CIBERSEGURANÇA DA INTERNET DAS COISAS

Fernando Machado de Lima[1]
Marcio Freitas[2]

1. Introdução

Nos últimos anos a internet teve uma enorme expansão e com a chegado do século XXI tivemos grandes inovações tecnológicas o'que ocasionou a nós uma nova compreensão em relação a sua capacidade, uma tecnologia que foi associado a este desenvolvimento é a internet das coisas que ganhou bastante popularidade, mas não foi o único a ganhar esse reconhecimento, algumas outras tecnologias importantes que tiveram vínculo a este avanço e também ganharam popularidade, por exemplo a robótica, biotecnologia e a inteligência artificial.

A internet das coisas (IdC) pode ser complexa de se aplicar em alguns casos, porém em outros ela é simples como o seu conceito, que seria poder conectar objetos a internet e uns aos outros sendo diretamente ou indiretamente, o que disponibilizaria o acesso remoto para o usuário final, o usuário que por sua vez sendo capaz de gerenciar seus dispositivos a qualquer momento e em qualquer lugar, tendo o potencial de ajudá-lo em simples tarefas de sua rotina ou em seus projetos pessoais, o'que resultaria na economia de seu tempo. A IdC é empregada em diversos outros setores, como por exemplo muitas organizações e empresas usam principalmente em setores industriais e comerciais, porém neste meio é conhecida como Internet Industrial das Coisas. A internet das coisas parece perfeita, mas além de todas essas vantagens e aspectos positivos a internet das coisas pode ser muito perigosa e é sobre isso que iremos discutir.

[1]Aluno Curso Técnico Alcides Maya
[2]Prof. Espec. Alcides Maya. marcio_freitas@alcidesmaya.edu.br

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

1.1 Definição do problema ou tema

O assunto a ser discutido neste projeto será sobre as condições que se encontram a segurança da informação em dispositivos que utilizam a tecnologia da internet das coisas e também iremos refletir sobre alguns pontos importantes que levam a vulnerabilidades nesses dispositivos e formaremos um pensamento sobre possíveis soluções básicas a serem tomadas.

1.2 Delimitações do Tema ou Problema

Temos como prioridade o tema cibersegurança na tecnologia conhecida como a internet das coisas.

1.3 Justificativa

Com grande entusiasmo pela área da segurança da informação, o pesquisador produziu este projeto com o intuito de ressaltar alguns pontos importantes na segurança da internet das coisas e discutiremos sobre alguns fatores de segurança que impedem que essa tecnologia tenha uma evolução saudável, podendo desenvolver-se de maneira que consiga comprir seus objetivos porém com segurança.

1.4.1 Objetivo Geral

Temos como propósito questionar e repensar sobre a atual segurança utilizada na internet das coisas. iremos por a discussão sobre as vulnerabilidades em objetos interligados a internet como o uso de sistemas ultrapassados, sistemas desatualizados e o

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

requisito constante de manutenção, comunicaremos sobre a segurança da internet das coisas e algumas de suas fraquezas.

1.4.2 Objetivos Específicos

a) Analisar dispositivos interligados à internet.

b) Analisar possíveis vulnerabilidades na segurança da internet das coisas. c) Identificar possíveis soluções aos problemas encontrados.

1.5 Metodologia

A pesquisa do tipo exploratória com abordagem qualitativa baseada no método de análise de documentos. Através da análises de periódicos acadêmicos, jornais, livros e revistas em busca da compreensão da cibersegurança da tecnologia das coisas, aplica-se a interpretação de forma comparativa e associativa das informações a fim de elaborar conclusões, limitando ao material pesquisado sem a oportunidade de experimento de campo.

2 Referencial teórico (bibliográfico)

2.1 Dispositivos Interligados à Internet.

Os dispositivos interligados à internet que usam a tecnologia da internet das coisa em ambientes domésticos podem ter inúmeras funções simples e complexas, desde de ligar uma simples lâmpada ou rádio a agendar as compras e até mesmo conectar a internet ao seu veículo e sua casa para ter diversos benefícios deixando-os ”inteligentes” e vulneráveis, mas também existem ideias que são realmente boas principalmente quando essa tecnologia é usada de forma segura em ambientes industriais controlados, essa tecnologia pode agilizar diversos processos.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

> A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à Internet. A conexão com a rede mundial de computadores viabiliza, primeiro, controlar remotamente os objetos e,segundo, permitir que os próprios objetos sejam acessados como provedores de serviços.Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial. Todavia, estas possibilidades apresentam riscos e acarretam amplos desafios técnicos e sociais (SANTOS *et al.*, 20-?, p. 2).

Em setores industriais a internet das coisas tem como o seu objetivo principal a comunicação entre máquinas e a inteligência da mesma, segundo Hurel e Lobato (2018, p. 19) Com essa tecnologia podendo evoluir suas funções e desenvolver novas técnicas para realizar seus deveres de formas mais avançadas. “O emprego de decisões automatizadas, através da incorporação de tecnologias de aprendizado de máquina e inteligência potencializa a facilita o surgimento de novas funções no mercado para IoT.” esses dispositivos além de apresentarem um ótimo desempenho suas futuras versões são consideradas promissoras podendo ser um salto tecnológico porém no momento essa tecnologia deixa a desejar por alguns de seus aspectos negativos.

Segundo Magrani (2018, p. 47), muitas vezes não é uma vantagem conectar diversos dispositivos objetos à internet, e muitas vezes pode até ser uma desvantagem “Em diversos casos, o objeto analógico mais simples, sem tecnologia avançada envolvida, atende suficientemente ao consumidor, sem precisar ser algo high tech.” mesmo sendo útil ter essa tecnologia facilitando as nossas tarefas ela ainda apresenta algumas irregularidades.

2.2 Identificando riscos na internet das coisas.

Como a internet das coisas é uma novidade tecnológica ela ainda tem algumas falhas que precisam ser tratadas, em alguns casos ocorre de vulnerabilidades do sistema serem ignorados ou passar despercebida pelo seus criadores que acabam liberando o sistema vulnerável e se essas vulnerabilidades forem descoberta por outras pessoas pode

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

ser tarde demais para corrigir, podendo ser um enorme problema, como por exemplo hackers mal-intencionados quando percebem essas vulnerabilidades em uma tecnologia tão poderosa como a internet das coisas ela acaba sendo usada como uma arma muito poderosa.

Segundo Magrani (2018, p.16) Os dispositivos inseguros com a tecnologia da internet das coisas são um grande perigo "[...] A internet foi projetada para resistir a uma explosão nuclear. Mas não a um ataque de torradeiras." Magrini em seu livro se refere aos ataques DDoS onde é utilizado diversos dispositivos vulneráveis conectados a internet como bots (robôs) para atacar um ou mais alvos até o tirarem do ar temporariamente, em nosso atual cenário onde se encontram diversos dispositivos utilizando essa tecnologia leva a internet das coisas ser uma ferramenta perfeita para reunir uma grande quantidade de bots.

Os principais pontos de vulnerabilidades são:

- Falta de revisão das políticas de segurança.
- Transferência e armazenamento de dados comprometidos.
- Criptografia Fraca.
- Falta gerenciamento de dispositivos.
- Redes inseguras.

Segundo Figueira (2016, pág. 28) aos dispositivos estarem interligados uns aos outros caso um dispositivo esteja mal protegido ele colocará os demais em risco, isso é extremamente negativo. E ainda existem muitas corporações que ainda têm o descompromisso com a sua segurança sendo uma atitude lamentável em qualquer setor a ser trabalhado, essa omissão de segurança pode acabar afetando até mesmo quem não é cliente de seus serviços, e essa falta de segurança ocorre por diversas motivos como por exemplo a carência de informação, comunicação, regras morais, interesse, e principalmente a falta de atenção podendo influenciar em condições como o uso de

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

sistemas ultrapassados e desatualizados, por isso é importante sempre conscientizar seus funcionários e clientes para não terem essas complicações. E também um aspecto que faz a segurança da internet das coisas ser instável é ter que manter um custo baixo em seus dispositivos para atingir o máximo de usuários, porém o foco em recursos de segurança acabam sendo dispensados.

> Para Hernández (2015) “ainda que os dispositivos IoT não contam com os recursos de segurança dos equipamentos tradicionais de tecnologias de informação (TI) (servidores, routers, etc.). O ácido desoxirribonucleico (ADN) dos atuais dispositivos IoT está ligado a um fator crítico: é essencial garantir um custo competitivo e baixo para produtos que são, afinal, para o mercado de massa. Isto é um desafio, pois a informação gerada pela IoT é essencial para trazer melhores serviços e melhor gestão dos dispositivos” (apud SANTOS, 2016, p. 16).

Além das normas que utilizamos atualmente que estão cada vez mais instáveis e existe uma deficit de comunicação entre as empresas e seus usuários, com as empresas apenas disponibilizando o seus produtos e não informando aos usuários o risco que tais possam se submeter, às empresas que não conscientizam seus usuários claramente menospreza a sua segurança e seus valores éticos.

2.3 Identificando possíveis soluções.

Compreendendo sobre todos essas complicações na segurança da internet das coisas é precisamos considerar possíveis soluções, primeiramente um ponto simples que pode fazer total diferença é a troca de criptografias ultrapassadas e comuns, em dispositivos que usam a tecnologia da internet das coisas é preciso de uma criptografia forte como a criptografia AES que é atualmente a mais recomendada porém pode variar dependendo do sistema a ser usada, mas não basta utilizar uma criptografia complexa e segura se sua senha for uma senha fraca, é preciso conscientizar seus usuários e clientes para usarem senhas mais robustas. E as corporações devem se manter com suas políticas de segurança atualizadas principalmente ao trabalhar com excesso de dados. É importante certificar-se de realizar todos os processos de segurança necessários.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

> Estabelecer padrões mínimos de segurança e interoperabilidade entre sistemas, o que inclui a criação de incentivos positivos e a inserção de valores no desenvolvimento dessas tecnologias, tais como confiança, transparência, segurança por padrão e por concepção. Desenvolvedores, autoridades reguladoras e possíveis implementadores devem estabelecer períodos de validade para os dispositivos, de modo a garantir a segurança do usuário; emitir certificados que indiquem que aquela tecnologia adere a um determinado nível padrão de segurança e privacidade e assim; repensar formas de comunicar riscos e com o consumidor (HUREL; LOBATO, 2018, p. 25).

Com um grande número de novos dispositivos conectados a internet a serem gerenciados o dispositivo responsável pela conexão dos demais acaba não ganhando a atenção devida, o wifi em redes de trabalhos se encontra um pouco mais protegido, mas na maioria das redes domésticos ele continua sendo usado com configurações padrões e muitas vezes sem firewall, deixando-o com uma enorme facilidade de ser invadido e as redes públicas não são diferentes é importante sempre verificar a sua procedência para evitar possíveis vazamentos de informações.

A internet das coisas está distante de ter uma ótima segurança, pois ainda precisa de muitas correções como:

- Revisar Políticas de segurança
- Ter cuidado com serviços de hospedagem e transferências.
- Alterar métodos de criptografia.
- Realizar testes de avaliações.
- Identificar redes vulneráveis.

Segundo Hernández (apud SANTOS, 2016, p.16) “[...] A própria natureza destes dispositivos torna-os vulneráveis” a frase dita por Hernández propõe que estes dispositivos são a própria vulnerabilidade o que não deixa de ser uma verdade, porém com algumas atualizações a maior parte de suas vulnerabilidade podem ser resolvidas. A internet das coisas provavelmente será muito útil futuramente, mesmo agora ela tendo algumas falhas em sua segurança quando receber novas modificações e atualizações de segurança ela

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

será uma tecnologia de grande utilidade, mas até essas mudanças ocorrem devemos fazer o uso destes métodos citados para reforçar a sua segurança momentaneamente.

> Dizer que um sistema ou dispositivo está protegido, pode ser uma afirmação totalmente incerta, pois a segurança, como muitas outras propriedades relacionadas é uma condição muito delicada, que só pode ser alcançada por completo através de uma análise de todas as situações e cenários de riscos possíveis a um determinado sistema ou dispositivo (FIGUEIRA, 2016. p.33).

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

3. Conclusão

A internet das coisas pode ser inovadora porém sua segurança não é, tendo diversas falhas que levam muitos de seus sistemas a serem vulneráveis, mesmo com o desenvolvimento na tecnológico nos últimos anos, ainda existem organizações e empresas que utilizam serviços com tecnologia ultrapassada e sistemas desatualizados, e muitas vezes acabam passando esses hábitos a seus usuários mesmo sem a sua consciência.

Mesmo com muitos defeitos e vulnerabilidades a serem resolvidos, a internet das coisas ainda tem muito o que progredir principalmente em termos de segurança e privacidade onde deveriam trazer modelos de dispositivos mais seguros pois ela é uma tecnologia extraordinária com o potencial para ser uma das maiores tecnologias.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

4. Referências

Blog Brasil. **5 pontos para considerar na segurança da internet das coisas.** Disponível em: <https://blogbrasil.comstor.com/5-pontos-para-considerar-na-seguranca-da-internet das-coisas> Acesso em 07 fev. 2021

CIO. **10 principais vulnerabilidades da internet das coisas**. Disponível em: <https://cio.com.br/gestao/10-principais-vulnerabilidades-da-internet-das-coisas/> Acesso em: 07 fev. 2021.

FIGUEIRA, Vitor Pinheiro. **"Internet das coisas": um estudo sobre questões de segurança, privacidade e infraestrutura.** RJ - Niterói: Universidade Federal Fluminense, 2016. Disponível em: <https://app.uff.br/riuff/bitstream/1/5150/1/TCC_VITOR_PINHEIRO_FIGUEIRA_FINA L%20%281%29.pdf> Acesso em: 09 fev 2021

HUREL, Louise Marie; LOBATO, Luisa Cruz. **Segurança e privacidade para a internet das coisas.** Minas Gerais: Instituto Igarapé, 2018. Disponível em: <https://www.researchgate.net/profile/Louise_Marie_Hurel/publication/329972976_S eguranca_e_Privacidade_para_a_Internet_das_Coisas/links/5c269915a6fdccfc706f3 001/Seguranca-e-Privacidade-para-a-Internet-das-Coisas.pdf> Acesso em: 08 fev. 2021.

MAGRANI, Eduardo. **A internet das coisas**. 1ed, Rio de Janeiro: FGV Editora, 2018. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%2 0das%20coisas.pdf?sequence=1&isAllowed=y> Acesso em: 06 fev. 2021.

SANTOS, Bruno P. *et al*. **Internet das Coisas: da Teoria à Prática.** Minas Gerais: UFMG, 20-?. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf> Acesso em: 06 fev. 2021.

SANTOS, Pedro Miguel Pereira. **Internet das coisas: O desafio da privacidade**. Setúbal: Escola Superior de Ciências Empresariais**,** 2016.
Disponível em:
<http://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%c3%a7%c3%a3o%20Pedro%20Santos%20140313004%20MSIO.pdf> Acesso em: 06 fev. 2021.