tráfego da rede.

4.3.1.1 Criptografia

Em um ambiente em que a indústria utiliza diversos dispositivos IoT em sua linha de produção, é estabelecida uma rede de alta comunicação, com dados sendo transmitidos a todo o momento e se não protegermos os dados que trafegam nela, ela estará suscetível a diversos ataques. Pessoas mal intencionadas podem se utilizar de ataques do tipo *man-in-the-middle* ou *sniffing* para “ouvir” o que está sendo transmitido na rede e se estes dados não estiverem protegidos, o atacante conseguirá entendê-los e até mesmo modificá-los mais facilmente.

Para que estes dados não sejam transmitidos diretamente pela rede (seja na rede interna da organização ou até chegar na nuvem), podemos utilizar a criptografia para os proteger, desta forma “embaralhando” o conteúdo da mensagem para que mesmo que o atacante consiga acesso aos dados, ele não conseguirá entendê-los facilmente.

Uma mensagem criptografada só poderá ser compreendida facilmente pelo seu receptor. O atacante que possuir acesso à mensagem terá que despender recursos computacionais para quebrar a criptografia, o que dependendo do algoritmo utilizado pode não compensar, levando em conta a criticidade ou valor dos dados da mensagem original.

Em relação ao seu tipo, a utilização do algoritmo de tipo simétrico ou assimétrico pode variar. A escolha pode ser influenciada pelos dispositivos presentes na rede, já que a capacidade de processamento deles pode influenciar na escolha, assim como o grau de sigilo dos dados trafegados pela rede, que podem exigir uma proteção mais robusta.

4.3.2 SOLUÇÕES PARA EVITAR RISCOS DE ATAQUES ATIVOS

Os ataques ativos tem como intuito alterar dados, criar dados falsificados ou até mesmo negação de serviços e são difíceis de ser prevenidos. Porém, podemos utilizar as seguintes técnicas para reduzir os riscos vindos deste tipo de ataque.

4.3.2.1 Detecção de tráfego normal e anormal

Uma técnica para mitigar os riscos em relação aos ataques de SI é a detecção de tráfego normal e anormal usando Sistemas de Detecção de Intrusão em Redes de Computadores (NIDS, *Network Intrusion Detection System* ou *IDS - Intrusion Detection System*).

Estes programas processam dados coletados da própria rede da organização para gerar informações e gráficos acerca dela. Estes dados processados se baseiam nas mensagens (pacotes) trocados entre os dispositivos da rede, sendo que este tráfego pode ser classificado de duas formas:

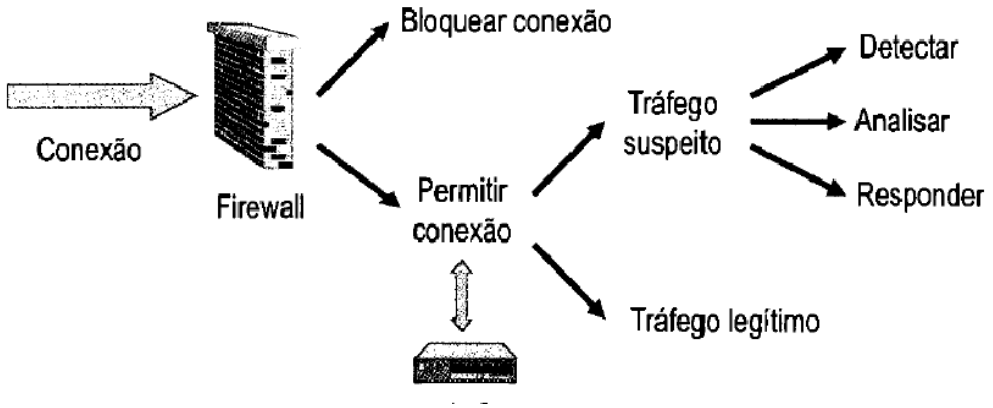
- Normal: Formado pelo tráfego legítimo da rede;
- Anômalo: Tráfego com anomalias e possíveis ataques, como interrupções nas trocas de pacotes na rede.

Os IDS (Sistemas de Detecção de Intrusão) são divididos em dois tipos, os baseados em Host (HIDS – *Host Based Intrusion Detection System*) e baseados em Rede (NIDS - *Network-Based Intrusion Detection System*).

Os Sistemas de Detecção de Intrusão baseados em Host atuam nos dispositivos em si, detectando acessos e alterações em arquivos importantes, alterações em privilégios, processos do sistema, programas que estão sendo rodados entre outros.

Já os Sistemas de Detecção de Intrusão baseados em Rede atuam no monitoramento do tráfego da rede utilizando os cabeçalhos e conteúdos dos pacotes para a análise, os comparando com padrões e assinaturas conhecidas.

Figura 16 - Funcionamento dos NIDS



Fonte: Nakamura, 2007

Na figura 16 temos o funcionamento de um Sistemas de Detecção de Intrusão em Redes de Computadores, onde após o *firewall* permitir uma conexão, temos o NIDS coletando e analisando o tráfego e classificando-o como legítimo ou suspeito. Utilizando os IDS é possível identificar ataques ativos e detectar alterações realizadas pelos atacantes baseado na análise de tráfego anômalo.

4.3.2.2 Firewall

O *firewall* é outra técnica que pode ser aplicada para combater ataques ativos e passivos, atuando como um “filtro” na rede, ajudando a proteger e controlar o fluxo de dados entre redes, auxiliando na defesa de acessos não autorizados.

O *firewall* pode ser implementado de duas formas, por *hardware* ou *software*, onde o equipamento físico (*hardware*) é mais utilizado para gerenciar múltiplos dispositivos, sendo mais robusto. Já o *software firewall* é mais utilizado diretamente em dispositivos específicos, sendo mais simples. A escolha entre as duas opções pode variar, levando em conta fatores como o número de dispositivos e tamanho da rede, o nível de segurança desejado ou o que exatamente está sendo protegido.

Portanto, ao possuir um firewall adequado ao cenário da organização, bem aplicado e configurado é possível aumentar o nível de segurança do ambiente. Porém, assim como qualquer outro dispositivo ou sistema, vulnerabilidades podem ser descobertas com o decorrer do tempo, desse modo o cuidado com as atualizações de

firewall deve ser constante.

4.3.3 SOLUÇÕES PARA EVITAR RISCOS DE ATAQUES DE SENHA

Em um ambiente corporativo, mesmo protegendo os dispositivos e a rede da empresa, ainda estamos suscetíveis a possíveis invasões. Pessoas mal intencionadas podem usar técnicas de engenharia social ou mesmo ataques como o força bruta, dicionário ou rainbow tables (descritas no capítulo 2 desta pesquisa) para conseguir acesso às senhas de usuários e dispositivos.

Se utilizando da senha obtida de um usuário, por exemplo, o atacante já possui acesso à rede da empresa e a partir deste ponto, pode utilizar outras técnicas, como o *sniffing*, para adquirir dados trafegados pela rede. Para diminuirmos os riscos referentes às senhas, algumas técnicas podem ser utilizadas.

4.3.3.1 Senhas fortes

Para a Segurança da Informação no contexto de senhas, a utilização de sequências de números, palavras comuns e até mesmo dados pessoais como datas de nascimento, casamento, números de documentos, nomes de pessoas e pets como senhas de acesso acabam gerando um risco. A utilização de dados como estes para compor a senha acaba tornando a senha de fácil adivinhação e passíveis de ataques de engenharia social. Senhas como as mostradas a seguir não devem ser utilizadas, pois são demasiadamente simples:

- 123456
- 123123
- password
- senha
- hello
- qwert

Além disso, utilizar a mesma senha em diversos dispositivos ou sistemas

acaba criando outra brecha na Segurança da Informação, pois se um dispositivo for atacado e invadido, o atacante pode conseguir acesso aos demais, pois a senha dos outros dispositivos é igual à anterior.

Ao pensar em senhas fortes, a melhor forma de planejar uma senha é combinando letras, números e caracteres especiais, como as pontuações como o ponto de exclamação ou interrogação, símbolos como o arroba (@), “E” comercial (&) ou cifrão ($), além disso, é importante que a senha tenha um número razoável de caracteres.

Ao utilizar uma senha forte, atacantes buscando adquirir a senha terão uma dificuldade maior em obtê-la ao realizar ataques de engenharia social, pois a senha não possui nenhuma informação diretamente ligada ao seu dono. Ou mesmo ataques de quebra de senha como o de força bruta, *rainbow table* ou de dicionário, pois a senha possui mais caracteres, pouca ou nenhuma sequência, além da complexidade da mescla entre números, letras e caracteres especiais.

4.3.3.2 Autenticação de 2 fatores

Quando utilizamos somente uma validação para acessar dispositivos ou sistemas da organização, podemos ficar vulneráveis a pessoas mal intencionadas que possuam alguma senha de acesso. Para reforçar esta segurança podemos utilizar a autenticação de dois fatores, onde além da senha de acesso o colaborador ou sistema terá que possuir um segundo validador.

Ao utilizarmos um segundo fator de autenticação, aumentamos a segurança de acesso, pois além do atacante ter que descobrir a senha, terá de saber qual é o segundo fator e como adquiri-lo.

Um grande exemplo da utilização da autenticação de dois fatores é em contas de e-mail, onde além de inserirmos o usuário e senha podemos cadastrar a chamada “Verificação em duas etapas” onde podemos receber um código enviado por SMS ou de aplicativos que geram uma chave eletrônica (*token*) que é atualizada de tempos em tempos e até mesmo leitura de biometria.

4.3.3.3 One time password

Outra forma de mitigarmos os riscos quando falamos em senhas de acesso é a chamada *one time password*, que se baseia no conceito de senhas descartáveis. Este modo de acesso utiliza uma senha que perde a validade após uma autenticação, fazendo com que o usuário utilize senhas diferentes em cada acesso. Realizar a autenticação desta forma impede técnicas de obtenção de senhas, como as descritas no capítulo 2 desta pesquisa, pois mesmo que o atacante obtenha a senha, ela já terá perdido a validade e desta forma se tornará inútil para ele.

As senhas descartáveis utilizam tecnologias de *software* e *hardware* para serem geradas. Nos *hardwares*, temos os tokens e smartcards como os agentes físicos que geram as senhas. Já dentre os *softwares*, temos diversos aplicativos que utilizam o mesmo conceito, como já citados no tópico anterior (Autenticação de 2 fatores). Em ambos os casos, as senhas são geradas automaticamente e tem validade por alguns segundos, quando são substituídas por uma nova senha.

4.3.4 SOLUÇÕES PARA EVITAR RISCOS DE ATAQUES DE PEOPLEWARE

Quando pensamos em segurança da informação, não podemos só nos preocupar com os dispositivos em si como alvos para pessoas mal intencionadas, mas sim em tudo que os rodeia. Os colaboradores da empresa que interagem com os dispositivos protegidos, podem acabar se tornando alvos de ataques de Engenharia Social e o invasor pode conseguir acesso a senhas, arquivos ou informações privadas sem precisar necessariamente ganhar acesso à rede da empresa.

Por isso, é aconselhável dar a devida atenção aos treinamentos dos colaboradores da empresa, os ensinando sobre quais informações devem ser protegidas e como protegê-las, para que desta forma, consigam identificar situações de alto risco, como um ataque de Engenharia Social.

4.3.4.1 Política de segurança da informação

No dia a dia dos colaboradores de uma empresa, os funcionários podem se deparar com situações onde necessitam consultar e manipular informações potencialmente sigilosas. Nestas ocasiões, é importante que o colaborador saiba o que ele pode ou não fazer com as informações sensíveis.

Por isso, elaborar e aplicar corretamente uma Política de Segurança da Informação (PSI) é importante. Com ela os colaboradores (independentemente de seus níveis técnicos) possuem de forma bem definida as orientações de comportamento para combater possíveis ameaças à Segurança da Informação.

Através do PSI são definidas orientações quanto ao uso dos recursos de TI, com suas atividades permitidas e não permitidas, recomendações referentes à controles de acesso, utilização de *softwares* corporativos ou terceiros, além de normas sobre a manipulação de informações.

4.3.4.1 Programas de treinamento e Conscientização

Além do PSI, uma outra solução importante para a proteção contra ataques peopleware e para a segurança da informação como um todo são os programas de treinamento e conscientização. Possuir as políticas somente em forma escrita na organização não basta para que os colaboradores se sintam engajados a cumprí-las, eles devem se sentir comprometidos com o tema, para que em momentos onde exista desconfiança, possam analisar corretamente a situação e fazer o certo. Para isso, assim como no PSI, os colaboradores devem ver o exemplo vindo de cima em relação ao programa de treinamento, com a direção comprometida e engajada.

O programa de treinamento deve chegar a todos os funcionários que tiverem acesso à informações sigilosas ou aos sistemas corporativos, sendo pensado e realizado de forma específica para cada tipo de grupo na empresa. Os treinamentos da equipe de TI vão ser diferentes dos treinamentos de equipes não técnicas, como assistentes administrativos por exemplo. Além disso, o programa deve ser dinâmico, pois assim como a tecnologia avança constantemente, e em decorrência disso novas ameaças e

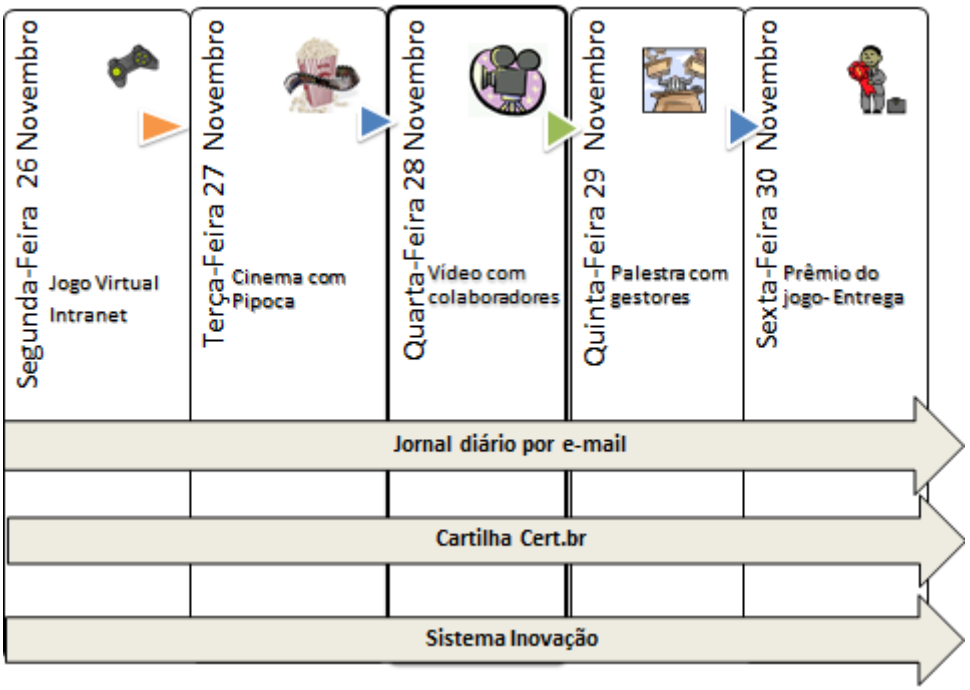
vulnerabilidades surgem, os programas de treinamento devem ser revisados sempre que necessário, para atualizar os colaboradores sobre essas novas ameaças e possíveis vulnerabilidades.

> Após a sessão de treinamento inicial, sessões mais longas devem ser criadas para educar os empregados sobre as vulnerabilidades específicas e técnicas de ataque relativas à sua posição na empresa. Pelo menos uma vez por ano é preciso fazer um treinamento de renovação. A natureza da ameaça e os métodos usados para explorar as pessoas estão sempre mudando, de modo que o conteúdo do programa deve ser mantido atualizado. Além disso, a consciência e o preparo das pessoas diminui com o tempo, de modo que o treinamento deve se repetir a intervalos razoáveis de tempo para reforçar os princípios da segurança. (FONSECA, 2009)

Ao observarmos a campanha de conscientização de SI de uma grande empresa do ramo elétrico (SANTOS, R., SANTOS, M., CARREIRA, 2016), implementada pela primeira vez na organização, podemos constatar que ela foi desenvolvida sob três diretrizes: A empresa deve garantir que a política e suas normas sejam amplamente divulgadas aos colaboradores; quaisquer alterações devem ser devidamente comunicadas aos colaboradores; A empresa tem que possuir um Plano Anual de Conscientização em Segurança da Informação objetivando a capacitação e disseminação da cultura de SI aos colaboradores.

O programa de treinamento em questão foi pensado em um formato de Semana de Conscientização de SI, onde as ações durante o cronograma foram pensadas tendo como foco seu principal público-alvo, porém eram abertas a todos os colaboradores da empresa.

Figura 17 - Cronograma da Semana de Conscientização de SI



Fonte: Santos, R., Santos, M., Carreira, 2016, p. 9

A Semana de Conscientização de SI foi iniciada com o jogo virtual on-line na Intranet, tendo como público-alvo o nível operacional, como mostrado na figura 17. Esta atividade é constituída de um jogo com perguntas ligadas a SI e extraídas da Política de Segurança da Informação e das normas específicas da empresa, disponibilizado a todos os colaboradores pela intranet da organização.

A segunda atividade foi composta por uma exibição de filme ligado à Segurança da Informação no auditório da empresa, com distribuição de pipoca e refrigerante, tendo como público-alvo o nível operacional. Antes de cada sessão, o gestor de SI da empresa falava brevemente sobre a importância do cumprimento da política de segurança.

Em seguida, a atividade escolhida foi a de vídeo com os empregados na Intranet, tendo como público-alvo os níveis tático e operacional. Com filmagens realizadas com os próprios colaboradores da empresa, foram criados quatro vídeos retratando as seguintes situações: Bloqueio do computador na ausência da estação de trabalho; Impressão de documentos confidenciais; Conversas em elevadores, corredores, táxis e

locais públicos; Login e senha são pessoais e intransferíveis.

A quarta atividade se constituiu de palestras de conscientização com nomes renomados na área, tendo como público-alvo os níveis estratégico e tático. Nas palestras, foram discutidos temas como riscos digitais, vazamento de informações, direitos autorais, linha do tempo mostrando a evolução das Políticas de SI e alguns ataques ocorridos no Brasil.

Durante toda a semana, ocorreram envios de dicas no jornal diário, encaminhado a todos os colaboradores por meio do e-mail corporativo. Além disso, foram compartilhadas cartilhas de segurança do Cert.br (Grupo de respostas a incidentes de segurança para a internet brasileira, mantido pelo Comitê Gestor da Internet no Brasil. Além do tratamento de incidentes, treinamento e conscientização e análise de tendência de ataque (CERT, 2016)) pela intranet da organização.

Por último, foi desenvolvida uma página chamada de “vitrine de ideias” com o tema de Segurança da Informação, por meio do sistema de gestão de inovação que a empresa possui. Com ele, o colaborador pode cadastrar ideias inovadoras para apoiar a organização em diversos temas, e após a Semana de Conscientização de SI, ela ganhou mais este tópico.

4.4 GUIA DE SEGURANÇA DA INFORMAÇÃO PARA DISPOSITIVOS IOT

Em um ambiente corporativo da Indústria 4.0, utilizando dispositivos IoT em seu meio, uma brecha na segurança da informação pode gerar impactos significativos na rede e em todos os seus serviços. Neste cenário, cuidar da segurança é essencial para manter o bom funcionamento da organização e para isso, algumas técnicas e cuidados podem ser aplicados para que estes riscos possam ser mitigados.

No quadro 2 pode-se observar de forma sintética as principais ameaças no cenário de Indústria 4.0 com dispositivos IoT e as estratégias de prevenção que podem ser aplicadas para mitigar seus riscos.

Quadro 2 - Comparativo entre ameaças e estratégias de prevenção no cenário de dispositivos IoT

Ameaças	Estratégia de prevenção
Ataques Sniffing (Passivo)	Aplicação de criptografia e utilização de Sistemas de Detecção de tráfego normal e anormal (IDS) e *Firewall*.
Ataques *Man-in-the-Middle* (Ativo/Passivo)	Aplicação de criptografia e utilização de Sistemas de Detecção de tráfego normal e anormal (IDS) e *Firewall*.
Ataques DDoS (Ativo)	Utilização de Sistemas de Detecção de tráfego normal e anormal (IDS) e *Firewall*.
Ataques de senha (força bruta, dicionário, *rainbow tables*)	Utilização de senhas fortes, autenticações adicionais (autenticação de 2 fatores), autenticações alternativas (*one time password*).
Ataques de Engenharia Social	Aplicação de uma Política de Segurança da Informação (PSI) e Programas de Treinamento e Conscientização.

Fonte: Elaborado pelo autor

O guia apresentado mostra recomendações de uso/aplicação de técnicas, políticas e cuidados que podem ser aplicados para melhorar a segurança da informação dos dispositivos IoT, para que desta forma, empresas e gestores possam utilizar estes dispositivos IoT com mais segurança. A apresentação do guia se divide em ações distintas a serem aplicadas a dispositivos e pessoas, apresentando recomendações para cada aspecto. O guia é apresentado na forma de um documento, para que possa ser extraído da presente pesquisa, desta forma facilitando sua utilização por empresas e gestores.

INSTITUTO FEDERAL DE SANTA CATARINA - IFSC

CÂMPUS FLORIANÓPOLIS

DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS

CST EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

RODRIGO GRANDO BERLANDA

GUIA DE SEGURANÇA DA INFORMAÇÃO PARA DISPOSITIVOS IOT

FLORIANÓPOLIS – SC

AGOSTO/2021

1. O QUE É O GUIA

Em um ambiente corporativo da Indústria 4.0, utilizando dispositivos IoT em seu meio, uma brecha na segurança da informação pode gerar impactos significativos na rede e em todos os seus serviços. Se um ponto da rede possuir uma falha de segurança da informação, seja ele um dispositivo desprotegido, desatualizado, um colaborador com uma senha fraca ou manuseando informações sigilosas de forma incorreta por exemplo, ele pode ser usado para que o atacante possua acesso a toda a rede da empresa. Desta forma, cuidar da segurança da informação dos dispositivos IoT e de todo o seu entorno se torna essencial para mitigar estes riscos.

O guia apresentado a seguir mostra recomendações de uso/aplicação de técnicas, políticas e cuidados que podem ser aplicados para melhorar a segurança da informação dos dispositivos IoT.

1.1 PÚBLICO ALVO

Este guia de segurança da informação é destinado para empresas, gestores e profissionais da área de segurança que estão adotando ou estão pensando em implementar dispositivos IoT em sua organização, para que a utilização destes dispositivos possa ser realizada com mais segurança.

2. GUIA

A apresentação do guia se divide em ações distintas a serem aplicadas a dispositivos e pessoas, apresentando recomendações para cada aspecto.

2.1 Dispositivos

As recomendações a seguir são direcionadas aos dispositivos (IoT e não IoTs) da organização, sendo referentes aos seus *hardwares* e *softwares*:

2.1.1 Selecione dispositivos IoT projetados pensando em segurança da informação

Selecionando dispositivos que foram construídos pensando em segurança da informação se torna mais simples implementar ações de segurança com suporte via *hardware*. Dispositivos desenvolvidos de forma simples (hardware e software) podem tornar a aplicação de técnicas de segurança no dispositivo uma tarefa difícil, pois os recursos dele podem ser limitados para este propósito.

2.1.2 Mantenha os dispositivos e sistemas da organização atualizados

Manter os dispositivos IoT e não IoT e demais sistemas da organização atualizados em relação a *software* e *firmware* contribui na prevenção contra possíveis vulnerabilidades que venham a ser descobertas pelos fabricantes.

No cenário IoT, onde diversos dispositivos iguais podem ser aplicados na rede, é importante que todos se mantenham atualizados, já que uma vulnerabilidade em um modelo pode afetar inúmeros dispositivos na rede da organização.

2.1.3 Elabore senhas e validações fortes

Elaborar senhas e validações fortes para os dispositivos e sistemas da organização contribui para minimizar os riscos de ataques de senha.

O dispositivo ou sistema ainda terá um grande risco de invasão caso as senhas de acesso dele sejam fracas, mesmo que o dispositivo esteja totalmente protegido de forma lógica, pois invasores podem utilizar ataques de senha para conseguir a senha de acesso. Neste cenário, preze pela utilização de senhas com letras, números e caracteres especiais, não sendo compostas por termos que sejam de fácil adivinhação, como o nome da empresa, nome do sistema ou dispositivo ou mesmo nome/número do modelo, por exemplo.

2.1.4 Utilize *firewalls*

Utilize *firewalls* bem configurados e atualizados, para monitorar e proteger a rede de acessos não autorizados. Os *firewalls* atuam como um “filtro” na rede, ajudando a proteger a rede contra ataques DDoS, por exemplo.

2.1.5 Utilize Sistemas de Detecção de Intrusão (IDSs)

Utilizar os IDS auxilia no monitoramento das atividades de comunicação dos dispositivos e da rede utilizada. Os IDS atuam após o *firewall*, analisando o tráfego da rede e classificando-o como legítimo ou suspeito.

Com a sua utilização é possível identificar ataques ativos e detectar alterações realizadas pelos atacantes baseado na análise de tráfego anômalo, sendo grandes aliados para a segurança da informação.

2.1.6 Monitore os dispositivos IoT

Monitorar os dispositivos IoT é uma etapa importante, com especial atenção aos dispositivos mais expostos, nas “bordas” da rede, avaliando a existência de tráfego de dados anômalo.

Os dispositivos IoT mais expostos estão mais suscetíveis a ataques, portanto é importante que sejam monitorados para que ações sejam tomadas assim que o tráfego anômalo seja detectado, sendo auxiliado pelos IDS.

2.1.7 Aplique algoritmos de criptografia na rede e na transmissão dos dados

Aplicar algoritmos de criptografia na rede e na transmissão dos dados para a nuvem para impedir que dados que trafegam em redes com e sem fio sejam acessados e utilizados de forma indevida. Desta forma, mesmo que o invasor ganhe acesso aos dados sendo trafegados na rede, ele não terá acesso direto aos mesmos, pois estarão criptografados.

2.1.8 Realize testes de penetração (*pentests*)

Realizar testes de penetração nos dispositivos e sistemas regularmente, utilizando diversas técnicas ajudam a avaliar a segurança da rede e identificar possíveis vulnerabilidades para que seja possível aplicar correções e se antecipar a possíveis ataques.

Aplicar técnicas de segurança sem a realização de testes pode abrir brechas na segurança da rede, pois sem os testes não é possível saber se o que foi aplicado é realmente eficaz e se está atualizado com as vulnerabilidades presentes.

2.1.9 Mantenha uma rotina de testes e treinamentos

Manter uma rotina de testes e treinamentos no uso das tecnologias, atualizando e aprimorando os recursos tecnológicos utilizados pela empresa para que brechas não sejam criadas nas tecnologias utilizadas ou no modo de utilização destas soluções pelos colaboradores.

2.2 Pessoas

As recomendações a seguir são direcionadas ao peopleware da organização:

2.2.1 Estabeleça regras sobre a formulação e utilização de senhas

Estabeleça regras sobre a formulação e utilização de senhas por todos os colaboradores da organização, para desta forma evitar que ataques de senhas sejam eficazes e que o invasor consiga acesso à rede.

Mesmo que os dispositivos ou sistemas da rede estejam protegidos, os invasores podem conseguir acesso através da senha de acesso de colaboradores. Neste cenário, preze pela utilização de senhas com letras, números e caracteres especiais, não sendo compostas por termos que sejam de fácil adivinhação, como o nome do funcionário, data de nascimento ou mesmo números de documentos.

2.2.2 Implemente outros meios de autenticação

Implemente outros meios de autenticação, como a autenticação de dois fatores ou *one time password,* fortalecendo o sistema de autenticação de usuários e senhas contra acessos indevidos.

Ao utilizar uma segunda validação como a autenticação de dois fatores ou mesmo uma validação alternativa (*one time password*) a rede fica mais protegida, pois dificulta ainda mais o acesso de invasores, mesmo que utilizem ataques de senha.

2.2.3 Elabore e aplique uma Política de Segurança da Informação (PSI)

Elaborar e aplicar uma Política de Segurança da Informação, formulada com base no cenário da organização, criando regras claras para colaboradores sobre a necessidade de adoção destas políticas de segurança auxilia na proteção da rede pois com o PSI os colaboradores possuem de forma bem definida as

orientações de comportamento para combater possíveis ameaças à Segurança da Informação.

2.2.4 Elabore e aplique programas de treinamento e conscientização

Elaborar e aplicar programas de treinamento e conscientização para os colaboradores da organização auxilia em manter a equipe de colaboradores sempre atualizada e engajada nas ações de segurança da informação.

2.2.5 Realize testes de penetração (*pentests*)

Realize testes de penetração utilizando técnicas de engenharia social para avaliar e validar os programas e políticas aplicados, verificando possíveis vulnerabilidades e não observância das políticas de segurança da informação

Aplicar os programas e políticas sem a realização de testes pode abrir brechas na segurança, pois sem os testes não é possível saber se os programas e políticas aplicadas são realmente eficazes e se estão atualizados com as vulnerabilidades presentes.

3. Conclusão

Com a aplicação das recomendações descritas neste guia é possível diminuir os riscos de segurança da informação provenientes da utilização de dispositivos IoT e da rede como um todo. O guia leva em consideração riscos identificados em relação ao *hardware*, *software* e *peopleware* dos dispositivos IoT e demais sistemas que a organização possa utilizar.

5. CONCLUSÕES

Neste capítulo serão apresentadas as conclusões a respeito do trabalho realizado, bem como algumas sugestões que poderão auxiliar em perspectivas futuras referentes a este assunto ou na mesma área.

A pesquisa investigou a estrutura dos dispositivos IoT voltados à indústria 4.0 e buscou referências sobre os riscos de segurança associados. Ao longo do capítulo 2, foram identificadas as possíveis falhas e pontos que merecem atenção durante a utilização de dispositivos IoT em relação a *hardware*, *software* e *peopleware*. Além disso, abordamos as características e estrutura dos dispositivos IoTs, que revelam a fragilidade destes em relação à segurança da informação. Em sua concepção, eles foram pensados em atender aos requisitos mínimos para o seu funcionamento, justamente para serem compactos e de baixo custo e aplicados em grande quantidade, porém, isso acaba dificultando a aplicação de técnicas de segurança da informação mais robustas para proteção.

Em relação aos principais ataques realizados contra os dispositivos IoTs, podemos verificar que muitos podem explorar a baixa preocupação e a ausência de técnicas de segurança em todas as partes da estrutura, *hardware*, *software* e *peopleware*. Além disso, como observado através da simulação relatada no capítulo 4 desta pesquisa, estes ataques podem ter um grande impacto para a rede e para os serviços por eles controlados na indústria ou em outras aplicações onde sejam utilizados.

5.1. EM RELAÇÃO AO OBJETIVO GERAL

No Brasil o cenário da indústria 4.0 ainda é inicial, porém em grande escala de crescimento. Entretanto, a preocupação com a segurança da informação neste cenário deve aumentar com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) no ano de 2020, onde a proteção dos dados passa a ser uma obrigação legal e os investimentos e as ações de segurança da informação no Brasil devem crescer.

A presente pesquisa teve como objetivo geral o desenvolvimento de um guia

de segurança da informação, com recomendações para empresas e gestores com técnicas, diretrizes e boas práticas para a adoção dos dispositivos IoT na Indústria 4.0. Tendo como base os dados obtidos a partir do referencial bibliográfico e dos testes realizados sobre a utilização dos dispositivos IoT pela indústria, foi possível detectar falhas e riscos que a falta de segurança da informação pode acarretar e identificar soluções que propiciam a melhora na segurança da informação com a utilização das técnicas, diretrizes e boas práticas, concluindo-se que o objetivo geral foi alcançado.

Porém, se as técnicas, orientações e diretrizes descritas no guia foram implementadas e praticadas, o risco tende a baixar consideravelmente, tanto ao dificultar que os invasores consigam acesso aos dispositivos e a rede (de forma física ou lógica), como ao bloquear o entendimento dos dados mesmo que o atacante tenha acesso a eles.

5.2. EM RELAÇÃO AOS OBJETIVOS ESPECÍFICOS

A partir da revisão bibliográfica sobre o tema IoT e indústria 4.0 foi possível observar o funcionamento e requisitos dos dispositivos IoT adotados na Indústria 4.0, levando em conta seu *hardware*, *software* e *peopleware* e temas correlatos, como *cloud computing*.

Os dispositivos IoT tem, em geral, características como seu baixo custo e sua escalabilidade de aplicação (com diversos dispositivos iguais ou parecidos sendo utilizados no mesmo ambiente organizacional), o que deve ser um grande ponto de atenção em relação à segurança da informação. Se uma vulnerabilidade for descoberta em um dispositivo, ela deve ser estudada e a possível correção aplicada a todos os dispositivos iguais na rede. Além disso, técnicas de proteção devem ser aplicadas da melhor maneira possível nos dispositivos IoT com o pouco recurso disponível neles devido às suas características de construção de baixo custo.

Ainda, na revisão bibliográfica sobre o tema IoT e indústria 4.0 foi possível observar os pontos de preocupação e riscos relacionados à arquitetura dos dispositivos IoTs, juntamente com os pontos de atenção referentes às suas aplicações práticas e os locais físicos de instalação e riscos relativos ao *hardware*, *software* e *peopleware*.

Em um ambiente de indústria 4.0 com dispositivos IoT, podem ser aplicados centenas de um mesmo tipo de dispositivo (como sensores, por exemplo) e em locais que podem ser de fácil acesso. Isto, em conjunto com a arquitetura pensando no baixo custo e softwares compactos acabam criando um cenário vulnerável à ataques que podem explorar estes pontos, podendo infectar dezenas de dispositivos da rede. Ainda, associado a isso, temos o peopleware que por vezes pode receber menos atenção em relação à segurança da informação, mas que pode possuir vulnerabilidades tão grandes quanto as demais.

Na revisão bibliográfica, ainda, foi possível classificar nesta pesquisa os principais tipos de ataques direcionados aos dispositivos IoT, classificados em ataques passivos, ativos, de senha e de *peopleware*.

O cuidado com a segurança da informação para impedir os ataques observados nesta pesquisa é importante para qualquer organização. O impacto dos ataques pode variar de um compartilhamento de informações sigilosas da empresa até falsificação de informações (manipulação dos dados), indisponibilidade completa de serviços e potencial dano a equipamentos se o atacante, por exemplo, alterar o medidor de um sensor que controla a temperatura de determinado equipamento.

A partir do desenvolvimento desta pesquisa foi possível apresentar os resultados dos testes práticos, realizados por meio de simulações em *software*, que mostraram que o impacto pode ser de grande escala, visualizável por meio de gráficos de consumo de energia dos dispositivos simulados e por meio da visualização dos pacotes transmitidos na rede sem proteção ou criptografia, cuja informação é transmitida de forma “livre”, podendo ser compreendida facilmente.

Através dos testes simulados, podemos ver a proporção dos efeitos que os ataques podem ter sobre os dispositivos IoT. Em uma rede simples com somente alguns dispositivos ao alcance do nó infectado, tivemos um aumento de 2566% no consumo de energia destes dispositivos. Em um cenário de uma indústria que utiliza centenas de dispositivos IoT iguais em uma mesma rede, onde um atacante consegue acesso a um deles, podendo infectar grande parte dos demais, o impacto pode ser assombroso.

Ainda, no desenvolvimento da pesquisa é possível observar as diretrizes,

políticas e boas práticas identificadas para melhorar a segurança da informação em um ambiente com dispositivos IoT, pensando nos principais ataques e riscos classificados no referencial.

Mesmo que existam diversos pontos de possíveis vulnerabilidades que merecem atenção com danos potenciais significativos, temos algumas técnicas e boas práticas para mitigarmos estes riscos. Com a elaboração e aplicação das práticas descritas nesta pesquisa podemos reduzir as ameaças em toda a rede.

Além disso, no desenvolvimento da pesquisa ainda é possível observar o guia com as recomendações de técnicas, políticas e cuidados, dividido entre ações distintas a serem aplicadas a dispositivos e pessoas, de forma a abordar as técnicas para mitigar riscos pensando nos tipos de ataques previamente apresentados (passivos, ativos, de senha e de *peopleware*).

Com a aplicação do guia com as recomendações de segurança da informação apresentadas nesta pesquisa, podemos mitigar os riscos relacionados aos dispositivos IoT e aos demais aspectos que influenciam na segurança da rede, como demais *softwares* e o *peopleware* da organização.

5.3. PERSPECTIVAS FUTURAS

Com as informações expostas na presente pesquisa, observa-se que a segurança da informação no contexto da aplicação de dispositivos IoT na Indústria 4.0 é essencial para manter o bom funcionamento das organizações.

Considerando que a presente pesquisa teve um foco mais amplo, ainda há muito mais a ser analisado, pois cada um dos tópicos abordados possui seu próprio conjunto de variáveis para ser estudado. Além disso, esta pesquisa pode servir para que organizações, alertadas pelos dados e falhas de segurança expostas, possam ter uma base para aperfeiçoar seu cuidado com a segurança da informação. Neste cenário, cada organização possui seu contexto diferente, onde mudanças podem ser necessárias e este guia aperfeiçoado com novas perspectivas, riscos detectados e novas soluções implementadas.

Considerando ainda que os testes apresentados nesta pesquisa foram realizados de forma simulada, há uma perspectiva futura para a adoção do guia e a análise dos resultados de forma prática, com execuções de *pentests* por exemplo.

Além disso, em relação a utilização do software Contiki para a realização dos testes simulados, existem outros diversos tipos de nós (*motes*) que podem ser utilizados e analisados e outros tipos de ataques para serem simulados dentro do software.

Ainda, o desenvolvimento de novos tipos de tecnologias como novos dispositivos IoT podem trazer novos riscos e brechas associados à eles. Portanto se faz necessária uma constante atualização e estudo acerca da descoberta de novas vulnerabilidades.

8. REFERÊNCIAS

95% dos brasileiros estão usando senhas fracas. 2019. Elaborada por Avast. Disponível em: https://press.avast.com/pt-br/95-dos-brasileiros-estao-usando-senhas-fracas. Acesso em: 02 ago. 2021.

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. ABNT, 2013.

ADVANTECH. **WISE-4051**: 8-ch digital input iot wireless i/o module with rs-485 port. 8-ch Digital Input IoT Wireless I/O Module with RS-485 Port. 2021. Disponível em: https://advdownload.advantech.com/productfile/PIS/WISE-4051/file/WISE-4051_DS(07062 1)20210706101711.pdf. Acesso em: 02 ago. 2021.

AL-FUQAHA, Ala et al. **Internet of Things**: a survey on enabling technologies, protocols, and applications. 17. ed. : Ieee Communication Surveys & Tutorials, 2015. 30 p.

ALBARELLO, Rafael Hickmann. **Avaliação De Algoritmos De Criptografia E Implementação De Um Protocolo Leve Para Troca De Chaves Em Dispositivos IoT**. Toledo: Universidade Tecnológica Federal do Paraná, 2019. 48 p.

ALMEIDA, Mário de Souza. **Elaboração de Projeto, TCC, Dissertação e Tese**: uma abordagem simples, prática e objetiva. São Paulo: Atlas, 2010.

ALVES, Cássio Bastos. **Segurança Da Informação Vs. Engenharia Social**: como se proteger para não ser mais uma vítima. Brasília: ., 2010. 128 p.

ANDRADE, Daniel Quintana de; SANTOS, Gabriel Castrillon Silva dos. **Ataque de Homem do Meio em Aplicações de Realidade Virtual**. 2018. 57 f. Monografia (Especialização) - Curso de Sistemas de Informação, Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: https://bsi.uniriotec.br/wp-content/uploads/sites/31/2020/05/201807DanielQuintanaGabriel

Castrillon.pdf. Acesso em: 02 ago. 2021.

ASSAD NETO, Anis et al. **A Busca de uma Identidade para a Indústria 4.0**. Joinville: XXXVII Encontro Nacional de Engenharia de Produção, 2017. 14 p.

AURÉLIO, Marco. **Privacidade e Segurança na Sociedade da Informação**. 2015. Disponível em: https://www.go2web.com.br/pt-BR/blog/privacidade-e-seguranca-na-sociedade-da-informacao.html. Acesso em: 02 ago. 2021

BORGES, Hélder Pereira et al. **Computação em nuvem**. Brasil, 2011. 48 p.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**

BUSTER, Bug. **O que é servidor?** Guia de introdução. 2018. Disponível em: https://bugbusters.com.br/2018/01/19/o-que-e-servidor-guia-de-introducao/. Acesso em: 02 ago. 2021.

CERT.BR (Brasil). **Cartilha de Segurança para Internet**. 2016. Disponível em: https://cartilha.cert.br/. Acesso em: 16 jun. 2021.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. **Indústria 4.0**: Novo Desafio para a Indústria Brasileira. Brasília: Núcleo de Editoração Cni, 2016.

CONSTANTIN, Lucian. **91% das transações de dados em dispositivos IoT não são criptografadas**. 2019. Disponível em: <https://computerworld.com.br/2019/05/25/91-das-transacoes-de-dados-em-dispositivos-iot-nao-sao-criptografadas/>. Acesso em: 05 jun. 2019.

Contiki: Cooja. Versão 3.0. Contiki-NG, 2021. Disponível em: <https://www.contiki-ng.org/>. Acesso em: 02 ago. 2021

EVANS, Dave. **A Internet das Coisas**: como a próxima evolução da internet está mudando tudo : Cisco Internet Business Solutions Group (Ibsg), 2011. 13 p.

FEIMEC. **Manufatura Avançada**: Tudo que você precisa saber sobre a 4ª Revolução Industrial e os desafios a serem enfrentados para sua implementação no Brasil. São

Paulo: Feimec, 2018.

FIGUEIRA, Vitor Pinheiro. **“Internet das Coisas”**: Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura.. 2016. 66 f. - Curso de Curso de Tecnologia em Sistemas de Computação, Universidade Federal Fluminense, Niterói, 2016.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação**: o fator humano. Curitiba: ., 2009. 16 p.

FUKUDA, Leonardo Massami. **Segurança da Informação em IoT**. 2019. 39 f. Monografia (Especialização) - Curso de Mba em Gestão da Tecnologia da Informação e Comunicação, Universidade Tecnológica Federal do Paraná, Curitiba, 2019. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/13066/1/CT_GETIC_VIII_2019_05.pdf. Acesso em: 02 ago. 2021.

GARTNER. **Internet of Things**. 2019. Disponível em: <https://www.gartner.com/it-glossary/internet-of-things/>. Acesso em: 20 maio 2019.

GEMALTO. **IoT Security**: The Key Ingredients for Success. 2018. 16 p.

GREENE, Tim. **DDoS attack takes down Krebs site**. 2016. Disponível em: https://www.csoonline.com/article/3123785/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html. Acesso em: 02 ago. 2021.

HARÁN, Juan Manuel. **123456 continua sendo a senha mais comum**. 2020. Disponível em: https://www.welivesecurity.com/br/2020/07/03/123456-continua-sendo-a-senha-mais-comum/. Acesso em: 02 ago. 2021.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação**. 3. ed. Rio de Janeiro: Brasport, 2018.

HUNG, Mark (ed.). **Leading the IoT**: gartner insights on how to lead in a connected world. : Gartner, 2017. 29 p. Disponível em: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. Acesso em: 02 ago. 2020.

IFAM - Instituto Federal de Educação, Ciência e Tecnologia do Amazonas. **Política De Segurança Da Informação (PSI)**. Manaus, 2012. 29 p.

INSTITUTO FEDERAL DE SANTA CATARINA - IFSC. Matriz Curricular e Ementário do Projeto Pedagógico do Curso: Engenharia Mecatrônica. Florianópolis, 2016. 79 p.

INSTITUTO FEDERAL DE SANTA CATARINA - IFSC. **Projeto Pedagógico de Curso**: Análise e Desenvolvimento de Sistemas, 2015. 101 p.

INSTITUTO FEDERAL DE SANTA CATARINA - IFSC. **Projeto Pedagógico do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação**. Florianópolis: IFSC, 2017. Disponível em: http://florianopolis.ifsc.edu.br/images/stories/ppc/graduacao/ppc_gti_2018.pdf. Acesso em: 15 jul. 2021.

ISOTANI, Seiji et al. **Web 3.0**: os rumos da web semântica e da web 2.0 nos ambientes educacionais. Os Rumos da Web Semântica e da Web 2.0 nos Ambientes Educacionais. 2008. Disponível em: http://www.br-ie.org/pub/index.php/sbie/article/view/767. Acesso em: 02 jun. 2021.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. Saraiva, 2016. 382 p.

LACERDA, Flavia et al. **Da necessidade de princípios de Arquitetura da Informação para a Internet das Coisas**. 2015. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2356. Acesso em: 20 abr. 2019.

LI, Qing; YAO, Caroline. **Real-Time Concepts for Embedded Systems**. Crc Press, 2003. 306 p.

Linux: Ubuntu. Versão 20.04.2.0 LTS. Canonical Ltd, 2021. Disponível em: <https://ubuntu.com/download/desktop>. Acesso em: 02 ago. 2021

MACHADO MEYER SENDACZ OPICE ADVOGADOS. **Lei 13.709/18**: Lei de Proteção de Dados Pessoais. São Paulo: Machado, Meyer, Sendacz e Opice Advogados, 2018.

MACHADO, Felipe Ribeiro. **Segurança da Informação numa perspectiva mais**

humana: falhas internas e procedimentos de prevenção e defesa da rede. Recife: Universidade Federal de Pernambuco, 2009. 65 p. Disponível em: https://www.cin.ufpe.br/~tg/2009-1/frm.pdf. Acesso em: 02 ago. 2021.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. **Segurança da informação**: uma visão sistêmica para implantação em organizações. João Pessoa: Editora Ufpb, 2019. 160 p. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1. Acesso em: 02 ago. 2021.

MENEZES, Wander. **Rede Mirai**: Ataques virtuais a dispositivos de IoT se tornam mais comuns. 2017. Disponível em: <https://computerworld.com.br/2017/08/07/rede-mirai-ataques-virtuais-dispositivos-de-iot-se-tornam-mais-comuns/>. Acesso em: 06 jun. 2019.

MILLER, Lawrence. **IoT Security for Dummies**. John Wiley & Sons, Ltd., 2016. 53 p.

MURINI, Cléber Taschetto. **Análise Dos Sistemas De Detecção De Intrusão Em Redes**: snort e suricata comparando com dados da darpa. Santa Maria: Universidade Federal de Santa Maria, 2014. 58 p. Disponível em: https://www.ufsm.br/app/uploads/sites/495/2019/05/2014-CleberMurini.pdf. Acesso em: 02 ago. 2021.

NAKAMURA, E. **Segurança em de redes em cooperativos**. São Paulo: Novatec, 2007.

NOLETO, Cairo. **Segurança da informação**: o que é e os 5 principais pilares!. o que é e os 5 principais pilares!. 2020. Disponível em: https://blog.betrybe.com/tecnologia/seguranca-da-informacao/. Acesso em: 02 ago. 2021.

OTÁVIO, Luis. **IoT**: 9 exemplos de aplicativos bem-sucedidos. 9 Exemplos de aplicativos bem-sucedidos. 2019. Disponível em: https://usemobile.com.br/iot-9-exemplos-de-aplicativos/. Acesso em: 01 jun. 2021.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

QUALCOMM. **How will 5G transform Industrial IoT?**. Qualcomm Technologies, 2019. 26

p. Disponível em: https://www.qualcomm.com/media/documents/files/how-5g-will-transform-industrial-iot.pdf. Acesso em: 02 ago. 2021.

RAIWANI, Y.P.. **Internet of Things**: a new paradigm. India: Dept. Of Computer Science And Engineering, H N B Garhwal University Srinagar, Srinagar Garhwal (Uttarakhand), 2013. 4 p.

REIS, Fábio dos. **O que é Rainbow Table**. 2019. Disponível em: http://www.bosontreinamentos.com.br/seguranca/o-que-e-rainbow-table/. Acesso em: 02 ago. 2021.

RIBEIRO, Raquel Maria Oliveira. **Segurança em IoT**: simulação de ataque em uma rede rpl utilizando contiki. Patos de Minas: Universidade Federal de Uberlândia, 2018. 70 p.

SANTOS, Rodrigo Costa dos; SANTOS, Manuela Fernandes dos; CARREIRA, Fernando Spencer. **Campanha de Conscientização em Segurança da Informação**: um estudo de caso. : XIII Simpósio de Excelência em Gestão e Tecnologia, 2016. 16 p.

SILVA, Danilo Goulart da. **Indústria 4.0**: Conceito, tendências e desafios. 2017. 42 f. TCC (Graduação) - Curso de Tecnologia em Automação Industrial, Universidade Tecnológica Federal do Paraná, Ponta Grossa, 2017.

SILVA, Elaine M. da. **Cuidado com a engenharia social**, 2008. Disponível em: <https://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm?utm_source=404corrigido&utm_medium=baixaki>. Acesso em: 08 ago. 2021

SIMKO, Christian. **Man-in-the-Middle Attacks**. 2016. Disponível em: https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot. Acesso em: 02 ago. 2021.

SOUZA, Paulo Henrique Moura de; CAVALLARI JUNIOR, Silvio Jose; DELGADO NETO, Geraldo Goncalves. **Indústria 4.0**: Contribuições para Setor Produtivo Moderno. Joinville: Xxxvii Encontro Nacional de Engenharia de Produção, 2017.

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC. **Matriz Curricular e Ementário do Projeto Pedagógico do Curso**: Ciências da Computação. Florianópolis. 3

p.

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC. **Matriz Curricular e Ementário do Projeto Pedagógico do Curso**: Engenharia Mecatrônica. Florianópolis. 5 p.

VERMULM, Roberto. **Políticas para o Desenvolvimento da Indústria 4.0 no Brasil**. 2018. 31 f. Dissertação (Mestrado) - Curso de Economia, Instituto de Estudos Para O Desenvolvimento Industrial, São Paulo, 2018.

ZABADAL, Bernardo Moreira; CASTRO, Bianca Francinny Lisboa Murta de. **IoT e Seus Principais Desafios**. 2017. 10 f. - Instituto Federal de São Paulo, Boituva, 2017.