VULNERABILIDADE, PRIVACIDADE E SEGURANÇA NA INTERNET DAS COISAS

Eduardo Rossetti Boeira[1]

Vinicius Zanchet de Lima[2]

RESUMO

O presente artigo tem como objetivo analisar os tipos de vulnerabilidades, as diversas brechas de privacidade e os principais meios de segurança relacionados a Internet das Coisas tanto no dia a dia das pessoas físicas quanto no meio organizacional. Um dos fatores que mais causam problemas de vulnerabilidades nos dispositivos IoT, se vem da baixa capacidade computacional que eles possuem, o que em retorno causam brechas maiores para atacantes conseguirem obter informações vitais das pessoas ou organizações. Por isso são destacadas questões sobre o direito da privacidade, categorizando a definição sobre privacidade e o que esses conceitos englobam, e como esses dispositivos ao serem utilizados no dia a dia podem acabar acarretando riscos a esses direitos. Por último foi pesquisado quais são as principais ferramentas de segurança para a proteção contra de ataques e as principais ferramentas na questão de proteção aos dados para garantir a segurança dos dados. Em conclusão essa análise mostrou que mesmo com os diversos meios de segurança, as vulnerabilidades ainda são mais fortes, mas como essa é uma tecnologia relativamente nova ela ainda possui uma grande chance de crescimento nas ferramentas de segurança capazes de proteger os mesmos, no final o que pode ser tirado de tudo isso é que essas vulnerabilidades não precisam ser vistas como limitações, mas como uma oportunidade de agregar valor à essa tecnologia, e as empresas que focarem nisso serão aquelas que ganharam mais destaque nesse meio.

Palavras chaves: Internet das coisas; Vulnerabilidade; Privacidade; Segurança; análise.

ABSTRACT

The present article aims to analyze the types of vulnerabilities, the various privacy breaches and the main means of security related to the Internet of Things both in the daily lives of individuals and in the organizational environment. One of the factors that most cause problems with vulnerabilities in IoT devices comes from the low computing capacity they have, which in turn causes greater gaps for attackers to obtain vital information from people or organizations. That is why issues about the right to privacy are highlighted, categorizing the definition of privacy and what these concepts encompass, and how these devices, when used on a daily basis, can end up posing risks to these rights. Finally, it was researched what are the main security tools to protect against attacks and the main tools in the matter of data protection to guarantee data security. In conclusion, this analysis showed that even with the various security means, the vulnerabilities are still stronger, but as this is a relatively new technology it still has a great chance of growth in the security tools capable of protecting them, in the end what can be taken

away from all this is that these vulnerabilities don't need to be seen as limitations, but as an opportunity to add value to this technology, and the companies that focus on this will be the ones that have gained more prominence in this environment.

Keywords: *Internet of things; Vulnerability; Privacy; Safety; analysis.*

1 INTRODUÇÃO

Pelo mundo estar cada vez mais conectado, ainda mais após o cenário pós pandêmico que teve como o principal entretenimento a internet e ferramentas tecnológicas, por causa das pessoas tendo que ficar isoladas em casa, graças e isso é necessário compreender como foi a evolução relacionada na internet e nos equipamentos nela conectados. A cada dia mais equipamentos se conectam a internet e trazem facilidades e melhorias, como interruptores, relógios inteligentes, lâmpadas, fechaduras entre tantos outros, esses equipamentos compõem os objetos na Internet das Coisas (IoT). Mas nesse meio vem o questionamento do quão seguros são esses equipamentos, quais meios para a proteção da privacidade existem e quais são os esforços para que eles sejam cada vez menos vulneráveis possibilitando assim a proteção das informações pelas ameaças da internet. (DELLA; FLORIAN, 2022)

A IoT está lentamente adicionando cada vez mais dispositivos à infraestrutura de rede global, de diferentes fabricantes e com características e configurações distintas, ao qual estão interconectados, esses dispositivos podem apresentar vulnerabilidades ao qual podem ser exploradas, pondo em risco assim, a disponibilidade, integridade e confidenciabilidade da informação (LEITE, 2019).

A privacidade é o direito de proteção ao qual os indivíduos possuem sobre sua pessoa e propriedade (WARREN e BRANDEIS, 1890). Os autores relatam que as vidas privadas e domésticas foram invadidas por causa das fotografias instantâneas e de eventos jornalísticos, mostrando que o que antes era colocado dentro de um armário, passou a ser dito nas coberturas das casas. Nos dias atuais, a tecnologia, cada vez mais, cria essa preocupação na sociedade, tornando assim esses riscos mais amplos e complexos.

Mesmo os equipamentos IoT trazendo grande benefícios devido a sua aplicabilidade em diferentes áreas, existem algumas questões de segurança e privacidade que podem vir a ser comprometidas, no momento em que esses dispositivos não possuem os mecanismos de proteção adequados. Isto se dá, em partes, pela produção em massa sem devidas precauções de projeto, bem como a ausência de conhecimentos tecnológicos por parte do consumidor (GILL; GARRAGHAN; BUYYA, 2019). Essa facilidade trazida por esses dispositivos pode fazer com que os usuários não se preocupem eficientemente com a segurança própria, de sua família, e a dos seus dados. Ao fazer o compartilhamento de seus dados digitalmente, se abre uma enorme via para pessoas com intenção de roubar esses dados, para falhas técnicas causadas por algum problema no dispositivo ou algum problema nos softwares, pois tal softwares tem sua codificação feita por humanos e esses estão sujeitos a falhas (SOUZA, 2016).

Nesse contexto, o objetivo deste trabalho foi apresentar as diversas vulnerabilidades nos dispositivos IoT e como essas vulnerabilidades podem trazer riscos para o capital da empresa e a vida das pessoas, após isso foi feita uma pesquisa sobre o que é privacidade e como ela está relacionada aos dispositivos IoT e ao cotidiano das pessoas e empresas, buscando assim relacionar qual o impacto que as vulnerabilidades têm diante a privacidade. Por último é feita uma busca sobre os principais meios de segurança que esses dispositivos possuem, em seus meios digitais, físicos, jurídicos e empresariais.

Desta forma, no que tange a estrutura do estudo, após a introdução, apresenta-se o método de pesquisa abordando a metodologia utilizada. Na sequência, a apresentação e discussão dos resultados onde será apresentada uma breve introdução à Internet das Coisas (IoT), após isso no segundo tópico serão apresentadas as vulnerabilidades que esses dispositivos podem vir a possuir, no terceiro tópico será apresentada o que é a privacidade e o que ela impõe nos dispositivos IoT, no último tópico serão apresentados os principais meios de segurança disponíveis para os dispositivos IoT. Finaliza-se com as considerações finais e as referências.

2 MÉTODO DE PESQUISA

Foi utilizada o método de pesquisa bibliográfica para a realização desse trabalho, fazendo uso de diversos repositórios de universidades, sites de busca e livros para formar a fundação teórica apresentada.

Pela visão de Treinta et al. (2014) a primeira etapa na construção da pesquisa bibliográfica é a definição dos elementos básicos que serão colocados no detalhamento da pesquisa, como sua contextualização, o problema da pesquisa e os objetivos que vão ter a função de esclarecer vários conceitos chaves da pesquisa.

Segundo Macedo (1996), a pesquisa bibliográfica é a procura por informações bibliográficas sobre um determinado assunto, ela pode ser nomeada também como revisão bibliográfica, pois ela traz consigo o estudo de alguma coisa que já é conhecida. Ela possui como principal intuito o levantamento bibliográfico já produzido de um determinado tema, não importando o formato utilizado, desse modo a partir dessa nova perspectiva ou abordagem utilizada durante o levantamento, novas conclusões inovadoras e dados atualizados podem ser assim produzidos (MARCONI; LAKATOS, 2010).

A pesquisa foi em sua maior parte feita com a base de dados da Google Acadêmico, com palavras relacionadas ao tema, como exemplos: “Internet das coisas”, “Vulnerabilidade na internet das coisas”, “Privacidade na internet das coisas”, “Proteção na internet das coisas”, os artigos encontrados demandaram a leitura e a seleção de diversas partes dos mesmos.

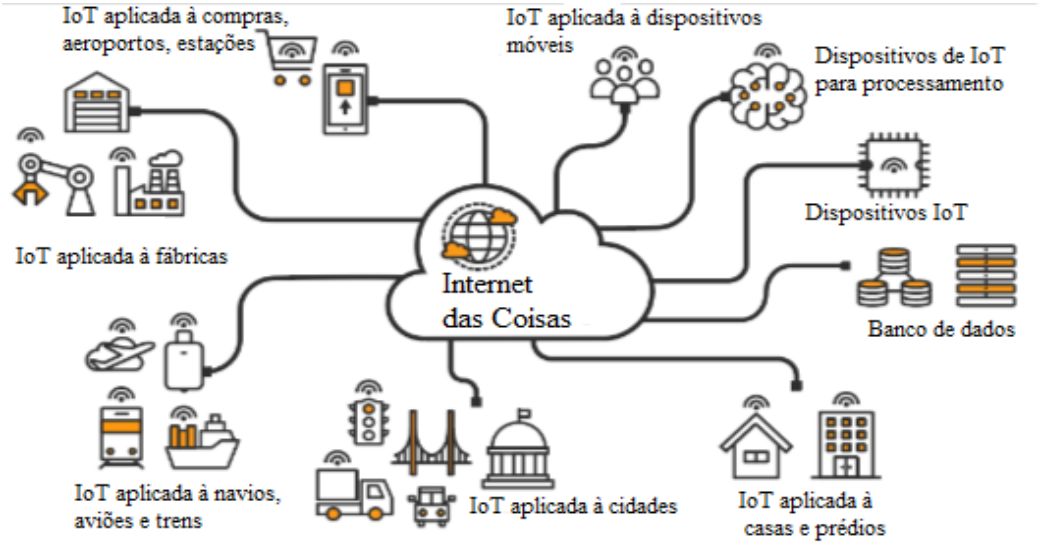
Com o auxílio das referências dos relatórios encontrados além dos relatórios ao qual essas referências se encontravam e na utilização de alguns livros foi possível fazer uma pesquisa mais aprofundada em diversos subtópicos específicos da pesquisa aqui apresentados, como: “Criptografia”, “Governança de dados”, “Lei Geral de Proteção aos Dados”, “Segurança da Informação”, “Privacidade”, esses subtópicos além de pesquisados por meio das referências, foi pesquisado diretamente através do Google Acadêmico, encontrando assim mais conteúdo sobre os temas aqui apresentados.

3 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

3.1 INTRODUÇÃO À INTERNET DAS COISAS

A internet das coisas (Internet of things) em um contexto geral, trata-se de uma evolução tecnológica que tornou a possibilidade da interligação e conexão de objetos físicos com a internet, tendo como principal objetivo a troca, armazenamento e coleta de dados para consumidores e empresas, através de aplicações de softwares (CARRION; QUARESMA, 2019). Estes objetos então são considerados como a "coisa" e podem estar inseridos em diversos locais como indústrias, hospitais, cidades, casas, entre diversas outras (Figura 1).

Figura 1 – Representação de um sistema formado por IoT



Fonte: Tibco, 2022

Com isso podemos entender a Internet das coisas como um paradigma que tem como objetivo criar uma ponte entre acontecimentos do mundo real e suas representações no mundo digital, com o objetivo de integrar o estado das coisas que consistem o nosso mundo em aplicações de software (VALENTE, 2011).

A origem do termo contudo, surgiu em 1999, quando o pesquisador britânico do Massachusetts Institute of Technology (MIT), Kevin Ashton, o utilizou no título para uma apresentação a empresa Procter & Gamble (P&G), sobre a aplicação da tecnologia de Identificação por Rádio Frequência (RFID) na cadeia de suprimentos da mesma (ASHTON, 2009). Na visão do pesquisador os computadores, e consequentemente a internet, dependem

quase que completamente de seres humanos para receber informação. O problema com isso é que pessoas possuem tempo, atenção e precisão limitadas, o que significa que eles não são muito bons em capturar dados sobre coisas do mundo real.

Segundo Kevin, nossa sociedade e sobrevivência não são baseadas em ideias ou informações, elas são baseadas em "coisas", não podemos afinal comer bytes, queimá-los para nos aquecer, ou colocá-los em nosso tanque de gasolina. Sendo assim propunha Kevin que se os computadores pudessem saber tudo que tem para saber sobre as coisas, usando dados que eles acumulam por si mesmos, nós conseguiríamos acompanhar e manter controle de tudo, conseguindo assim uma grande redução de custos, perdas e desperdícios.

3.2 VULNERABILIDADE NA IOT

Graças ao baixo poder computacional dos dispositivos IoT, podem existir diversas dificuldades para a implementação de medidas de segurança como criptografia, senhas e também na utilização de algoritmos mais sofisticados, podendo assim trazer grande prejuízo no ambiente onde estão atuando. Com a comunicação sem fio, diversas vulnerabilidades desta tecnologia são agravadas pela dificuldade na utilização de criptografias mais robustas, comprometendo assim, questões de segurança da informação (MORAES, 2010).

O Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), identificou em 2017, mais de 800 mil ataques cibernéticos pelo país, no qual 53.10% foram varreduras em redes de computadores, com o intuito de "identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles" sendo "amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador." (CERT, 2018a) Desse total de ataques notificados ao CERT.br em 2017, 220.188 foram ataques de negação de serviço (DOS), que se originou de dispositivos IOT. (CERT, 2018b) Esse número de ataques ocorre porque em países como o Brasil, muitos dos produtos IoT são desenvolvidos com sistemas operacionais e softwares antigos e desatualizados (COMPUTER WORLD, 2016). Há também uma grande falta de critérios e padrões mais extensamente adotáveis de segurança na fase de desenvolvimento desses dispositivos. (DUC et al., 2017).

A OWASP (Open Web Application Security Project) ou Projeto Aberto de Segurança em Aplicações Web é uma comunidade online que disponibiliza diversas ferramentas para o campo de segurança em aplicações web (OWASP, 2018). Com o intuito de ajudar fabricantes, desenvolvedores e consumidores a entender melhor questões de segurança a IoT. No fim de 2018, a OWASP divulgou uma lista com as 10 principais vulnerabilidades de IoT para 2019, ao qual são descritas na tabela abaixo:

Tabela 1 - 10 principais vulnerabilidades da IoT para 2019

Vulnerabilidade	**Descrição**
Senhas fracas, previsíveis ou dentro do código	A utilização de senhas que não podem ser alteradas e são fáceis de adivinhar através da técnica de força bruta, ou até mesmo *backdoors* em *firmware* ou *software* cliente ao qual obtém acesso não autorizado a sistemas, aproveitando-se dessas senhas vulneráveis.
Serviços de rede inseguros	Serviços desnecessários ou inseguros de rede em funcionamento no dispositivo, especialmente naqueles expostos a internet, que comprometem a confiabilidade, integridade ou disponibilidade da informação ou que permitem controle remoto não autorizado.
Ecossistema de interfaces inseguros	Problemas de segurança em interfaces web, API (Application Programming Interface) de *backend*, na nuvem, ou dispositivos móveis em ecossistemas fora daquele ao qual o dispositivo permite, assim comprometendo o dispositivo ou seus

	componentes. Problemas comuns incluem falta de autenticação, falta ou fraca criptografia, e falta de filtragem na entrada e saída.
Falta de mecanismos de atualização seguros	Falta de uma forma segura para a atualização dos dispositivos. Isso pode incluir uma falta de validação do *firmware* do dispositivo, falta de segurança na transferência (tráfego não seguro), falta de mecanismos para evitar reversão e falta de notificações sobre alterações de segurança devido às atualizações.
Uso de componentes inseguros ou obsoletos	Utilização de componentes de software obsoletos e/ou inseguros que permitem que o dispositivo seja comprometido. Isso inclui customizações inseguras do sistema operacional da plataforma e uso de softwares de terceiros ou componentes de hardware de um vendedor comprometido.
Proteção da privacidade insuficiente	Uso da informação pessoal armazenada dentro do dispositivo ou no ecossistema de forma insegura, imprópria ou sem permissão.
Transferência e armazenamento de dados de maneira insegura	Falta de criptografia ou controle para o acesso de dados sensíveis em qualquer lugar do ecossistema, incluindo com o dispositivo em repouso, em transferência ou durante o processamento.

Falta de controle de gerenciamento dos dispositivos	Falta de suporte de segurança nos dispositivos em produção, incluindo gestão de ativos, gestão de atualização, desarme seguro, monitoramento do sistema e capacidade de resposta.
Configuração insegura por padrão	Dispositivos ou sistemas enviados com padrões de configuração inseguros ou a falta da habilidade para aplicar restrições aos operadores de modificar certas configurações.
Segurança física insuficiente	Poucas medidas de segurança física, permitindo criminosos a ganhar informações sensíveis que podem ajudar em um futuro ataque remoto ou tomar controle remoto do dispositivo.

Fonte: Elaborado pelo autor, baseado em OWASP (2018)

Muitas vezes esses dispositivos têm sido alvos de ataques, apenas na intenção de transformá-los em "zumbis" de forma que fiquem à disposição dos invasores, eles então são utilizados em ataques, normalmente de negação de serviços. Ainda nessa questão, um invasor pode se passar por um usuário legítimo e autorizado, conseguindo assim roubar informações ou até mesmo danificar fisicamente ou logicamente esses aparelhos. Em muitos casos, esses aparelhos estão sendo utilizados em pontos críticos, como no sistema de controle do espaço aéreo, em sensores de nível de chuva ou no controle de temperatura de uma linha de montagem em uma fábrica. Estes aparelhos podem estar exercendo tarefas que demandem um grande nível de precisão e disponibilidade, e caso seu objetivo não for cumprido de maneira correta, podem ocorrer prejuízos financeiros ou riscos de vida para as pessoas envolvidas (TONEZER, 2017).

Uma outra ameaça frequente é a de *eavesdropping*, no qual a comunicação em uma rede IoT pode ser interceptada e decifrada. Esses ataques normalmente ocorrem caso o canal de

comunicação não está devidamente protegido, alguns desses ataques podem ocorrer caso a chave de cifragem, parâmetros de segurança ou definições de configuração, forem trocados de maneira clara ou se não foi utilizado algoritmos criptográficos fortes e adequados para a proteção (RIBEIRO, 2021).

3.3 PRIVACIDADE NA IOT

Para se ter uma concepção mais ampla de como a inovação tecnológica pode vir a se tornar uma ameaça, é preciso antes compreender os conceitos de privacidade, ao quais são muito amplos (SOLOVE, 2008). Segundo o autor, a privacidade abrange diversos conceitos como a liberdade de pensamento, controle sobre o próprio corpo, solidão na própria casa, controle sobre informações pessoais, liberdade de vigilância, proteção da reputação e proteção de interrogatórios e procuras. Ele criou assim seis categorias para a definição de privacidade: direito de ficar sozinho; acesso limitado ao “eu”, direito ao sigilo, controle de informação pessoal, personalidade e intimidade.

Porém o mercado de dados pessoais já é a principal fonte de receita em algumas partes da economia mundial. O maior limitador para a expansão desse mercado é o direito à privacidade, uma transparência completa do dia a dia das pessoas está sendo procurada pelas forças do mercado. Além disso, a vigilância por parte do Estado também busca restringir o direito à privacidade (SILVEIRA et al. 2016).

A presença evasiva desses dispositivos gera diversos riscos a privacidade dos usuários, aonde cada iteração entre o usuário e estes dispositivos possuem a tendencia de gerar uma quantidade enorme de dados que são coletados sem possuir um padrão ou metodologia (LIU et al. 2018).

Com a introdução desses dispositivos no cotidiano das pessoas, são levantadas então duas questões principais relacionadas à temática do consentimento: o conhecimento de que os dados pessoais de qualquer natureza estão sendo coletados, tanto em ambientes públicos, quanto privados; e a possibilidade de autorizar, ou impedir que essas informações sejam capturadas ou compartilhadas.

Para a comercialização de produtos e serviços é comumente utilizado estratégias baseadas em contratos de adesão ou acordos com termos de uso, assim deixando pouca, ou nenhuma opção para o indivíduo acerca do que de fato ele deseja fazer com seus dados, reduzindo seu poder de conceção (ROSNER, 2016). Por exemplo, um carro que pode constantemente rastrear sua localização, deve existir a possibilidade para que o condutor desabilite por completo essa opção? Ou ainda, deve existir uma manifestação constante de concessão sobre todas as informações coletadas e transmitidas sobre o indivíduo? Outro ponto importante a destacar é relacionado à proteção dos dados pessoais de crianças e adolescentes. Pela sua capacidade limitada na avaliação de riscos e consequências, são necessárias regras de proteção especificas em questões de coleta, transmissão e uso destas informações, inclusive em fins comerciais.

O desenvolvimento da IoT deve então seguir princípios básicos de proteção da privacidade pessoal, por meio de leis, modelos de proteção à privacidade, regulamentações e tecnologias que garantam a essa inviolabilidade da privacidade pessoal, tentando assim, remover obstáculos e barreiras para as suas aplicações (ZHANG; YE, 2010), mas por essa grande preocupação da privacidade dos usuários em relação à Internet das Coisas, podemos ter limitações em questões cruciais de implementações da visão IoT (MIORANDI et al., 2012). O controle desse ambiente complexo, assim como a troca de dados invisíveis e constante entre as coisas e as pessoas, e entre as coisas e outras coisas, necessita ocorrer de forma anônima, sem o conhecimento dos proprietários e criadores desses dados. A escala e capacidade cada vez maior dessas novas tecnologias vai ampliar esse problema. Ter um controle dos dados recolhidos por todos os objetos que compõem esse ambiente inteligente é uma tarefa chave no desenvolvimento dessa nova realidade (CHABRIDON et al., 2014).

3.4 SEGURANÇA NA IOT

A utilização dos dispositivos IoT’s em escala pelas indústrias e residências mostra uma necessidade desses equipamentos possuírem mecanismos para a garantia de sua integridade física e virtual, assim certificando de que a privacidade e segurança das informações armazenadas e processada por eles sejam garantidas, obtendo assim proteção de possíveis

ataques. Graças a isso, soluções aplicadas à segurança desses dispositivos passaram a ganhar mais destaque, tendo em vista que o risco da exposição de dados pode gerar danos aos usuários, ao valor pessoal e empresarial dessas informações. (KASTNER et. al, 2019)

Como afirma Ribeiro (2021), a segurança é algo primordial em IoT, uma vez que a tecnologia usada nestes dispositivos tem como principal objetivo recolher informações de forma discreta, porém, em diversos casos são recolhidas informações sensíveis, tanto para as pessoas, como para as organizações, o que implica em uma preocupação ainda maior com segurança e privacidade.

Segundo Shelby e Bormann (2011), existem pelo menos três grupos de objetivos desejáveis para a segurança, sendo elas, confidencialidade, integridade e disponibilidade. A confidencialidade determina que os dados não podem ser "escutados" por terceiros fora da comunicação, os dados devem permanecer secretos exceto para os participantes autorizados a essa comunicação. A integridade determina que os dados não podem ser alterados por terceiros não autorizados, tendo assim a necessidade da implantação de criptografia para verificação da integridade nas mensagens enviadas e com posterior verificação do lado receptor da mensagem. Por fim, a disponibilidade determina que o sistema esteja sempre disponível para os utilizadores autorizados e seguro contra os ataques maliciosos.

3.4.1 Principais Tipos de Defesas em Sistemas IoT

3.4.1.1 Segurança Criptográfica

Para que um algoritmo de criptografia possa ser considerado seguro, ele deve misturar suficientemente o conteúdo original para que seja inviável ao computador descobrir o conteúdo da mensagem original. Esses algoritmos podem ser classificados em duas importantes cifras: simétricas e assimétricas (ALBARELLO, 2019).

A criptografia simétrica consistente na utilização de somente uma chave primaria para a criptografia e descriptografia da informação. Um ponto que requer atenção nessa criptografia é que para que a informação seja compreendida é necessário o compartilhamento da chave com

o destinatário, o que pode muito bem comprometer a segurança caso feita de maneira indevida (MENEZES; OORSCHOT; VANSTONE, 1996).

Já a criptografia assimétrica consistente em duas chaves uma privada e outra pública, ao qual são utilizadas de maneira conjunta para a criptografia e descriptografia da informação. Nessa criptografia, somente a chave pública precisa ser compartilhada, onde ela é utilizada para criptografar a informação, enquanto a privada é utilizada para descriptografar (STALLINGS, 2015).

O quadro abaixo mostra a relação entre as criptografias simétricas e assimétricas e leva em conta as vantagens e desvantagens de cada tipo:

Tabela 2 - Criptografia simétrica e assimétrica

Criptografia simétrica e assimétrica		
	Vantagens	**Desvantagens**
Simétrica	Segurança forte	Troca de chaves segura
	Performasse rápida	Gestão de chaves
	Poucos recursos computacionais	
Assimétrica	Sem problemas de troca ou gestão de chaves	Precisa de chaves maiores para uma segurança de equivalência a simetria
	Altamente escalável	Performasse mais lenta
	Múltiplos usos (autenticação, controle de acesso, confidencialidade e privacidade, integridade dos dados, não repúdio)	Ele requer mais recursos computacionais

Fonte: Miller, 2016, tradução própria

Os dois algoritmos possuem vantagens e desvantagens, portando a maneira como é utilizado vai depender do cenário da organização, sempre tendo em consideração as informações que devem ser protegidas, a capacidade de processamento disponível e como os dados serão transmitidos (BERLANDA, 2021).

3.4.1.2 Segurança Física

A proteção das instalações talvez seja um dos recursos mais importantes que a IoT precisa, pois é uma forma de garantir a integridade física dos dispositivos, sejam eles, computadores, servidores firewalls ou de dados, entre outros. Essa segurança é alcançada usando barreiras físicas para o bloqueio de pessoas não autorizadas, sistemas de monitoramento e detecção de invasão para verificar comportamentos anormais, controle de acesso para garantir que apenas usuários autorizados entrem nas instalações da IoT e até mesmo utilização de segurança patrimonial, a fim de garantir a total segurança dos dispositivos (LEITE, 2019).

3.4.1.3 Segurança de dados

3.4.1.3.1 Segurança da Informação

A segurança da informação é responsável por tomar medidas para proteger a informação. Ela tem que garantir a continuidade das atividades, a integridade da informação e a disponibilidade da informação e dos serviços das organizações (OLIVEIRA et al. 2016). Em outras palavras deve buscar proteger um grupo de informações que tem valor para uma pessoa ou organização (NOBRE et al., 2019).

Segurança da informação é uma área do conhecimento dedicada a proteger a informação independentemente do seu grau de sigilo de conteúdo, assim tendo em vista a limitação de seu acesso e utilização a apenas pessoas a quem lhe é destinada (SÊMOLA, 2014).

O padrão de segurança que pode ser dito como fundação da segurança da informação é o conjunto de normas da família ISO 27000, que buscam trazer através de seus conceitos uma maior segurança das informações através de um Sistema de Gestão de Segurança da Informação (SGSI) para uma organização. Estas normas trazem consigo uma séria de controles, boas práticas e um conjunto de mecanismos para a garantia de revisão e melhoria nos processos de negócio a fim de evitar percas para uma companhia (OLIVEIRA et al. 2016). Essas normas devem ser utilizadas como base para a segurança da informação quando houver necessidade de tratar-se desse tema.

As limitações técnicas devida a baixa capacidade dos dispositivos IoT não deve ser interpretada como apenas um problema, mas um pedaço chave correto no manuseio dos mesmos. A segurança da informação abrange diversas soluções para garantir os três grupos de objetivos da segurança, anteriormente descritos. Um método de controle pode ser desde um recurso técnico de TI (Tecnologia da informação), como um processo ou verificação ou sua frequência de ocorrências (REPINOSKI; MORÃES, 2017). Uma simples utilização de um log de ações por exemplo, já configura um processo de segurança para um determinado dispositivo, pelas informações ali encontradas. Isso pode ser verificado quando esses processos e atividades são devidamente documentos, sendo a utilização dessas práticas formas de controles da gestão de conhecimento que visa a garantia da continuação dos processos da empresa ou organização.

3.4.1.3.2 Governança de Dados

A governança de dados tem por finalidade tratar os dados como algo valioso as organizações, ou seja, como ativos. Para isso a governança de dados dispõe de processos, políticas, padronizações e tecnologias que buscam tratar e garantir a disponibilidade, acessibilidade, qualidade, consistência e segurança dos dados (SANTOS, 2010). Uma utilização de um *framework* de governança de dados pode ajudar as organizações a utilizarem os dados com mais eficiência. Esse *framework* deve prover definições consistentes, estabelecer uma administração de dados na organização e ser capaz de mensurar e rastrear a qualidade dos dados.

Ao serem adotadas as boas práticas de governança de dados, é possível assegurar que os dados gerados estejam disponíveis a quem os necessita, podendo ser acessados de forma rápida. A governança de dados busca também a garantia da segurança, consistência e qualidade dos dados, podendo assim ser auditados para diferentes finalidades (ESPÍNDOLA et al., 2018).

3.4.1.3.3 Lei Geral da Proteção de dados (LGPD)

No dia 14 de agosto de 2018, foi sancionada parcialmente, com alguns vetos, pelo Presidente da República Brasileira Michel Temer, a lei N° 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), com o intuito de proteger os dados pessoais e sigilosos dos usuários e

fortalecer a transparência nas operações de tratamento e armazenamento desses dados (AGOSTINELLI, 2018). Essa nova lei, entrou em vigor então em setembro de 2020, com multas e penalizações sendo aplicadas após três anos, entrando em vigência no dia 1 de agosto de 2021 (LORENZON, 2021).

O principal objetivo da LGPD, é de proteger os direitos de liberdade e privacidade de todos os cidadãos que estejam no Brasil. Graças a essa legislação é possível criar um cenário com segurança jurídica a todos os negócios que envolvem o tratamento de dados, a padronização de regulamentos e práticas para garantir a proteção aos dados pessoais. Um outro objetivo gerado é a criação de um ambiente com desenvolvimento econômico e tecnológico, com o uso de regras flexíveis e aprimoradas para cuidar de modelos de negócios baseados no uso de dados pessoais. O Brasil também fica apto a processar dados com origem de países que exigem níveis de proteção de dados (MAGRI, 2019).

A LGPD visa tornar-se responsável por algumas vantagens no processamento de dados em território brasileiro, facilitando assim a vida da sociedade. Para isso a LGPD estabeleceu regras únicas e harmônicas sobre o uso dos dados pessoais, independentemente do setor, atribuindo maior flexibilidade para o uso dos dados pessoais. Ela também possui o objetivo de redução de custos operacionais por incompatibilidades feitas por agentes diversos, além de estimular uma maior qualidade de dados no ecossistema (NOBRE et al, 2019).

Jéferson C. Nobre (2019), destaca três pontos principais ao qual devem ser considerados como maior desafio na implantação das normas da LGPD em dispositivos restritos de IoT, sejam eles por limitações técnicas ou custos: coleta, transmissão e armazenamento de dados.

4 CONCIDERAÇÕES FINAIS

O objetivo desse trabalho foi analisar as principais vulnerabilidades existentes na IoT, como a privacidade se relaciona e impacta os dispositivos IoT, e quais são os principais meios de segurança existentes nos diversos meios ao qual os dispositivos estão inseridos e como esses assuntos se relacionam e geram valor uns aos outros. Diante desses objetivos, foi necessário analisar primeiramente os tipos de vulnerabilidades que esses dispositivos possuem e com isso

foi possível verificar como elas possuem influência na privacidade e proteção dos dispositivos nos tópicos seguintes. Considerando os objetivos iniciais, o trabalho atingiu os resultados esperados proporcionando aprendizagem e clareza também sobre outros tópicos relevantes ao assunto como as questões de segurança sobre os dados.

Como os dispositivos IoT são relativamente novos e com capacidade computacional limitada a pesquisa enfatiza a necessidade de boas medidas de segurança para os dispositivos IoT, ainda mais por eles estarem cada vez mais inseridos no dia a dia das pessoas físicas e no ambiente empresarial. Ainda assim, questões de segurança jurídica relacionada a segurança de dados mostram-se também muito novas, como a LGPD que entrou em vigor somente em 2021, com isso podemos ver que o mundo está cada vez mais preocupado com a segurança de dados privados, tornando então a busca pelo aperfeiçoamento da segurança e eliminação das vulnerabilidades existentes dos dispositivos IoT como um ativo maior para os fabricantes dos mesmos e demonstrando assim que aqueles que transformarem os dispositivos mais seguros, ganharam vantagem comercial contra aqueles que não investirem no mesmo.

Outro fator importante que deve ser considerado é o fator humano, por mais que sejam desenvolvidos protocolos e leis de segurança que estejam bem estabelecidos, a falha humana não deixa de estar presente e é uma questão que deve ser levada em consideração na elaboração desses protocolos.

No meio acadêmico, o trabalho contribuiu como base de estudo sobre segurança nos meios digitais, e pode ser usado como um comparador para novos estudos futuros sobre o assunto, demostrando o quanto que esses dispositivos mudaram para retirar essas vulnerabilidades e o quão bem as regras na questão do gerenciamento de dados para a privacidade dos indivíduos se adaptaram.

Considerando a quantidade de dispositivos novos que estão surgindo a cada ano, esse tema acaba se tornando relevante, já que a maior parte das empresas busca essa facilidade na adaptação das máquinas, principalmente com a nova realidade sendo as indústrias 4.0 que são indústrias que adaptam os dispositivos IoT nos diversos meios de produção, ou com as “smart houses”, que são residências que adaptam os dispositivos ao nas casas das pessoas. Por isso é necessário para as empresas e fabricantes dessas tecnologias estarem atentas as questões aqui

apresentadas, para assim criar um ambiente onde esses dispositivos estão seguros para serem utilizados.

A maior limitação foi em relação à metodologia utilizada, onde encontrou-se uma ampla disponibilidade de conteúdo, mas nada muito específico sobre algumas das questões de segurança física dos dispositivos. Para novas pesquisas, uma sugestão é a análise da segurança física nas empresas, verificando o quão seguros esses dispositivos realmente estão e se essas empresas possuem as medidas certas para mantê-los seguros. Outra sugestão é a análise da segurança desses dispositivos no cotidiano das pessoas, para avaliar o quão seguros eles realmente são, o quanto de informação eles processam diariamente das pessoas e o quão informadas as pessoas estão sobre essa informação sendo retirada delas.

REFERÊNCIAS

AGOSTINELLI, J. A importância da lei geral de proteção de dados pessoais no ambiente online. **ETIC-Encontro De Iniciação Científica-ISSN 21-76-8498**, v. 14, n. 14, p. 1-22, 2018.

ALBARELLO, R. H. Avaliação De Algoritmos De Criptografia E Implementação De Um Protocolo Leve Para Troca De Chaves Em Dispositivos IoT. **Toledo: Universidade Tecnológica Federal do Paraná**, p.1-48, n. 4, 2019.

ASHTON, K. **That 'Internet of Things' Thing.** 2009. Disponível em: https://www.rfidjournal.com/articles/view?4986. Acesso em: 26 ago. 2022.

BERLANDA, R. G. Guia de segurança da informação para a conectividade de dispositivos IoT. **Instituto Federal Santa Catarina**, p. 1-93, 2021.

CARRION, P.; QUARESMA, M. Internet da Coisas (IoT): Definições e aplicabilidade aos usuários finais. **Human Factors in Design**, v. 8, n. 15, p. 49-66, 2019.

CERT.br. 2018a. **Estatísticas dos Incidentes Reportados ao CERT.br.** Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 21 set. 2022

CERT.br. 2018b. **Incidentes Reportados ao CERT.br - janeiro a dezembro de 2017.** Disponível em: https://www.cert.br/stats/incidentes/2017-jan-dec/analise.html. Acesso em: 21 set. 2022

CHABRIDON, S. et al. A survey on addressing privacy together with quality of context for context management in the Internet of Things. **annals of telecommunications-annales des télécommunications**, v. 69, n. 1, p. 47-62, 2014.

COMPUTER WORLD. 2016. **"Sistemas desatualizados são a principal vulnerabilidade crítica no Brasil".** Computer World. Disponível em:

https://computerworld.com.br/2016/10/18/sistemas-desatualizados-sao-principal-vulnerabilidade-critica-no-brasil/. Acesso em: 22 set. 2022

SILVEIRA, S. A. et al. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, v. 12, n. 2, p.1-14, 2016.

DELLA R., L.; FLORIAN, F. Estudo sobre segurança e privacidade na internet das coisas (IOT). **RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218**, v. 3, n. 6, p. 1-11, 2022.

DUC, A. N. et al. Security challenges in IoT development: a software engineering perspective. In: **Proceedings of the XP2017 scientific workshops**. p. 1-5, 2017.

ESPÍNDOLA, P. L. et al. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 16, n. 3, p. 274-298, 2018.

GILL, S. S.; GARRAGHAN, P.; BUYYA, R. ROUTER: Fog enabled cloud based intelligent resource management approach for smart home IoT devices. **Journal of Systems and Software**, v. 154, p. 125-138, 2019.

KASTNER, A.; KURITZKY, M.; LUKACS, R. **The Global Risks Report 2019.** Ed. 14, Geneva: World Economic Forum, 2019.

LEITE, L. R. C. **Internet das Coisas (IoT): Vulnerabilidades de Segurança e Desafios.** p. 1-45, 2019. Trabalho de conclusão de curso (Tecnólogo em segurança da informação). São Paulo: FATEC – Faculdade de Tecnologia de Americana.

LIU, J.; ZHANG, C.; FANG, Y. Epic: A differential privacy framework to defend smart homes against internet traffic analysis. **IEEE Internet of Things Journal**, v. 5, n. 2, p. 1206-1217, 2018.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD E GDPR) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia**, v. 1, p. 39-52, 2021.

MACEDO, N. D. D. **Iniciação à pesquisa bibliográfica.** Ed. 2, São Paulo: Edições Loyola, 1996.

MARCONI, M. A.; LAKATOS, E. M. **Metodologia do trabalho científico: procedimentos básicos, pesquisa bibliografia, projeto e relatório, publicações e trabalhos científicos.** 6. Ed, São Paulo: Atlas, 2010.

MAGRI, M. DA ROCHA. Lei geral de proteção de dados: principais aspectos e impactos de sua vigência. **Anais UniCathedral-Eventos**, n. 1, p.1-17, 2019.

MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S. A. **Handbook of applied cryptography.** Boca Raton: CRC Press, 1996.

MILLER, L. **IoT Security for Dummies**. Gret Britain: John Wiley & Sons, Ltd., 2016.

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

MORAES, A. F. De. **Segurança em Redes: Fundamentos**. São Paulo: Érica, 2010.

NOBRE, J.; LOPES, R.; GOMES, M.; OLIVEIRA, N. de. **Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd).** Revista Eletrônica de Iniciação Científica em Computação, v. 17, n. 4, 2019.

OLIVEIRA, M. S. et. al. Aplicação das normas abnt nbr iso/iec 27001 e abnt nbr iso/iec 27002 em uma média empresa. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, v. 6, n. 2, 2016.

OWASP (Open Web Application Security Project, 2018). **OWASP Internet of Things Project, 2018.** Disponível em: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main. Acesso em: 22 set. 2022

REPINOSKI, B. C.; MORÃES, M. J. F. A implementaçao da iso/iec 27002 em uma empresa. **Anais do EVINCI-UniBrasil**, v. 3, n. 1, p. 328-328, 2017.

RIBEIRO, A. J. J. **Problemas de Segurança na Internet das Coisas**. Leiria: IPL, 2021. Tese (Mestrado em Cibersegurança e Informática Forense). Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria, 2021.

ROSNER, G. **Privacy and The Internet of Things.** 1 Ed. Califórnia: O'Reilly Media Inc., 2016.

SANTOS, I. M. F. d. **Uma proposta de governança de dados baseada em um método de desenvolvimento de arquitetura empresarial.** Rio de Janeiro: UNIRIO, Dissertação (Mestrado em Informática), Universidade Federal do Estado do Rio de Janeiro, 2010.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva.** Ed. 2, Rio de Janeiro: Elsevier, 2014.

SHELBY, Z.; BORMANN, C. **6LoWPAN: The wireless embedded Internet.** London: John Wiley & Sons, 2011.

SOLOVE, D. J. Understanding privacy. **GWU Legal Studies Research Paper**, n. 420, p. 1-24, 2008.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas.** Ed. 6, São Paulo: Pearson Education, 2015.

TIBCO Software Inc. 2022. **O que é a Internet das Coisas (IoT).** Disponível em: https://www.tibco.com/pt-br/reference-center/what-is-the-internet-of-things-iot. Acesso em: 26 ago. 2022.

TONEZER, G; ZEM, J. **Segurança em internet das coisas.** 2017.

TREINTA, F. T. et al. Metodologia de pesquisa bibliográfica com a utilização de método multicritério de apoio à decisão. **Production**, v. 24, n.3, p. 508-520, 2014.

VALENTE, B. A. L. **Um middleware para a Internet das coisas.** Lisboa: ULISBOA, 2011. Tese (Mestrado em Informática). Faculdade de Ciências, Universidade de Lisboa.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. **Harvard law review**, v. 4, n. 5, 1890.

ZHANG, J.; YE, L. The internet of things and personal privacy protection. **In: ICLEM 2010: Logistics For Sustained Economic Development: Infrastructure, Information, Integration.** p. 2892-2898, 2010.