INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO - CAMPUS FLORESTA
CURSO DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

ELDER FRANKLIN DA SILVA GOMES

SEGURANÇA DE REDES: BOAS PRÁTICAS E MECANISMOS DE SEGURANÇA PARA DISPOSITIVOS CONECTADOS À IOT (INTERNET OF THING).

Floresta-PE, 2018

ELDER FRANKLIN DA SILVA GOMES

SEGURANÇA DE REDES: BOAS PRÁTICAS E MECANISMOS DE SEGURANÇA PARA DISPOSITIVOS CONECTADOS À IOT (INTERNET OF THING).

Trabalho de Conclusão de Curso apresentado ao Curso de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta, como requisito parcial à obtenção do grau de Tecnólogo.

Orientador (a): Prof. Elismar Moraes dos Santos

Floresta-PE, 2018

Dados Internacionais de Catalogação na Publicação (CIP)

G633s Gomes, Elder Franklin da Silva

Segurança de redes: boas práticas e mecanismos de segurança para dispositivos conectados a IOT (Internet of Thing). / Elder Franklin da Silva Gomes - Floresta, 2018.

66 f. il.

Orientador: Elismar Moraes dos Santos.
Trabalho de Conclusão de Curso – Tecnólogo em Gestão da Tecnologia da Informação Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta.

1. Segurança da informação. 2. Internet of things (IoT). 3. Dispositivos conectados . 4. Práticas e mecanismos de segurança . 5. Segurança de redes.

I. Santos, Elismar Moraes dos . II. Título.

CDD: 004.65

Elaborada pela bibliotecária Ednaene de Menezes CRB4/2133

ELDER FRANKLIN DA SILVA GOMES

SEGURANÇA DE REDES: BOAS PRÁTICAS E MECANISMOS DE SEGURANÇA PARA DISPOSITIVOS CONECTADOS À IOT (INTERNET OF THING).

Aprovado em: __ / __ / ____

Nota: _____

BANCA EXAMINADORA

Elismar Moraes dos Santos – Orientador

Instituto Federal do Sertão Pernambucano – Campus Floresta

Ana Patrícia Vargas Borges – Avaliador

Instituto Federal do Sertão Pernambucano – Campus Floresta

Severino do Ramo de Paiva – Avaliador

Instituto Federal do Sertão Pernambucano – Campus Floresta

AGRADECIMENTOS

Agradeço primeiramente a Deus pela saúde e força que me deu durante todos os anos até a final da graduação em Gestão da Tecnologia da informação. Também a minha família que foi a peça fundamental de incentivos para iniciar o curso e chegar até aqui, em especial a minha mãe que infelizmente não está mais presente fisicamente entre nós, mas tenho certeza que me guiou durante todo o curso, a meus amigos e colegas, que sempre me incentivaram nessa jornada que não foi fácil.

Quero agradecer a todos os professores do IF SERTÃO que se dedicaram a cada dia em me ensinar seus conhecimentos, a desenvolver todas as minhas habilidades, onde foi de grande importância durante minha formação e carreira no mercado de trabalho. Agradeço ao professor Elismar Moraes por ter aceitado ser meu orientador, por ter me incentivado, por ter compartilhado todo o conhecimento e ensinamentos, por ser sempre paciente e companheiro. E por fim, agradecer a todos aqueles que contribuíram de forma direta ou indireta. Muito obrigado!

"As portas da oportunidade são amplas. Não digas que não pudestes entrar por elas se nada fizeste para isso."

(O. S. Mardem)

DEDICATÓRIA

Dedico este trabalho em especial à minha mãe Vilanir, que infelizmente não está mais presente entre nós; à minha madrinha Pricila por sempre estar presente nos momentos difíceis; à minha noiva Jandaira pelo companheirismo, ao meu Pai Evanir, meus irmãos Eric e Ênio; aos demais familiares, aos meus amigos, e a todos aqueles que estiveram comigo e dedicaram seu tempo para que eu chegasse até o fim do curso. Também a todos os meus professores pelos esforços diariamente.

RESUMO

Ao longo dos anos, a evolução tecnológica tornou a vida menos complexa quando se trata de atividades cotidianas, tanto para empresas quanto para indivíduos. As inúmeras vantagens que a internet oferece hoje são surpreendentes, como facilidade para realizar transferências e pagamentos, cursos à distância, realizar compras e vendas e outros serviços ligados a ela. Todas essas vantagens fazem com que o nosso tempo se multiplique, devido à realização de certas atividades com um simples clique em um smartphone, por exemplo. Com o aperfeiçoamento e o aumento de dispositivos IoT (Internet of Things), tudo que já é fácil tende a ficar mais fácil ainda, porém se a IoT vai facilitar ainda mais nossas tarefas diárias, é provável que aumente o número de usuários mal-intencionados em busca de vulnerabilidades que surgirão na rede desses dispositivos. Com isso, o provável aumento de "ataques" virtuais com o uso da IoT se tornará um grande problema para a área de segurança. Assim, o presente trabalho de abordagem descritiva visa discutir a importância de se possuir uma rede segura quando falamos em internet das coisas, apresentando as práticas de segurança a serem utilizadas e mecanismos disponíveis que possa ajudar a tornar essa tecnologia mais segura.

Palavra-chave: Segurança de redes, Segurança da Informação, Internet of Things (IoT), dispositivos conectados, práticas e mecanismos de segurança.

ABSTRACT

Throughout the years, the technological evolution has made life less complex when it is about daily activities, both for companies and individuals. The many advantages that the internet gives nowadays are amazing, such as transfer and payment facilities, distance learning courses, shopping and sales, telepresence and other services connected to the internet causes our time to multiply due to certain activities with a simple click on a smartphone for instance. With all improvement and increase of IoT (Internet of Things) devices worldwide, it is likely to facilitate common activities even more. However, if the IoT is going to facilitate our daily chores, it is possible to increase the number of malicious users looking for vulnerabilities that will emerge on the network devices, so, as a result, the likely increase in virtual "attacks" with the use of IoT is major security issue. Thus, the present work of descriptive approach, aims to discuss the importance of having a secure network when we relate about the Internet of Things, presenting safety practices to be used and available mechanisms that might help to turn this technology safer.

Keyword: Network security, Information security, Internet of Things (IoT), connected devices, Safety practices and mechanisms.

LISTA DE ABREVIATURAS E SIGLAS

ARPANET – Advanced Research Agency Network

CD – Compact Disc

CPU – Central Processing Unit

DDoS – Distributed Denial of Service

DMZ – Demilitarized Zone

DVD – Digital Versatile Disc

GSM – Global System for Mobile Communication

HD – High Definition ou Hard Disk

HIDS – Host-Based Intrusion Detection System

HTTP – Hypertext Transfer Protocol

ICT - Information and Communication Technology

IDS – Intrusion Detection System

iOS – iPhone Operating System

IoT – Internet of Things

IPS – Intrusion Prevention System

IPSec – IP Security

NIDS – Network-Based Intrusion Detection System

NAT – Network Address Translation

RFID - Radio Frequency Identification

SMBV1 – Server Message Block 1.0

SSH – Secure Shell

SSL – Secure Socket Layer

USB – Universal Serial Bus

VPN – Virtual Private Network

WEP – Wired Equivalent Privacy

WWW – World Wide Web

LISTA DE FIGURAS

Sumário

1. INTRODUÇÃO

A área de segurança sempre é um assunto bastante discutido no meio tecnológico, e agora com o crescimento e o aperfeiçoamento da Internet of Things (IoT) ou Internet das Coisas isso não será diferente. Segundo dados da CISCO (2016) em 2020 a internet interconectará 50 bilhões de coisas em todo o mundo, pois a mesma disponibiliza conexões globais que facilitam a navegação na Web, as mídias sociais e aos dispositivos móveis inteligentes, tornando maior a comunicação através da rede.

Com o passar dos anos, as maneiras que são utilizadas para a comunicação evoluem constantemente, antes éramos limitados em interações presenciais e com as inovações tecnológicas, expandimos o alcance de nossas comunicações, como *smartphones*, a televisão e até a telepresença. Isso nos ajudou a aperfeiçoar e facilitar mais e mais a comunicação entre as pessoas.

De acordo com a CISCO (2016), "a rede é a base da Internet". Existem diversos tipos de redes: as simples, conectando dois computadores e as responsáveis por conectar milhões de dispositivos. Na IoT, a quantidade de dispositivos conectados, desde TVs, geladeiras, despertadores, chuveiros e até cafeteiras, tem como missão facilitar mais e mais o nosso dia a dia. Isso é algo a se elogiar, porém, a vulnerabilidade que esses dispositivos podem apresentar não é nada animadora, devido a grande maioria ser conectado por redes sem fios que são consideradas mais vulneráveis que as redes físicas.

Conforme matéria divulgada em 2017 pelo site Olhar Digital, uma empresa de segurança digital da Eslováquia denominada ESET divulgou um relatório que mostra a preocupação da empresa com a segurança dos usuários em relação aos dispositivos conectados. Foi dado como exemplo os hospitais que possuem diversos equipamentos conectados e o tamanho do risco aos usuários a utilizar esses dispositivos. Por exemplo, um dispositivo de marca-passos, cujo objetivo obviamente é a saúde de um indivíduo, logo as informações contidas nele são de extrema

importância, então é necessário que este tipo de dispositivo possua um alto nível de segurança, pois caso seja *hackeado* o marca-passo não pare de funcionar.

Conforme Tanenbaum e Wethereall (2011, p. 516), "a rede sem fio é um sonho que se tornou realidade para o espião". Como os fabricantes procuram desenvolver dispositivos que facilitem a utilização pelo usuário, ao mesmo tempo faz com que aumente a quantidade de pessoas mal-intencionadas em busca de vulnerabilidades para acessar esses tipos de dispositivos, e com isso, começamos a nos perguntar e pensar se realmente essa tecnologia poderá possuir uma segurança adequada para os dias atuais.

Com todos esses dispositivos trocando informações o tempo todo, a demanda pela segurança dos dados tende a ser maior. Então, neste trabalho falo um pouco sobre a segurança da informação, segurança de redes, sobre conceitos da Internet das Coisas, sobre as características da IoT, as necessidades de se ter uma boa segurança, as ameaças que a IoT pode trazer para os usuários, boas práticas e mecanismos para segurança em IoT.

1.1 Justificativa

Hoje em dia é fácil roubar e usar dados sem autorizações. Sendo assim, é bastante natural se preocupar com esse tipo de problema, já que tudo está conectado na IoT. Como a maioria da comunicação dos dispositivos conectados à IoT é através de redes sem fios, o trabalho de um hacker acaba se tornando mais simples que em conexões físicas, então são necessários cuidados redobrados quando falamos em IoT.

A abordagem sobre esse assunto é bastante interessante para a minha área de formação, pois com a quantidade de informações circulando nesses dispositivos conectados à internet, faz com que as pessoas se preocupem mais com a segurança de suas informações, então a tendência é surgir diversas oportunidades no mercado de trabalho voltadas para a área de TI.

O trabalho foi concebido na necessidade de mostrar a importância de se realizar uma boa segurança, conhecendo mecanismos e práticas capazes de ajudar a neutralizar qualquer tipo de ameaças a suas informações e que sem uma boa segurança na sua rede, a tecnologia IoT não passa de uma ferramenta criada para os cibercriminosos.

1.2 Problemática

Com o pouco conhecimento sobre a tecnologia IoT, muitas pessoas imaginam que este tipo de tecnologia nos trará somente benefícios e que não teremos nenhum tipo de problema. Teoricamente, sim, estaremos conectados o tempo todo e resolvendo quase tudo com apenas um clique. Porém, quanto mais dispositivos existem para serem conectados, mais chances deles serem acessados por pessoas mal-intencionadas.

De acordo com a Cert.br, independente do tipo de tecnologia utilizada, qualquer dispositivo que for conectado à rede pode estar sujeito algum tipo de ameaça, como por exemplo:

- **Furto de dados**: com a exploração de vulnerabilidades, informações pessoais e outros tipos de dados podem ser adquiridos;
- **Uso indevidos de recursos**: O *hacker* pode utilizar um dispositivo conectado à rede para realizar atividades maliciosas, como disseminar códigos maliciosos, adquirir arquivos, entre outras atividades indesejáveis;
- **Varredura**: O *hacker* tenta descobrir outros dispositivos conectado à rede para realizar atividades maliciosas em busca de vulnerabilidades para conseguir acesso;
- **Interceptação de tráfego**: O *hacker* pode ter acesso à rede e tentar coletar dados que estejam sendo transmitidos sem o uso da criptografia;
- **Ataque de negação de serviços**: O *hacker* envia grande número de mensagens para um dispositivo com o intuito de tornar o sistema incapaz de se comunicar;

- **Exploração de vulnerabilidades**: Um dispositivo pode ser invadido e passar a ser utilizado para participar de ataques, como: compartilhando códigos maliciosos e redirecionar os usuários para sites fraudulentos, tudo isso sem que o dono saiba que está ocorrendo esse tipo de ataque.
- **Quebra da confidencialidade**: Ocorre quando alguém não autorizado acessa informações sigilosas, seja elas, senhas ou arquivos privados.

Em matéria publicada por Rodrigo Martins, em 2016, no portal Atitude Reflexiva, ele diz que de acordo com a *Proofpoint*, empresa da área de proteção de informações, no período entre dezembro de 2013 e janeiro de 2014, foi realizado o primeiro ataque cibernético com dispositivos inteligentes. Os *hackers* utilizaram mais de cem mil dispositivos, desde geladeiras conectadas à internet até televisores inteligentes, fazendo com que esses dispositivos propagassem mais de setecentos mil *e-mails* com *malwares*. A empresa ainda noticiou que na maioria dos ataques não foram utilizadas nenhuma técnica avançada para tomar o controle desses objetos, sendo eles acessados em redes públicas devido a configurações incorretas e senhas padrão.

Com todas essas ameaças que podem aparecer, surge a dúvida. Quais as práticas e mecanismos importantes a serem utilizados para manter um nível satisfatório de segurança em dispositivos IoT?

1.3 Objetivo Geral

Analisar as melhores práticas e mecanismos de segurança que podem ser utilizados em dispositivos conectados à IoT.

1.3.1 Objetivos Específicos

- ✓ Apresentar conceitos sobre segurança de redes, segurança da informação e sobre Internet of Things (IoT);
- ✓ Listar as principais características da IoT;
- ✓ Apresentar os problemas que podem ocorrer devido as vulnerabilidades de redes na IoT;

- ✓ Identificar as melhores práticas e mecanismos que podem ser utilizados para manter um nível satisfatório de segurança em dispositivos conectados à IoT.

1.4 Metodologia

Segundo Marconi e Lakatos (2010, p. 139), "a pesquisa é um procedimento formal, com método de pensamento reflexivo, que requer um tratamento científico e se constitui no caminho para conhecer a realidade ou para descobrir verdades parciais". A pesquisa realizada neste trabalho é caracterizada como descritiva, pois o seu objetivo é analisar as melhores práticas e mecanismos de segurança que podem ser utilizados para proteger as informações que circulam em dispositivos conectados à internet contra ameaças na rede.

De acordo com Marconi e Lakatos (2010), o desenvolvimento de um projeto de pesquisa compreende seis passos:

- Seleção do tópico ou problema para investigação;
- Definição e diferenciação do problema;
- Levantamento de hipóteses de trabalho;
- Coleta, sistematização e classificação dos dados;
- Análise e interpretação dos dados;
- Relatório do resultado da pesquisa.

Conforme Marconi e Lakatos (2010, p. 65),

> O método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo, conhecimentos válidos e verdadeiros, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista.

Na pesquisa bibliográfica são utilizadas informações que já foram trabalhadas e registradas por outros autores, com isso, ela é a base da pesquisa descritiva. De acordo com Severino (2007, p. 122), a pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses etc.

Uma das principais maneiras utilizadas para a realização do trabalho foi a pesquisa bibliográfica e análise sobre o tema. Através da utilização de diversos meios, como livros adquiridos na biblioteca do IF Sertão-PE-Campus Floresta, em artigos, e principalmente em sites como o Google acadêmico, CERT.br (Centro de Estudos, Respostas e Tratamento de Segurança no Brasil), Kaspersky Lab, que é uma empresa bastante conceituada na área de segurança virtual, CISCO Networking Academy, programa criado em 1997 pela própria CISCO que busca desenvolver habilidades profissionais e carreiras no setor de TI, e entre outros sites de tecnologia. Só assim foi possível colher fundamentos científicos para chegar ao objetivo proposto no trabalho.

Severino (2007, p. 13) diz o seguinte sobre a utilização da Internet como fonte de pesquisa:

> A internet, rede mundial de computadores, tornou-se uma indispensável fonte de pesquisa para os diversos campos de conhecimentos. Isso porque representa hoje um extraordinário acervo de dados que está colocado à disposição de todos os interessados, e que pode ser acessado com extrema facilidade por todos eles, graças à sofisticação dos atuais recursos informacionais e comunicacionais acessíveis no mundo.

Do ponto de vista da análise dos dados, a pesquisa realizada neste trabalho pode ser classificada como qualitativa, pois foi realizada através do conhecimento desenvolvido com base em dados bibliográficos e com isso foi possível adquirir conceitos básicos sobre segurança de redes, segurança da informação e sobre Internet das Coisas.

Depois da coleta de informações, foi descrito quais as práticas e mecanismos de segurança que podem ser utilizados na busca de uma segurança satisfatória em redes de dispositivos IoT.

2. FUNDAMENTAÇÃO TEÓRICA

Nesta seção são apresentados os capítulos que fundamentam esta pesquisa a respeito de segurança da informação, de rede e conceitos relacionados a Internet das Coisas, que servem de base para o desenvolvimento deste trabalho.

2.1 Segurança da Informação

Devido ao crescimento constante da internet, a troca de informações entre dispositivos vem aumentando cada vez mais. Com isso, empresas e indivíduos passaram a se preocupar mais com a segurança de suas informações, devido a elas estarem cada vez mais disponíveis em meios eletrônicos.

> A segurança da informação diz respeito à proteção de dados, informações, sistemas e demais ativos de uma organização, contra erros, desastres e manipulação não autorizada, de modo a minimizar os riscos e impactos de possíveis incidentes, com o intuito de proteger os valores que esses ativos possuem para uma empresa ou indivíduo (Paiva, 2017, p. 22).

Para que a segurança da informação possa funcionar perfeitamente, é necessário estabelecer alguns níveis de segurança para depois iniciar a implementação dos controles mais adequados.

Conforme Nakamura (2007, p. 51), "apesar da segurança ser, atualmente, essencial para os negócios das organizações, a dificuldade em entender sua importância ainda é muito grande. Muitas vezes, a única segurança existente é a obscuridade".

De acordo com Paiva (2017), a Confidencialidade, Integridade, Disponibilidade e Autenticidade são os pilares da segurança da informação e que se um ou mais não forem respeitados a informação da organização será comprometida. Segue abaixo um pouco sobre esses princípios.

2.1.1 Confidencialidade

A confidencialidade é utilizada para garantir que as informações só sejam acessadas por pessoas que forem autorizadas, ou seja, se por acaso alguém não autorizado acessar de forma intencional ou não informações, seja elas, senhas ou documentos privados, isso se torna um incidente da segurança da informação por quebra de confidencialidade (PAIVA, 2017).

Conforme Paiva (2017, p.25), "o princípio da confidencialidade, visa garantir o resguardo das informações para que não sejam acessadas por pessoas ou entidades não autorizadas para tal ação".

Para que a confidencialidade das informações disponíveis em computadores ou dispositivos tenha um nível de segurança apropriado, é necessário que principalmente os usuários que possuem acesso a essas informações tenham conhecimentos suficientes para compreender quais os dados podem ser expostos e quais são os sigilosos.

2.1.2 Integridade

A Integridade tem como papel garantir a confiabilidade das informações transmitidas de uma organização ou pessoa, ou seja, ninguém sem autorização pode alterá-las. A integridade em uma empresa é fundamental, pois para esta se manter competitiva é necessário que as pessoas a vejam como confiável; então é preciso garantir que as informações acessadas estejam corretas, sem alterações indevidas e, assim, a integridade das informações é indispensável (PAIVA, 2017).

De acordo com Paiva (2017, p. 26),

> O princípio da integridade visa garantir que as informações acessadas ou enviadas pelos sistemas de comunicação, de uma determinada empresa ou indivíduo, permanecerão completas e sem alterações indevidas, gerando confiabilidade para quem tem domínio sobre tal informação.

Em empresas a quebra da integridade é causada quando uma informação é alterada propositalmente, ou seja, por usuários internos ou externos a organização.

> A falsificação de um documento, alteração de registros em um banco de dados ou qualquer ação que resulte numa alteração da informação original de maneira indevida, é considerado uma quebra de integridade no contexto de segurança da informação (Paiva, 2017, p. 27).

2.1.3 Disponibilidade

A disponibilidade visa garantir que as informações sempre estejam à disposição quando um indivíduo precisar acessá-las. Segundo Paiva (2017), dos quatros pilares da segurança da informação, podemos dizer que a disponibilidade é umas das mais importantes para a parte operacional de uma empresa. Hoje em dia todas as empresas trabalham com trocas constates de informações, então, caso alguma informação estiver indisponível, o processo posterior pode ser afetado.

Para manter a disponibilidade das informações, é necessário criar algumas práticas, como: realização de *Backups*, possuir equipamentos para reposições, entre outras maneiras.

2.1.4 Autenticidade

Segundo Paiva (2007, p. 29), "a autenticidade visa garantir a identidade de uma pessoa ou órgão que prestou, alterou ou descartou uma determinada informação". Isto porque a autenticidade visa e garante que uma certa informação foi desenvolvida, modificada ou excluída por uma empresa, sistema ou indivíduo. Sendo assim, ela consequentemente está relacionada ao princípio da integridade.

Para que exista segurança de informações em redes de computadores, é necessário que sejam utilizadas a assinatura e o certificado digital, pois isto deixa claro se o emissor ou o receptor é realmente quem diz ser, estabelecendo assim uma comunicação segura (PAIVA, 2017).

2.2 Segurança de Redes

Rede de computadores é um conjunto de computadores e dispositivo de computação interconectados que trocam informações entre si, facilitando assim a comunicação entre diversos usuários (TANEMBAUM; WENTHEREALL, 2011).

Para manter a comunicação de redes segura, é necessário a existência de uma boa segurança de redes. A segurança de redes visa proteger a rede contra problemas na usabilidade e na integridade de suas conexões e dados através da utilização de várias camadas de segurança em conjunto, como: Políticas de segurança, *Firewall*, ferramentas de IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*), ferramentas de Criptografia, entre outras.

Em uma rede sem fio, a segurança acaba se tornando um pouco mais complexa em relação a uma conexão com fio, pois de acordo com o alcance de um *Wi-Fi,* qualquer pessoa pode ter um fácil acesso a essa rede. Abaixo seguem alguns pontos básicos que podem ser utilizados em busca da segurança de redes sem fio; porém há que se destacar que mesmo utilizando essas configurações, os dispositivos sem fio podem ser facilmente acessados por indivíduos mal-intencionados com habilidades de *hacking* (CISCO, 2016):

- Protocolos de autenticação fortes com senhas fortes;
- Configuração da segurança administrativa;
- Alterar todas as configurações padrão;
- Sempre manter atualizado o *firmware*.

É preciso ter em mente que, com o aumento da conectividade por causa da Internet das Coisas, os ataques têm mais possibilidade de acontecer. Atzori *et. al.,* (2010), *apud* Jamil *at. al.,* (2016), dizem o seguinte em relação a segurança dos dispositivos conectados à IoT, que em muitas vezes, os componentes conectados a IoT passam maior parte do tempo sem vigilância tornando-os alvos fáceis e a maior parte das comunicações serão sem fio, o que torna a espionagem mais simples.

Existem tipos de vulnerabilidades em alguns dispositivos que muitas vezes podem facilmente serem evitadas pelos fabricantes. Entretanto, de acordo com Nakamura (2007, p. 47), "muitas organizações estão mais interessadas em finalizar rapidamente os seus produtos para colocá-los no mercado antes de seus concorrentes". Isso faz com que vários produtos apresentem falhas com pouco tempo de uso.

Para as empresas, os recursos que são disponibilizados pelas redes facilitam uma maior produtividade e criação de novos produtos e serviços, aumentando consequentemente o lucro da organização. Devido a isso, muitas empresas têm a preocupação em fornecer os produtos rápidos em vez de produtos com qualidade, trazendo assim, problemas para o usuário final.

2.3 *Internet of Things* (IoT)

Imagine um mundo com bilhões de objetos conectados, se comunicando e trocando informações a todo instante e em qualquer lugar que você ande. Isso começou desde o período da Guerra Fria nos anos 60, onde tivemos um pequeno surgimento da internet, que levou o nome de ARPANET (*Advanced Research Projects Agency Network*). Inicialmente a ARPANET foi utilizada para fins militares, onde os mesmos usavam para se comunicarem, caso houvesse ataque inimigo. Porém, foi no ano de 1990, na Suíça, que a Internet começou a se popularizar. O Britânico Berners-Lee desenvolveu um sistema de documentos com acesso a informações exibidas no formato de hipertexto, ou seja, textos em formato digital. Esse acesso passou a ser chamado de WWW (*World Wide Web*) que possibilitava a criação de sites mais dinâmicos, onde se deu início a uma nova era da tecnologia (MARTINS, 2008).

Para Tanenbaum (2003, p. 54) a internet é definida da seguinte forma: "A internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns".

O avanço constante da internet permite a comunicação e a facilidade para a troca de informações entre pessoas e as coisas e as coisas entre elas próprias, tornando

cada vez mais frequente essa comunicação. Essa interação entre diversos objetos conectados à rede, recebe o nome de *Internet of Things* (IoT).

Segundo Rajput *et al.* (2016, p. 451), "a Internet das Coisas (IoT), é uma tecnologia de fácil crescimento e fácil de se usar, que permite que tudo seja conectado e também permite a comunicação efetiva entre as "coisas" conectadas.

Para Patel *et al.* (2016, p. 6122), a internet não é mais apenas uma rede de computadores e sim uma rede de dispositivos de todos os tipos e tamanhos, como: veículos, telefones inteligentes, brinquedos, eletrodomésticos e todos os objetos que possam se conectar.

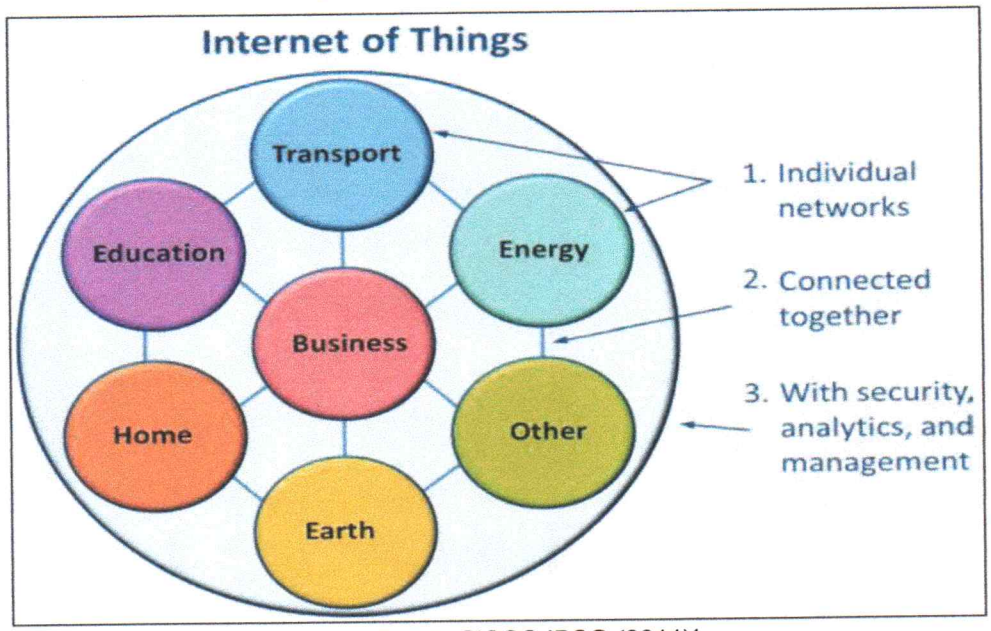
> A Internet das coisas é um conceito e um paradigma que considera presença difundida no ambiente de uma variedade de coisas/objetos que através de conexões sem fio e com fio e esquemas de endereçamento únicos são capazes de interagir uns com os outros e cooperar com outras coisas/objetos para criar novos aplicativos/serviços e alcançar objetivos comuns (Patel *et al.* 2016, p. 6122).

Para muitos, a internet revolucionou a tecnologia, porém a IoT pode chegar mais além. Conforme Madakam *et al.* (2015, p. 166), "a IoT é uma revolução tecnológica que representa o futuro da computação e da comunicação, e seu desenvolvimento depende de inovação em vários campos importantes, desde sensores sem fio até a nanotecnologia".

De acordo com Patel *et al.* (2016, p. 6122) "a Internet das Coisas é uma nova revolução da Internet. Os objetos se tornam reconhecíveis e obtêm inteligência ao tomar decisões relacionadas ao contexto, isso graças ao fato de poderem comunicar informações sobre si mesmos".

Com tudo isso, a IoT pode vir a ser uma revolução na comunicação, sendo que qualquer coisa que esteja conectada em algum tipo de rede, seja ela pública ou privada, estará trocando informações em tempo real. Na Figura 1 podemos ver a apresentação da IoT como uma rede de redes.

Figura 1 - IoT como uma rede de redes



Fonte: CISCO IBSG (2011)[1].

Segundo Pandikumar *et al.*, (2014), *apud* Jamil, (2016), a arquitetura da IoT é uma convergência de várias tecnologias como: *Ubiquitous*/computação pervasiva, sensores/atuadores, tecnologias de comunicação e informação (ICT) e sistemas embarcados.

Computação pervasiva apoia a criação de sistemas distribuídos fazendo com que os espaços físicos se transformem em ambientes de computação inteligentes. ICT, computação pervasiva e protocolos de Internet são responsáveis por gerenciar as interações dos usuários com os dispositivos (JAMIL, 2016).

A tecnologia RFID é um sistema de identificação por rádio frequência e pode ser bastante útil para a IoT, o mesmo pode ser utilizado para controlar os objetos conectados à Internet. Conforme Kadlec *et al.*, (2014), *apud* Jamil (2016), RFID (Radio

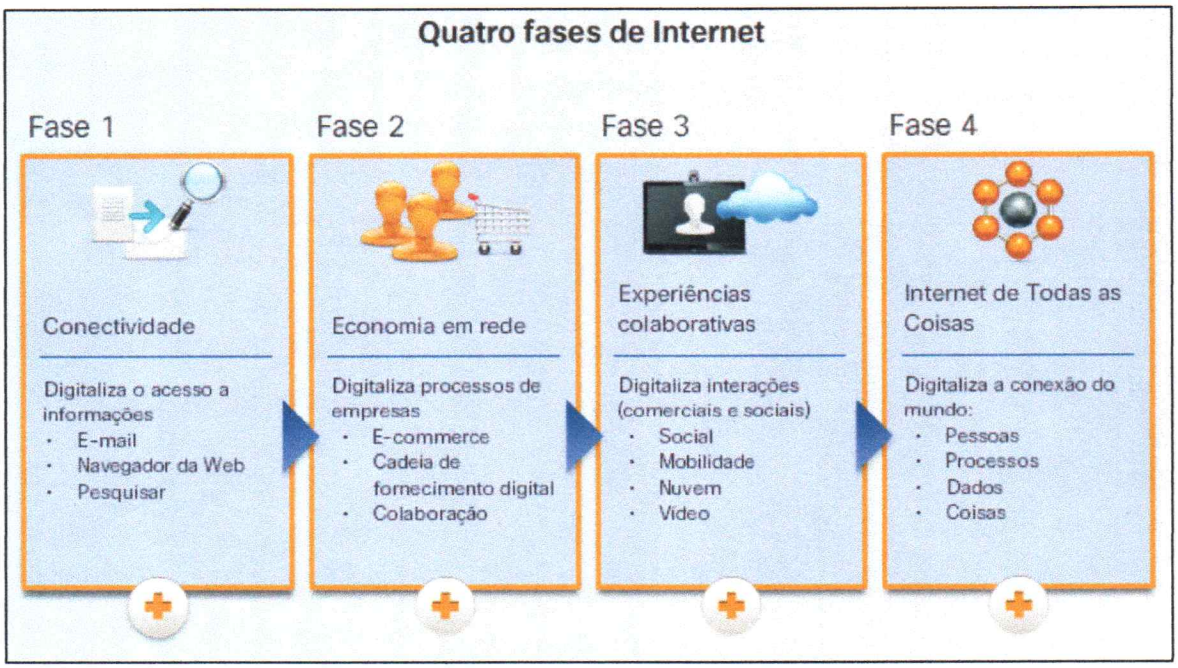
---

[1]Disponível em: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf.

Frequency Identification) é uma tecnologia para a Internet das Coisas e pode ser utilizado para identificar e controlar seus equipamentos.

A CISCO (2016) diz que a internet durante seu avanço realizou quatro fases distintas, e a cada evolução o efeito da internet nos negócios e na sociedade era maior. Abaixo, na Figura 2, podemos visualizar as quatro fases da internet.

Figura 2 - As quatro fases da Internet



Fonte: CISCO Networking Academy (2016)[2].

Após alguns anos com a evolução constante da Internet, entramos na quarta fase, a fase da Internet de Todas as Coisas (do inglês *Internet of Everything* (IoE), onde podemos afirmar que essa internet é formada não só pelas coisas, mas também por pessoas, processos e dados (CISCO, 2016).

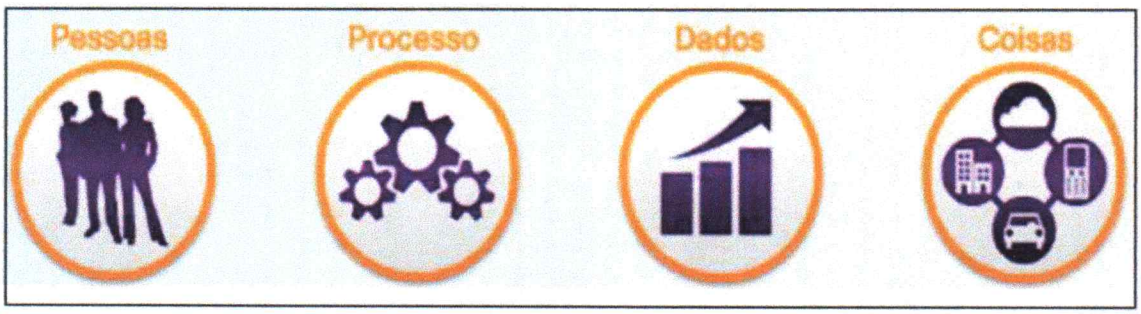
Conforme a CISCO (2016), a IoE é considerada a evolução da IoT devido a ser formada por coisas, pessoas, processos e dados. Porém, segundo Patel *et al.* (2016, p. 6122), a IoT também é formada por coisas, pessoas, processos e dados, pois ela

[2] Disponível em: https://www.netacad.com.

está dividida em três conexões, são elas: Pessoas para pessoas, Pessoas para máquina e Máquina para máquina.

Na Figura 3, podemos visualizar os quatros pilares da IoT que, segundo a Cisco (2016), são importantes para a evolução das conexões de redes.

Figura 3 - Os quatros pilares da IoT



Fonte: CISCO Networking Academy (2016)[3].

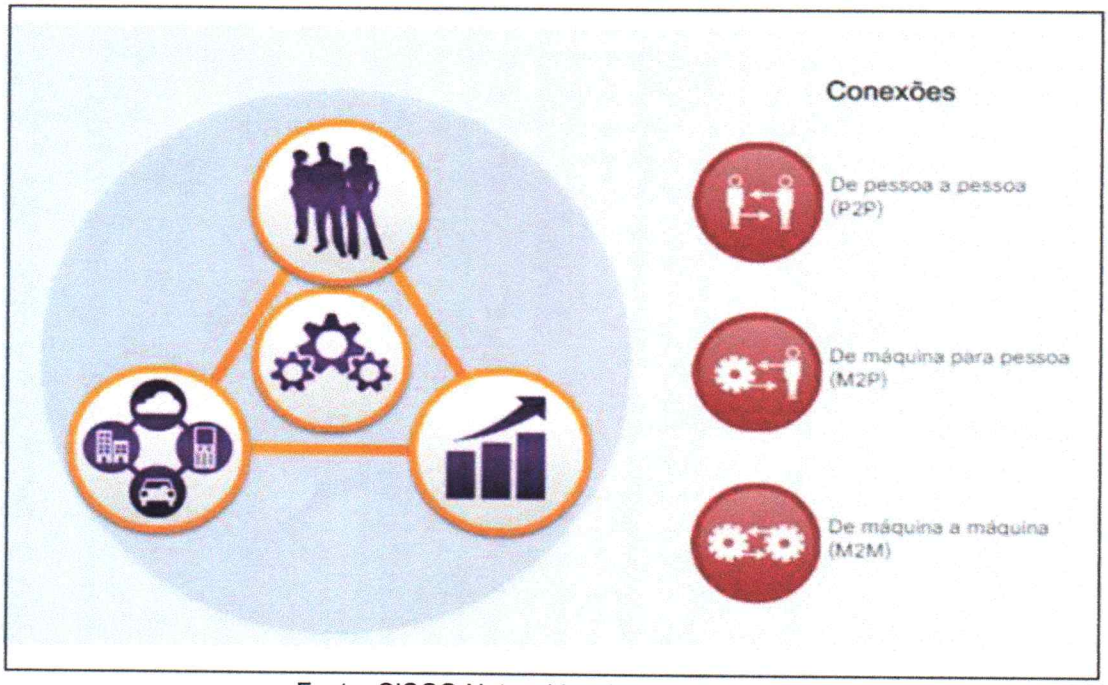
- **Pessoas –** Hoje em dia todos nós nos conectamos através de dispositivos com acesso à internet. De acordo com a evolução da internet, iremos nos conectar das mais diversas maneiras. Atualmente os dispositivos conhecidos como "*wearable*", ou seja, pulseiras, relógios, óculos de realidade virtual, já estão mudando a forma da comunicação.
- **Processos –** São os que ocorrem entre todos os pilares. Se forem realizados os processos corretamente, as conexões serão melhores e farão com que as informações sejam transmitidas da melhor forma possível e no momento correto para a pessoa certa.
- **Dados –** São as informações geradas por pessoas e coisas. Os dados são analisados e passam a oferecer as melhores informações para as pessoas e máquinas, alcançado os melhores resultados e tomando as melhores decisões.
- **Coisas –** São os objetos físicos que estão conectados à internet e entre outras coisas. Esses objetos estão coletando e monitorando dados com

[3] Disponível em: https://www.netacad.com.

reconhecimento de contexto e fornecendo as informações necessárias para ajudar as pessoas e máquinas.

Na Figura 4 podemos observar as conexões que são criadas pelos quatros pilares da IoT.

Figura 4 - Conexões da IoT



Fonte: CISCO Networking Academy (2016)[4].

2.3.1 Características da IoT

Quando ouvimos falar em IoT, logo imaginamos que a sua principal função é conectar tudo que se possa imaginar. Conforme Patel *et al.* (2016, p. 6122), a principal característica da IoT é: "permitir que as "coisas" sejam conectadas a qualquer momento, em qualquer lugar, com qualquer coisa usando qualquer caminho ou rede e qualquer serviço". Essa principal característica pode ser difundida em várias

[4] Disponível em: https://www.netacad.com.

características fundamentais da IoT que serão apresentadas a seguir (PATEL *et al.*, 2016, p. 6123).

Interconectividade: No contexto IoT, qualquer objeto pode se conectar com a estrutura global de informação e comunicação.

Serviços relacionados a coisas: A IoT fornece serviços relacionados a coisas, como proteção de privacidade entre coisas físicas e virtuais. Para que esses serviços possam ser fornecidos, tanto as tecnologias físicas quanto virtuais mudarão.

Diversificada: Com base em várias plataformas e redes de *hardware* diferentes, os dispositivos da IoT podem interagir com diversos dispositivos de redes diferentes.

Alterações dinâmicas: A situação dos dispositivos altera dinamicamente, ou seja, conectar e/ou desconectar, dormir e acordar entre outras alterações.

Grande escala: A quantidade de dispositivos que precisa ser gerenciado e que trocam informações entre si será muito maior que os conectados à internet na atualidade.

Segurança: Da mesma maneira que podemos obter benefícios com a IoT, a nossa segurança pode ser comprometida. Então, devemos nos assegurar que os nossos dados pessoais e a nossa segurança física possam estar sempre bem protegidos.

Conectividade: A conectividade permite acessibilidade e compatibilidade de rede, ou seja, a acessibilidade tem o papel de receber do servidor e passar a melhor experiência para o usuário; já a compatibilidade fornece a capacidade de utilizar e produzir dados.

Com o aperfeiçoamento da IoT, a tendência é que as características evoluam cada vez mais, tornando o uso dos dispositivos inteligentes cada vez mais práticos e eficientes sem que ocorram grandes problemas.

3. IOT NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

3.1 Por que se preocupar com a segurança na IoT?

A segurança sempre será um fator essencial em qualquer setor existente, seja ela física ou virtual. Conforme a CERT.br, é necessário termos cuidados com o uso da Internet da mesma forma como temos quando vamos ao banco, vamos fazer compras em lojas, passar informações para estranhos, entre outros cuidados. Com a IoT a segurança deve ser levada muito a sério desde o fabricante até chegar ao ponto final, seja empresa ou indivíduo, pois a enorme quantidade de informações circulando nessas redes são como chaves de acesso para os usuários mal-intencionados.

Conforme Paiva (2017, p. 53),

> As ameaças podem ser definidas como um evento ou atitudes que sejam indesejáveis que possam acarretar algum problema desabilitando, danificando ou até mesmo destruindo um recurso, comprometendo a missão das empresas e atingindo os ativos que a organização possui, quase sempre, causando prejuízos.

A cada avanço na tecnologia surge o aumento de vulnerabilidades em sistemas, dispositivos, computadores e tudo que possa se conectar a internet também aumenta; isso acontece devido a já existência ou surgimento de novos métodos e ferramentas com a missão de acessar, sem autorizações, informações sigilosas, buscando prejudicar os usuários atacados.

3.1.1 Métodos e ferramentas de ataques

Pessoas mal-intencionadas estão presentes em todos os lugares possíveis, porém na internet das coisas os ataques podem ocorrer frequentemente e de diversas maneiras. Segundo Paiva (2017), existem diversos métodos e ferramentas utilizadas para invadir sistemas, seguindo abaixo algumas delas:

3.1.1.1 Vírus

Os vírus são programas criados com a missão de trazer problemas para um sistema; ou seja, o vírus é um agente que tem a capacidade de contaminar redes de dispositivos ou computadores, causando problemas no funcionamento de máquinas de empresas ou de algum indivíduo (PAIVA, 2017).

Os vírus podem apresentar diversas características no uso de computadores ou dispositivos, como por exemplo, lentidão na utilização do aparelho devido ao vírus espalhar cópias de si mesmo em vários programas e arquivos, podendo até causar perda total em alguns desses arquivos infectados.

Devido ao avanço da internet, a utilização de *e-mails* e outros tipos de comunicações faz com que os computadores ou dispositivos possam facilmente serem infectados por algum tipo de vírus, como podemos ver abaixo (PAIVA, 2017).

Vermes/*Worms* – Esse tipo de vírus não precisa de programas ou arquivos para se espalhar, ou seja, sua multiplicação se dá pelo fato da existência de falhas ou alguma vulnerabilidade nos *softwares* dos computadores. Paiva (2017, p. 56) diz, "*Worm* é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador".

Spyware – Esses tipos de programas entram no computador de forma silenciosa, com o objetivo de monitorar as atividades do computador. Ele está dividido em: ***Keylogger,*** que é uma ferramenta com a missão de copiar o que está sendo digitado, ***Screenlogger,*** capaz também de copiar o que está sendo digitado em teclados virtuais, e ***Adware,*** que são propagandas com a missão de levar os usuários para páginas falsas (PAIVA, 2017).

***Trojan* (Cavalos de Tróia)** – Esse tipo de *malware* é sempre baixado sem que o usuário possa perceber, pois sempre ficam alojados em processos simples do dia a dia com intuito de alterar o sistema e gerar algum tipo de vulnerabilidade para que ocorra um ataque ao computador. Conforme LAUFER *et al.*, (2013) *apud* PAIVA,

(2017), "alguns cavalos de Tróia podem criar "portas dos fundos" (*backdoors*) para liberar o acesso ao computador para usuários maliciosos executarem comandos remotamente, possivelmente permitindo que informações seja obtida".

Backdoors – São programas com a missão de garantir um fácil acesso ao computador infectado, ou seja, faz com que não seja necessário a utilização de técnicas de invasão novamente, caso o invasor deseje retornar aos computadores infectados anteriormente (PAIVA, 2017).

Ransomware – Esse tipo de ataque sempre acontece através da internet; o mesmo é conhecido como sequestro de dados, pois, ao roubar informações, os *hackers* solicitam uma certa quantia para que seja feita a devolução das informações roubadas. De acordo com Paiva (2017), esses ataques geralmente são realizados em organizações, pois a mesma possui informações importantes, e dependendo dos arquivos roubados os usuários irão pagar bem para conseguir de volta. Em 2017, um tipo de *ransonware* que ficou bastante conhecido por ter se espalhado rapidamente em diversas empresas, foi o *WannaCry*.

> A diferença entre os ataques anteriores do *WannaCry* e o último é um componente semelhante a um verme que infecta outros computadores explorando uma vulnerabilidade crítica de execução remota de código na implementação do protocolo *Server Message Block* 1.0 (SMBv1) do *Windows* (DG News Service, 2017 *apud* PAIVA, 2017).

3.1.1.2 *Spoofing*

O *spoofing* é uma técnica utilizada para acessar um sistema através de uma identidade falsa, sendo possível somente com a utilização de um IP falso ou dados roubados. Depois de conseguir o acesso ao sistema através de um IP falso ou de um legitimo o ataque a arquivos e pastas sigilosas começa (PAIVA, 2017).

3.1.1.3 *Repudiation*

O *repudiation* é um ataque difícil de ser detectado, o mesmo é utilizado para negar que um usuário invasor ou não tenha feito algum tipo de execução ou transação

especifica e que sem uma auditoria adequada é quase impossível de provar que o sistema foi acessado (PAIVA, 2017).

3.1.1.4 *DdoS (Distributed Denial of Service)*

O ataque DdoS é bastante semelhante ao DoS, pois busca sobrecarregar um computador tornando seu sistema indisponível. Diferente do DoS, o DdoS dificulta qualquer tipo de ação de defesa, pois seu ataque parte de diversos lugares ao mesmo tempo. Segundo Stallings (2008, p. 440), "a primeira etapa em um ataque de DDoS é o atacante infectar diversas máquinas com *software* zumbi que, por fim, serão usadas para executar o ataque".

De acordo com Stallings (2008), segue abaixo os ingredientes essenciais da primeira etapa de um ataque de DDoS:

- *Software* capaz de realizar o ataque DDoS. O *software* tem que ser capaz de ser executados em diversas máquinas, ocultar a sua presença e de se comunicar com o atacante;
- Vulnerabilidades em sistemas. É preciso o atacante conhecer algum tipo de vulnerabilidade que ainda não foi corrigida no sistema para que seja possível instalar o *software* zumbi;
- Realizar o processo de varredura para localizar máquinas vulneráveis.

3.1.2 A Internet das Coisas pode ser uma ameaça?

A cada ano o aumento de "coisas" conectadas no mundo traz consigo a evolução da tecnologia e a praticidade para o dia a dia da sociedade, ou seja, eleva a qualidade de vida das pessoas e faz com que organizações possam melhorar seus negócios. Porém, a segurança na IoT passa a ser complexa devido a esse grande número de possibilidades de ameaças disponíveis em um ambiente totalmente conectado; para os *hackers* quanto mais aparelhos disponíveis em uma rede, maiores serão as chances de ataques.

Hoje em dia, a utilização dos dispositivos inteligentes para realizar ataques de DDoS é um dos caminhos mais atraente para os *hackers*. Em 2017, um ataque que levou o nome de "*botnet Mirai*" derrubou mais de 80 sites e serviços online no mundo. Isso ocorreu com a utilização de milhares de dispositivos conectados a internet, e o que mais chamou atenção nesse ataque foi a facilidade que os *hackers* tiveram para dominar esses dispositivos, pois não houve uso de técnicas sofisticadas e nem de tecnologia moderna.

De acordo com uma matéria publicada por Altieres Rohr, em 2017, no site G1, a CERT.br, Centro de Estudos, Respostas e Tratamento de Segurança no Brasil, divulgou um aumento de 138% dos relatos de ataques DDoS no brasil, sendo câmeras de vigilância e gravadores digitais uns dos mais atacados.

Os ataques de *botnets* são apenas alguns no meio da IoT. Imagine o que pode vir a acontecer caso ocorra algum tipo de ataque de *ransomware* nesses dispositivos, como por exemplo, se um *ransomware* infectar o sistema de um carro, as consequências podem ser enormes, desde travamento de portas, ligar e desligar o motor, até desativar os freios com o carro em movimento. Então, esse tipo de ataque acaba preocupando até a segurança física dos usuários.

Em janeiro de 2018, a *Kaspersky Lab*, empresa internacional de segurança virtual, divulgou em seu portal que foram realizados diversos testes em dispositivos inteligentes, dos quais os resultados foram bem preocupantes. A empresa testou oito tipos de objetos, sendo um carregador, um carrinho de controle remoto, um receptor-transmissor, uma balança, um relógio, um ferro de passar, um aspirador e uma câmera. Apenas um dispositivo mostrou um nível de segurança satisfatório, os demais mostraram vulnerabilidades em senhas padrão fracas e informações sigilosas fáceis de serem acessadas.

Então, com tudo isso, a Internet das coisas pode sim ser uma ameaça para a segurança dos usuários e empresa caso não exista uma segurança apropriada, e que infelizmente no Brasil ainda não vemos movimentos que alertem os usuários e os

orientem para que os fabricantes tenham mais preocupação em relação à segurança desses dispositivos.

3.2 Aplicando segurança na IoT

Com a implantação de vários dispositivos no contexto da IoT, a possibilidade do fácil acesso a informações representa perigo à segurança e privacidade dos indivíduos e empresas. Nakamura (2007, p.220), diz: "A necessidade de utilização cada vez maior da internet pelas organizações e a constituição de ambientes cooperativos levam a uma crescente preocupação quanto à segurança".

Como na IoT os dispositivos são fabricados em uma variedade enorme de *software* e *hardware,* muitos estão conectados a redes sem fios, com isso a tendência é esses dispositivos apresentarem diversas vulnerabilidades.

Em estudos realizados pela CISCO (2016), foi identificado que a segurança dentro de um ambiente totalmente conectado precisa ser difundida das seguintes maneiras:

- Consistente, automatizada e extensiva aos limites estabelecidos entre as organizações;
- Para que seja possível identificar ameaças em tempo real é necessário que a segurança seja dinâmica;
- Inteligente, com clara visibilidade em todos os elementos da infraestrutura e em todas as conexões;
- Com etapas definidas, para atender às necessidades que forem surgindo;
- Ágil, capaz de reagir em tempo real;
- Solução completa fim a fim.

Com uma segurança difundida, a facilidade de gerenciamento dela é maior, pois não seria necessário ter pessoal e conhecimentos técnicos para auxiliar. Já a segurança fim a fim surge devido a segurança de redes não se resumir apenas a

dispositivos individuais. A necessidade de um monitoramento constante da rede serve para agregar e identificar dados em todo o ambiente conectado, agindo quando for necessário e tirando proveito das informações colhidas (CISCO, 2016).

Com esses dispositivos interagindo a todo instante, são transmitidos dados de locais não confiáveis e com isso acaba deixando uma dúvida em relação a nossa privacidade; então a utilização de boas práticas e mecanismos adequados para a segurança se faz necessário no contexto IoT.

3.2.1 Práticas de segurança

Existem diversas práticas de segurança que já são utilizadas e que são bastante úteis para elevar o nível de segurança dos dispositivos conectados à internet. Abaixo podemos ver algumas dessas práticas.

Fabricantes e dispositivos de qualidade – Sempre que tiver interesse em adquirir um novo dispositivo, tenha certeza que o fabricante disponibiliza produtos de qualidade e com atualização de segurança nos dispositivos. Antes de comprar qualquer dispositivo conectado à internet, é necessário verificar se a senha padrão do dispositivo pode ser alterada.

***Software* livre** – Sempre que for escolher algum tipo de *software* livre verificar se o mesmo possui uma comunidade ativa, pois caso tenha algum tipo de problema a solução possa ser rápida.

E-mails – A cada *e-mail* recebido se faz necessário verificar a autenticidade do mesmo, existem diversas dicas para diferenciar *e-mails* verídicos de falsos. *E-mails* com solicitação de dados pessoais, erros ortográficos, documentos em anexos que não foram solicitados e domínio do *e-mail* estranho, são algumas dicas para saber se o *e-mail* é falso ou não, ao notar alguma dessas observações não abra o *e-mail* e exclua-o.

Senhas – É necessário que se utilize senhas complexas, ou seja, em cada senha existente é ideal utilizar uma combinação de letras maiúsculas, minúsculas, símbolos e números. Para a existência de senhas seguras e complexas é necessário a troca dela de 1 em 1 mês.

Atualizações – Mantenha sempre atualizados seus dispositivos, *firewalls*, sistemas e *softwares*, pois esse tipo de atualização corrigi vulnerabilidades protegendo seus dispositivos contra *malwares*.

Backups – A utilização de *backups* é sempre fundamental. Com a quantidade de informações produzidas por diversos dispositivos conectados, o ideal é possuir HDs externo, *Pendrives* e até na nuvem para armazenamento adicional.

Proteção física – Controlar o acesso a portas USB e a qualquer outro meio físico de conexão ao dispositivo.

Câmeras e *Webcams* – O ideal é sempre ter cuidado com relação a câmeras dos computadores, *smartphones* ou qualquer outro tipo de dispositivo conectado a internet que possa ser utilizado para roubo de senhas por *hackers*.

Interfaces de comunicação – Mantenha sempre *Wi-Fi*, infravermelho e *bluetooth* desabilitados quando não estiver utilizando. Mantenha também o seu dispositivo invisível quando estiver com o *bluetooth* ativado, pois você só receberá solicitações para recebimentos de arquivos quando tirar do modo invisível.

Aplicativos – Tenha cuidados com aplicativos em redes socias que são baseados em geolocalização, esses tipos de aplicativos podem comprometer a sua privacidade.

3.2.1.1 Política de Segurança

Nas empresas é necessário adotar processos que possam melhorar a segurança e evitar qualquer tipo de falha. Conforme Nakamura (2007, p. 191), "o que deve ser

mantido não é apenas a proteção contra *hackers*, mas também a disponibilidade da infraestrutura da organização". A existência dos processos na política de segurança deve estar voltada para o combate de situações não programadas. Segundo Nakamura (2007), ainda, vigilância, atitude, estratégia e tecnologia são os elementos importante para a implementação de uma boa política de segurança. Abaixo podemos conhecer melhor cada um deles:

- **Vigilância:** A vigilância é o acompanhamento constante do que se trafega na rede, responsável por responder a alertas, responsável pelo monitoramento das implementações, responsável por monitorar as mudanças nos dispositivos de segurança e como ser vigilante com relação às senhas dos usuários.
- **Atitude:** A atitude de um funcionário é reflexo da existência de treinamentos que visam o desenvolvimento de habilidades em relação à segurança.
- **Estratégia:** Deve ser criada uma estratégia de defesa de rede que seja adaptável as mudanças que podem surgir no ambiente e que não afete a produtividade dos usuários.
- **Tecnologia:** É muito importante a existência de diversas tecnologias flexíveis e práticas de segurança em uma empresa, pois só assim poderá suprir as necessidades estratégicas e apresentar um nível de segurança satisfatório.

Como a CISCO é pioneira no setor de segurança, a mesma está posicionada com exclusividade no mercado da IoT. Abaixo podemos visualizar as arquiteturas de segurança da CISCO, mostrando que ela usa camadas de infraestrutura, de plataforma e de aplicação para disponibilizar um conjunto de ferramentas e de sistemas.

Princípios de Arquitetura da CISCO *Security*

A seguir a CISCO (2016) apresenta os princípios básicos da arquitetura de segurança utilizada pela empresa:

1. **Controle de acesso –** Com base na política, é fornecido acesso para qualquer usuário ou dispositivo que acesse a rede distribuída. Os usuários são

autenticados e autorizados, os dispositivos também são analisados para determinar se estão em conformidade com a política de segurança. Automaticamente também são identificados os dispositivos sem autenticação, como: impressoras, câmeras de vídeos, sensores e controladores.

2. **Políticas com reconhecimento de contexto –** Utiliza uma linguagem comercial descritiva simplificada para definir política de segurança com base no contexto da situação: quem está enviando informações, quais informações, quando, onde e como. Elas ajudam a empresa a fornecer uma segurança mais eficaz para atender os objetivos com maior eficiência operacional e controle.
3. **Inspeção e execução com reconhecimento de contexto –** Utiliza a rede e a inteligência global para realizar tomadas de decisões. Opções de implantação flexíveis, como serviços de segurança integrada, dispositivos autônomos ou serviços de segurança baseados em nuvem aproximam os mecanismos de proteção do usuário.
4. **Rede e inteligência global –** Utiliza a relação de dados globais para garantir que a rede esteja ciente de ambientes não totalmente seguros. Elas fornecem informações detalhadas de ameaças na rede, para que a proteção seja mais rápida e precisa e para que seja possível realizar aplicação de políticas.

3.2.2 Mecanismos de segurança

Firewalls, Antivírus, Criptografia, IDS e IPS são mecanismos na arquitetura de segurança que podem ser usados para controlar o acesso, analisar o conteúdo, remover ameaças e propor políticas de segurança na tecnologia IoT.

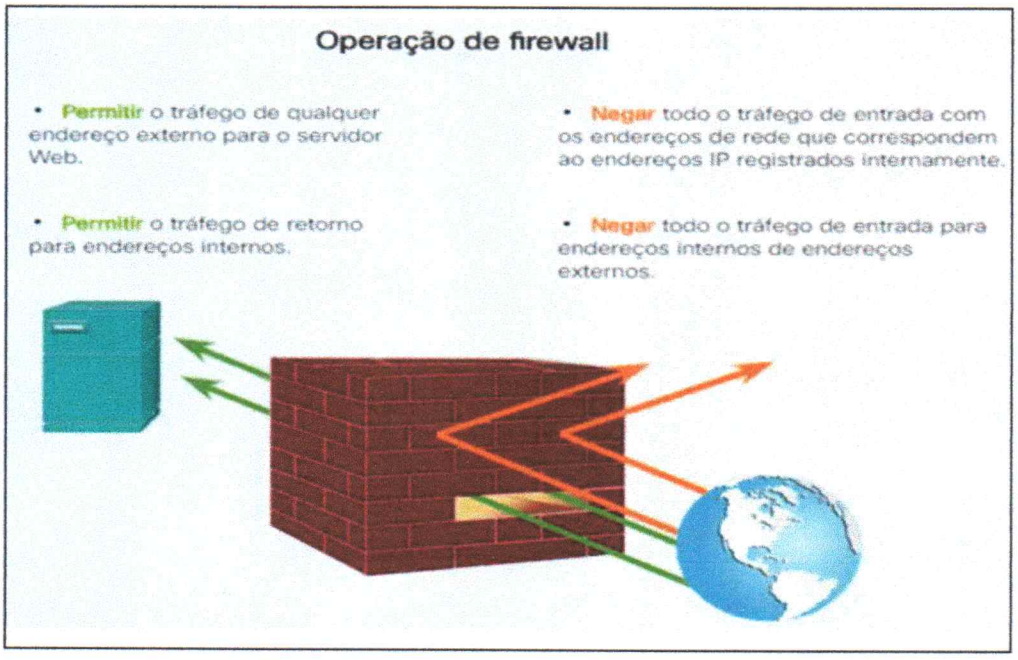
3.2.2.1 *Firewall*

O *Firewall* é utilizado como uma "parede" entre redes interna (protegida) com a rede externa (internet) e vice-versa; o mesmo verifica o tráfego de dados na rede e permite ou não que esse tráfego navegue entre essas redes através dos processos que foram programados nele (NAKAMURA, 2007).

Conforme Cheswick *et al.* (2005, p. 177),

> Um *firewall* é qualquer dispositivo, *software*, arranjo ou equipamento que limita o acesso à rede. Ele pode ser uma caixa que você compra ou constrói, ou uma camada de *software* em alguma outra coisa. Atualmente, os *firewalls* vêm "gratuitamente" dentro de muitos dispositivos: roteadores, *modens*, estações de base sem fio e *switches* de IP.

Figura 5 - Operação de *Firewall*



Fonte: CISCO Networking Academy (2016)[5].

O *firewall* é composto por diversos componentes com a missão de desempenhar papéis importantes para a segurança através de suas funcionalidades. Conforme Nakamura (2007), abaixo podemos ver as funcionalidades que formam os componentes clássicos de um *firewall*.

Filtros – Os filtros têm por finalidade rotear os pacotes que trafegam na rede e depois decidir se vão aceitar ou descartar esses pacotes. Além do processo de

[5] Disponível em: https://www.netacad.com.

roteamento de pacotes, os filtros também tomam decisões de acordo com os estados das conexões.

Proxies – Os *proxies* são os responsáveis por permitir que os usuários realizem alguma solicitação e recebam o retorno desta solicitação.

Bastion hosts – Como os *bastion hosts* são a base para a instalação dos serviços ligados à internet, é necessário que possuam uma proteção maior, pois a exposição a diversas conexões pode ser um perigo.

Demilitarized Zone ou Zona desmilitarizada – Responsável por ser a parede entre uma rede interna com a externa. A DMZ (Demilitarized Zone) faz com que a rede interna não sofra impacto mesmo depois de algum equipamento ser comprometido.

Network address translation **(NAT)** – Funcionalidade criada para ser a responsável por resolver os problemas em redes de grande porte, esses problemas aparecem devido à pouca quantidade de endereços IP.

Rede privada virtual (VPN) – Realiza a comunicação de redes baseadas em determinados protocolos com diversas redes diferentes. A VPN utiliza o conceito de criptografia, pois garante o sigilo, integridade e a autenticação das informações que foram transmitidas.

Autenticação e a certificação – São os endereços IP, senhas, certificados digitais, *smartcards*, biometria ou *token*.

Balanceamento de cargas – Realiza a divisão de tráfego de dados entre *firewalls* que trabalham simultaneamente.

Alta disponibilidade – Garante a que a disponibilidade dos serviços que são acessados pelos usuários seja mantida mesmo quando o *firewall* não estiver disponível.

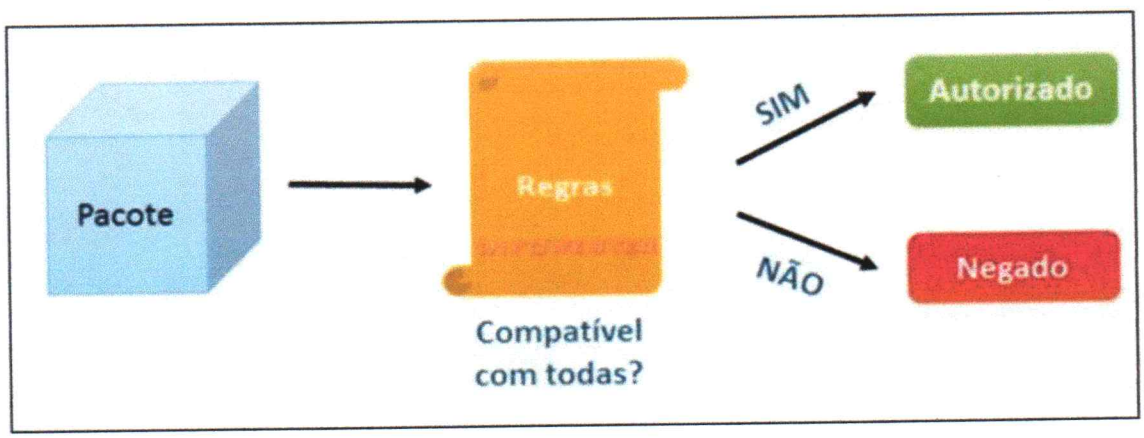
3.2.2.1.1 Tipos de *Firewalls*

O sistema operacional onde o *firewall* se encontra e o que o usuário pretende proteger são alguns dos vários critérios para definir qual o tipo de *firewall* será utilizado. Os mais conhecidos tipos de *firewall* são a filtragem de pacotes, *firewall* de aplicação e inspeção de estados.

Firewall de filtragem de pacotes

De acordo com Nakamura (2007), um *firewall* de filtragem de pacotes é o tipo mais simples e limitado, mesmo oferecendo um nível de segurança considerado bom. Esse *firewall* trabalha na camada de rede e de transportes do conjunto TCP/IP liberando o usuário caso as informações forem compatíveis ou bloqueando caso não seja.

Figura 6 - Filtragem de pacotes



Fonte: INFOWESTER[6].

Existem dois tipos de filtragem de pacotes, a estática e a dinâmica. A filtragem estática tem a missão de liberar ou bloquear os dados de acordo com as regras estabelecidas mesmo se os pacotes possuírem ligações entre eles. Já a Filtragem

---

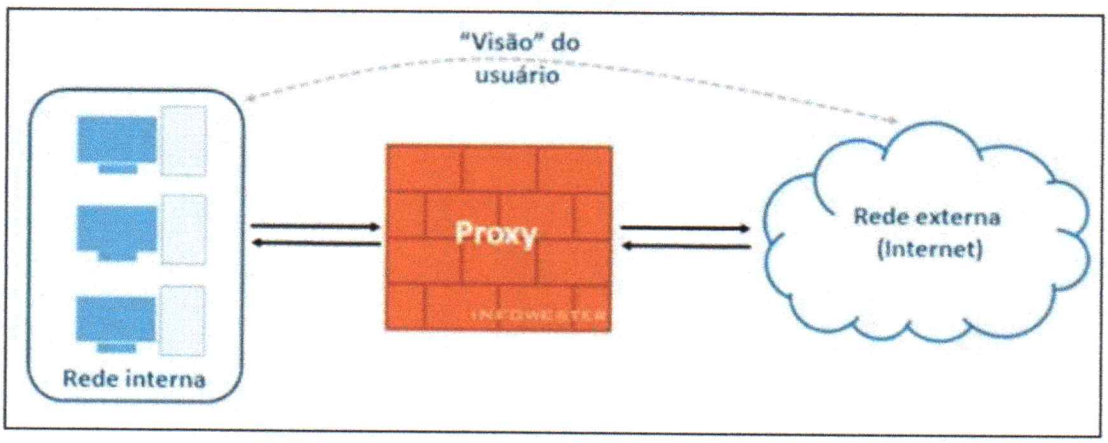
[6] Disponível em: https://www.infowester.com/firewall.php

dinâmica veio para suprir as necessidades que podem ser criadas com as limitações que os filtros estáticos possuem.

Firewall de aplicação

Esse tipo de *firewall* cria uma barreira entre a rede interna com a internet, sem permitir a interação direta entre origem e o destino, ou seja, antes da comunicação passar para a rede interna, a mesma passa primeira pelo firewall de aplicação (NAKAMURA, 2007).

Figura 7 - *Firewall* de aplicação



Fonte: INFOWESTER[7].

Firewall de inspeção de estados

Responsáveis por realizar a comparação entre o que pode acontecer com o que já está acontecendo, ou seja, caso alguma informação transmitida ocorra por portas não autorizadas o *firewall* logo identificará a inconsistência e irá bloquear essas informações (PAIVA, 2017).

---

[7] Disponível em: https://www.infowester.com/firewall.php

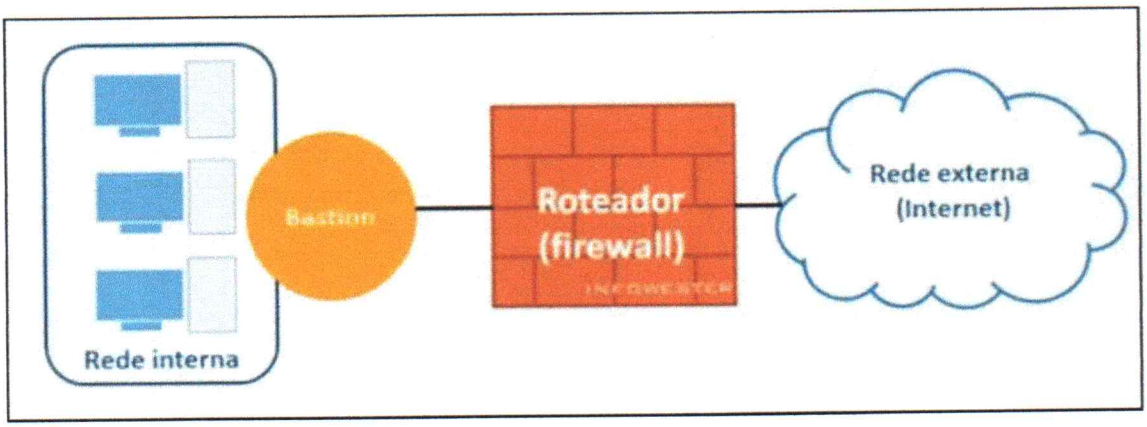
3.2.2.1.2 Arquiteturas do *Firewall*

Para definir uma arquitetura de um *firewall* é também necessário saber qual a necessidade a ser atendida, utilizando os componentes e as funcionalidades de um *firewall*. Conforme Nakamura (2007), *Dual-homed host*, *Screened host* e *Screened subnet* são as principais arquiteturas de um *firewall*.

Arquitetura *Dual-homed host* – Essa arquitetura trabalha como um separador entre duas redes e a sua principal vantagem é a capacidade de controle de tráfego. Um dos problemas que essa arquitetura pode trazer é caso ocorra uma invasão, e com isso o tráfego pode ser paralisado (NAKAMURA, 2007).

Arquitetura *Screened host* – Nessa arquitetura a conexão de um usuário externo com a rede interna só é permitida após o mesmo se conectar ao *bastion host*, como explicado anteriormente o *bastion host* atua entre o roteador e a rede interna. O problema que pode ocorrer nessa arquitetura é caso o *bastion host* seja comprometido, a comunicação da rede interna ficará disponível para qualquer usuário externo (NAKAMURA, 2007).

Figura 8 - Arquitetura *Screened host*

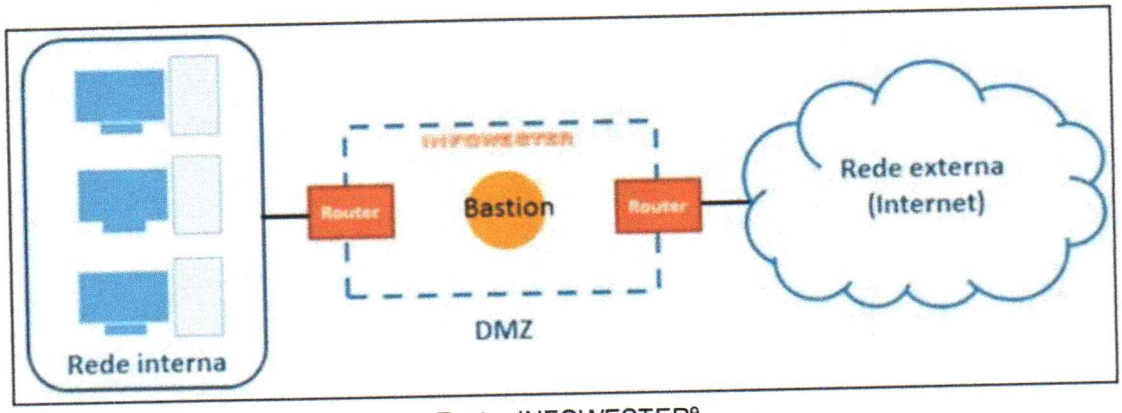


Fonte: INFOWESTER[8].

[8] Disponível em: https://www.infowester.com/firewall.php

Arquitetura *Screened Subnet* – O nível de segurança dessa arquitetura é considerado maior que da arquitetura anterior, isso acontece devido o *bastion host* ficar dentro da rede DMZ que é uma rede que se encontra entre dois roteadores, um responsável por separar ela da rede interna e o outro da rede externa. Essa arquitetura se torna mais cara devido possuir configurações flexíveis tornando o nível de segurança maior que as outras. Abaixo podemos ver melhor como essa arquitetura funciona (NAKAMURA, 2007).

Figura 9 - Arquitetura *Screened Subnet*



Fonte: INFOWESTER[9].

Segundo Cheswick (2005, p. 194), "os *firewalls* são inúteis contra ataques internos. Um ataque desse tipo pode ser feito por um usuário legítimo que se bandeou para o lado negro, ou por alguém que obteve acesso a uma máquina interna por outros meios". Então, apesar de todas essas funcionalidades, componentes e arquiteturas, é importante saber que o *firewall* é apenas uma peça de um conjunto de mecanismos que podem ser utilizados na busca por uma boa segurança de rede.

3.2.2.2 Antivírus

O Antivírus tem por finalidade prevenir, detectar e remover ameaças que possam afetar o desempenho de um computador ou dispositivo. Conforme Paiva (2017), de

---

[9] Disponível em: https://www.infowester.com/firewall.php.

acordo com as informações de ameaças obtidas no banco de dados dos antivírus, os fabricantes de software de proteção podem buscar informações e compará-las com outras já armazenadas no banco de dados, à procura de novas ameaças na rede. Esse processo torna os antivírus eficazes na hora de detectar as ameaças ao seu computador ou dispositivo.

Abaixo podemos ver alguns processos que, segundo matéria publicada em 2018 pelo site Canaltech, são realizados pelo antivírus na busca de impedir a entrada de programas que tem a missão de danificar um sistema.

- **Escaneamento de vírus:** Sempre que o antivírus realiza um escaneamento e localiza um novo vírus é feito o seguinte processo: O Antivírus encaminha o código do vírus para um local onde são enviados os códigos maliciosos e depois realiza identificação do vírus; após isso, o antivírus inicia uma varredura para verificar se existe esse vírus em algum programa, se encontrado, é feita a remoção e enviado para um local que pode ser acessado depois.
- **Sensoriamento heurístico:** Após o usuário solicitar o escaneamento do dispositivo, o antivírus realiza a varredura em busca de alterações em arquivos executáveis. Esse método não é considerado confiável devido a possibilidade de ocorrer gravação de um arquivo corrompido no arquivo original.
- **Busca algorítmica:** O resultado do escaneamento se dá devido a utilização de algoritmos.
- **Checagem de integridade:** Tem a missão de criar um banco de dados e registrar dígitos verificadores para que depois possa compará-los, ou seja, quando o banco de dados for verificado e caso exista alguma alteração o usuário será avisado.

Existem diversas ferramentas de antivírus, tanto as ferramentas grátis quanto as que são pagas podem ser eficientes. Um dos softwares de antivírus mais utilizados atualmente é o Avast, abaixo segue um pouco sobre o *Avast Free* Antivírus.

O *Avast* tem como função identificar algum tipo de problema na segurança e informar imediatamente ao usuário a melhor maneira a ser utilizada para resolver o problema. O *Avast* é responsável também por analisar todos os arquivos suspeitos antes mesmo de liberar o acesso e toda essa proteção é realizada em tempo real (PAIVA, 2017).

De acordo com Paiva (2017), seguem abaixo algumas funções realizadas pelo *Avast*.

- Detecção de vírus, como por exemplo, a detecção de *ransonware*;
- *Wi-Fi Inspector* – Avisa ao usuário quando um roteador precisa ser configurado para não ser acessado por pessoas não autorizadas;
- *CyberCapture* – Detecção de ameaças em tempo real. Aumenta consideravelmente a proteção contra ataques desconhecidos.

3.2.2.3 Criptografia

A criptografia é uma das principais ferramentas de segurança que pode ser utilizada na proteção contra ameaças da internet. Segundo a CERT.br, "a criptografia é considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código".

Segundo Comer (2007, p. 549), "a criptografia embaralha os *bits* da mensagem de tal modo que somente o receptor pretendido possa recompor a mensagem".

A cifragem e a decifragem ocorre com a utilização de códigos com funções matemáticas que modificam um texto legível para um texto totalmente em códigos. A criptografia possui uma função essencial para a segurança da informação, pois ela ajuda a adquirir os seguintes processos: Integridade, Autenticidade, não-repúdio e sigilo (NAKAMURA, 2007).

Segundo Nakamura (2007), existem diversas maneiras para se utilizar a criptografia em busca de proteção do sigilo, integridade e autenticação da informação e comunicação. Abaixo seguem algumas dessas maneiras.

- A comunicação por celulares da tecnologia GSM (*Global System for Mobile Communication*) é protegida pelo algoritmo COMPI28-2;
- As compras na internet são protegidas pelo protocolo de segurança SSL (*Secure Socket Layer*);
- As transferências eletrônicas da Internet *Banking* são protegidas com o protocolo de segurança SSL com mais algum protocolo criptografado;
- São utilizados protocolos como o SSH (*Secure Shell*) para acessos remotos em servidores;
- O protocolo WEP (*Wired Equivalent Privacy*) é utilizado em redes sem fio para controlar os acessos;
- Em redes VPN (*Virtual Private Network*) são utilizados protocolos como o IPSec (*IP Security*) em busca de proteção nas comunicações entre empresas.

Apesar da criptografia ser bastante utilizada atualmente, não quer dizer que esteja livre de falhas. O grande aumento da comunicação através da internet faz surgir diversos fatores causadores de problemas em sistemas criptografados. Abaixo segue alguns desses fatores (NAKAMURA, 2007).

- Falha na checagem do tamanho dos valores;
- A utilização mais de uma vez de parâmetros aleatórios;
- Existe sistemas que não exclui as mensagens que já foram decifradas;
- Pode ocorre falhas na utilização da base de dados de recuperação de chaves.

3.2.2.3.1 Criptografia de chaves simétrica

Segundo a CERT.br, "a criptografia de chave simétrica utiliza uma mesma chave, tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados".

Conforme Stallings (2008), um esquema de criptografia simétrica possui cinco ingredientes, são eles:

- **Texto claro**: Mensagens originais, inteligíveis, alimentados no algoritmo como entrada;
- **Algoritmo de criptografia**: Realiza várias substituições e transformações no texto claro;
- **Chave secreta**: A chave secreta é a entrada para o algoritmo de criptografia, independente do texto ou algoritmo a chave é um valor só. As substituições e transformações realizadas pelo algoritmo dependem da chave;
- **Texto cifrado**: O texto cifrado é um fluxo de dados de modo aleatório, tornando a mensagem embaralhada;
- **Algoritmo de decriptografia**: Responsável pela decifragem. Através do texto cifrado e da chave secreta é possível produzir o texto claro e original.

3.2.2.3.2 Criptografia de chaves assimétricas

Conforme Comer (2007, p. 550), "a criptografia de chave pública pode ser usada para garantir confidencialidade. Um remetente que deseja que uma mensagem permaneça confidencial usa a chave pública do receptor para cifrar a mensagem. Esse tipo de criptografia é responsável por disponibilizar para cada usuário um par de chaves".

Uma das vantagens da utilização de uma chave pública é que mesmo revelando ela para alguém, continua segura, pois as funções utilizadas para criptografia e decriptografia possui uma propriedade de sentido único, ou seja, mesmo a chave pública sendo revelada, não é possível que alguém forje uma mensagem que pareça ser criptografada por uma chave privada (COMER, 2007).

3.2.2.3.3 Funções *hash*

Conhecido também como função de resumo, o *hash* é um método criptográfico que independente do tamanho da informação ele gera um único resultado e de tamanho fixo (CERT.br)

De acordo com o CERT.br, o *hash* pode ser utilizado de para os seguintes fins:

- Verificação da integridade dos arquivos em seu computador ou em *backups*;
- Verificação da integridade de arquivos adquiridos da internet;
- Geração de assinaturas digitais.

Seguindo o mesmo caminho do *Firewall,* a criptografia é mais uma boa opção de mecanismo de segurança a ser utilizada nos dias atuais, com a missão de realizar proteção das informações que circulam nas redes.

3.2.2.3.4 Ferramentas de Criptografia

Existe diversas ferramentas disponíveis utilizadas para criptografar arquivos, pastas, mensagens e imagens, em disco local, em CDs, em e-mails e até na nuvem. Abaixo segue 4 tipos de ferramentas de criptografia: as ferramentas *DocSecrets, Cyph e a Jumble,* que segundo o site Canaltech (2018) são ferramentas simples e fáceis de se usar. E a ferramenta Steganos Safe que é um dos melhores *softwares* de criptografia do mercado, segundo o site Segurisoft (2016).

DocSecrets – *DocSecrets* é utilizado para criptografar informações e/ou documentos do *Google Drive.* Essa ferramenta é de fácil utilização, basta selecionar qual informação deseja ocultar e adicionar uma senha para acesso.

Cyph - É tipo uma sala de bate papo onde as conversas são criptografadas automaticamente. Com o *Cyph* ainda é possível enviar imagens, anexos, vídeos e áudios, porém toda a conversa precisa ser rápida, pois a sala de bate papo expira em 10 minutos e exclui as mensagens automaticamente.

Jumble – *Jumble* pode ser utilizado tanto como uma extensão para o *Google Chrome* quanto como aplicativo para iOS. O *Jumble* é responsável por criptografar mensagens do *Gmail*, porém o receptor da mensagem também precisa usar o *Jumble* para descriptografar os *e-mails*.

Steganos Safe – Diferentes das ferramentas simples citadas anteriormente, *Steganos Safe* é considerado o melhor *software* do mercado. Este *software* utiliza algoritmo AES-XES de 384 bits para realizar a criptografia de arquivos e pastas, em disco local, em memórias USB, CDs, DVDs, HDs externos e até na nuvem (*Google Drive, Dropbox e OneDrive*). O *Steganos Safe* traz consigo uma ferramenta invulnerável para geração de senhas, inclui também um teclado virtual eficaz contra *keyloggers* e ainda permite a criação de senhas em imagens garantindo uma segurança maior na hora de abrir alguma unidade.

3.2.2.4 Sistema de detecção de intrusão (IDS)

O IDS (*Intrusion Detection System*) tem a missão de detectar ameaças e avisar ao usuário sobre a existência de possíveis ataques ou atividades suspeitas em uma rede. Os sistemas de detecção de intrusões são compostos por vários componentes, como: sensores, consoles e um mecanismo central. Os sensores são responsáveis por gerar eventos de segurança; os consoles são responsáveis por controla os sensores e verificar eventos e alertas; e o mecanismo central é responsável por gerar alertas de acordo com os eventos de segurança que foram coletados (PAIVA, 2017).

Comer (2007, p. 556) diz o seguinte em relação a função de um IDS para a internet.

> Um sistema que monitora todos os pacotes que chegam em um site e notifica o administrador se uma violação de segurança é detectada. Um IDS pode ser configurado para detectar ataques como um *scanning* de portas (um estranho tenta números de portas de protocolos TCP sucessivos para determinar as portas nas quais o site tem um servidor) e sobrecarga SYN (para deixar um computador instável, um estranho envia segmentos TCP que aparentemente requerem uma nova conexão TCP; quando a máquina receptora tenta completar a conexão, o estranho não responde).

De acordo com Nakamura (2007), abaixo segue algumas características do IDS:

- Monitora e analisa as atividades dos usuários e sistemas;
- Responsável por avaliar a integridade dos arquivos e dados do sistema;
- Analisa atividades anormais;
- Detecção em tempo real;
- Identifica o possível destino do ataque;
- Capacidade de prevenir possíveis ataques;
- Transparência, não permitindo que o sistema mostre qual local da rede está sendo monitorado;
- Flexibilidade para respostas de possíveis danos.

O IDS também trabalha em conjunto com o *firewall* na liberação de conexões na rede. Esse trabalho acontece após o *firewall* liberar as conexões para que em seguida o IDS analise, detecte e possa responder a qualquer tipo de tráfego suspeito. O IDS pode ainda detectar atividades maliciosas em portas legítimas mesmo que elas não possuam a proteção de um *firewall* (NAKAMURA, 2007).

3.2.2.4.1 Tipos de IDS

Conforme Nakamura (2007), existe dois tipos primários de IDS, um que é baseado em *host* (*Host-Based Intrusion Detection System* – HIDS) e o outro que é baseado em rede (*Network-Based Intrusion Detection System* – NIDS). O Uso de vários tipos de IDS em conjunto ajuda a melhorar a segurança contra ameaças aos dispositivos presentes em uma rede.

HIDS

Caso ocorra algum tipo de alteração no sistema, seja ela nos arquivos, nos processos, nas permissões dos usuários, na CPU ou em programas que estão sendo executados, o HIDS irá detectar. O mesmo realiza o monitoramento do sistema

através das informações recebidas dos agentes de auditorias ou de arquivos de *logs* (NAKAMURA, 2007).

Conforme Nakamura (2007), o HIDS possui diversos pontos fortes e fracos, abaixo podemos ver quais são:

Pontos fortes

- Com base nas informações dos arquivos *logs* do sistema, o HIDS verifica se um ataque foi concluído ou não;
- Monitora as atividades do sistema, como: *logon* e *logoff* de um usuário, alterações em permissões de arquivos, permissões do administrador entre outras;
- Detecta ataques físicos no servidor;
- Pode detectar ataques que utilizam criptografia;
- Pode ser utilizado em redes separadas por *switches*;
- Poucas vezes mostra alertas falsos;
- Não é obrigatório *hardware* adicional.

Pontos fracos

- Problemas de escalabilidades devido o HIDS ser difícil de se configurar em todos os *hosts* monitorados;
- HIDS diferentes para cada sistema operacional;
- Não detecta ataques de redes;
- Em um HIDS infectado as informações contidas nele podem ser perdidas;
- Necessidade de armazenamento adicional;
- O desempenho de um *host* cai quando ele está sendo monitorado.

NIDS

Este tipo de IDS é responsável pelo monitoramento da rede à procura de ataques que estão em andamento. O NIDS é ideal contra ataques como *port scanning,* IP *spoofing* e ataques em servidores WEB; ele também é capaz de detectar ataques na rede em tempo real. Segundo Nakamura (2007, p. 272), "a detecção é realizada com a captura e análise dos cabeçalhos e conteúdo dos pacotes, que são comparados com padrões ou assinaturas conhecidas".

As partes que compõem um NIDS levam o nome de sensores e console, os sensores têm a missão de capturar, formatar os dados e verificar o tráfego da rede; já o console é responsável por fazer os sensores serem geridos de modo que tenham os tipos de respostas corretas para cada tipo de ameaça detectada. É necessário que a comunicação desses componentes do NIDS seja criptografada (NAKAMURA, 2007).

Conforme Nakamura (2007), o NIDS também possui diversos pontos fortes e fracos, abaixo podemos ver quais são:

Pontos fortes

- Fornece monitoramento para diversas plataformas;
- Capaz de detectar ataques como *port scanning* e IP *spoofing*;
- Monitora comportamentos suspeitos em portas conhecidas que são utilizadas pelo HTTP;
- Detecta ataques em tempo real;
- Dificulta a ação dos *hackers* na hora de apagar os rastros depois de um ataque;
- Dificulta a identificação da existência de um NIDS por parte dos *hackers*;
- Não prejudica o desempenho da rede.

Pontos fracos

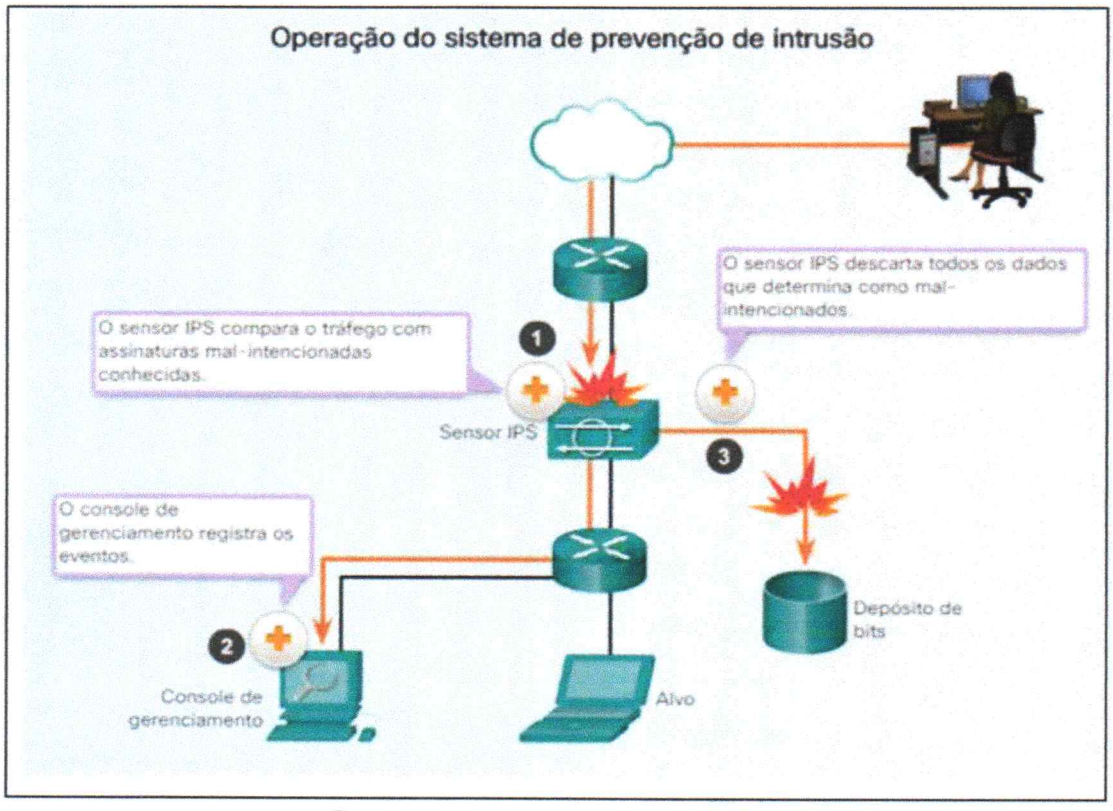
- Perdas de pacotes em redes saturadas;

- Dificuldade para compreender protocolos de aplicação;
- Não monitora o tráfego cifrado;
- Dificuldade de utilização em redes com *switches*.

3.2.2.5 Sistema de prevenção contra invasões (IPS)

O IPS (*Intrusion Prevention System*) tem a capacidade de restaurar uma conexão caso identifique atividades maliciosas na rede e podendo também descartar qualquer tipo de tráfego de dados que possam trazer problemas à rede (CISCO, 2016). Abaixo, vemos como é uma operação do IPS:

Figura 10 - Operação do sistema de prevenção de intrusão



Fonte: CISCO Networking Academy (2016)[10].

[10] Disponível em: https://www.netacad.com.

Conforme a CISCO (2016), devido ao IPS ser um complemento do IDS ele tem um grau elevado de técnicas de alertas e respostas sobre ameaças aumentando consideravelmente o nível de segurança de uma rede sem que ela sofra queda na disponibilidade.

3.2.2.5.1 *SNORT*

Existe diversas ferramentas de IDS e IPS, a seguir podemos conhecer melhor uma delas, a ferramenta *SNORT*.

O *Snort* é um sistema de prevenção de intrusão *open source* com a função de verificar tráfego em tempo real. Ele pode realizar o registro de pacotes em redes IP, analisar protocolos e também pode ser utilizado para detectar diversos tipos de ataques, como varreduras de portas invisíveis, ataques de impressão digital do sistema operacional entre outras. (*SNORT, s.d.).*

O *Snort* possui três modos para ser utilizado.

- O primeiro modo é que ele pode ser usado como um *sniffer* de pacotes direto, ou seja, mostra na tela a leitura realizada nos pacotes de rede;
- O segundo modo é como o *tcpdump*, um *logger* de pacotes que é utilizado para a limpeza de tráfego de rede;
- E o terceiro modo é como um IPS de rede completo.

O *Snort* é apenas uma das diversas ferramentas de IDS/IPS disponíveis na atualidade que pode ser utilizada para detectar e prevenir ameaças em redes que possuam milhares de dispositivos conectados.

3.2.2.6 *Kaspersky IoT Scanner*

Pensando na utilização de dispositivos inteligentes a empresa *Kaspersky* criou um aplicativo chamado *Kaspersky* IoT *Scanner* com a função de analisar a rede doméstica e criar uma lista com o nome de todos os dispositivos conectados,

mostrando suas vulnerabilidades. O *Kaspersky* IoT *Scanner,* irá varrer toda a rede doméstica e verificar quais portas dos dispositivos estão fechadas e quais estão abertas. Caso encontre alguma porta aberta o aplicativo informa ao usuário e solicita que a mesma seja fechada.

O *Kaspersky* IoT *Scanner* ainda possui dois recursos. O primeiro é que o aplicativo mostra todos os dispositivos que estão conectados na sua rede *Wi-Fi* e o segundo recurso é que o aplicativo também verifica e detecta as portas de novos dispositivos conectados à rede, facilitando a identificação por parte do usuário se esse dispositivo conectado é seguro ou não.

4. CONCLUSÃO

4.1 Considerações finais

Este trabalho teve como objetivo discutir a importância de boas práticas e mecanismos de segurança para dispositivos conectados à IoT, mostrando os conceitos e as principais características da IoT e o que pode acontecer caso esses dispositivos sejam acessados por usuários mal-intencionados.

Os resultados obtidos durante a realização da pesquisa chamaram atenção para a quantidade de problemas que podemos ter com o uso indevido de dispositivos conectados à IoT. Dispositivos que são mal fabricados, sistemas não atualizados, câmeras expostas a usuários externos, falta de um antivírus, *firewall* desatualizado, não uso de ferramentas de criptografia, IDS e IPS podem nos trazer diversos problemas, desde senhas de *Wi-fi* alteradas até falhas nos comandos de um veículo.

Muitas vezes a falta de conhecimento por parte do usuário, ou até mesmo o pouco interesse dos fabricantes em desenvolver manuais que orientem práticas básicas de segurança, torna-se uma barreira para o funcionamento da Internet das Coisas.

Portanto, pode-se perceber que sem uma segurança bem definida e ajustada para cada tipo de dispositivo ou sistema, a existência da internet das coisas fica quase que improvável no mundo atual.

A nível de contribuição, este trabalho põe em evidência um tema atual e muito em tendência em um futuro próximo, possibilitando o aprofundamento de estudos na área IoT.

4.2 Trabalhos futuros

Depois de todos os estudos sobre esse tema, é interessante aprofundar melhor na tecnologia IoT, devido a ela estar praticamente associada a tudo no nosso dia a dia. Seguem abaixo alguns temas que podem ser utilizados em futuras pesquisas:

- Estudos de ferramentas de IDS e IPS voltadas especialmente para os dispositivos domésticos conectados à IoT;
- A importância da Internet das Coisas no desenvolvimento das cidades inteligentes;
- As principais vantagens e desvantagens da utilização da tecnologia IoT na fabricação de automóveis;
- Quais as melhorias que uma implantação de dispositivos IoT em ambientes corporativos pode trazer para os funcionários e para a própria organização.

5. REFERÊNCIAS

ALECRIM, Emerson. **O que é firewall? Conceitos, tipos e arquiteturas.** Disponível em: <https://www.infowester.com/firewall.php>. Acesso em: 10 agosto 2018.

BENETTI, Ticiano. **Segurança da Informação – Confidencialidade, Integridade e Disponibilidade (CID).** Disponível em: <https://www.profissionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/>. Acesso em: 16 maio 2018.

CANALTECH. **O que é antivírus**? Disponível em: <https://canaltech.com.br/antivirus/o-que-e-antivirus/>. Acesso em: 14 agosto 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet: Criptografia**. Disponível em: <https://cartilha.cert.br/criptografia/>. Acesso em: 27 agosto 2018

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet: Segurança de redes**. Disponível em: <https://cartilha.cert.br/redes/>. Acesso em: 08 setembro 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet: Segurança em dispositivos móveis**. Disponível em: <https://cartilha.cert.br/dispositivos-moveis/>. Acesso em: 24 agosto 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet: Segurança na Internet**. Disponível em: <https://cartilha.cert.br/seguranca/>. Acesso em: 24 agosto 2018.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D.. **Firewalls e Segurança na Internet: Repelindo o hacker ardiloso**. 2. Ed. Bookman. Porto Alegre, 2005. 400 p.

CISCO Networking Academy. **Introdução à Internet de Todas as Coisas**. Disponível em: <https://www.netacad.com>. Acesso em: 09 julho 2018.

COMER, Douglas E. **Redes de computadores e Internet**. 4. ed. Bookman. Porto Alegre, 2007. 632p.

COMPUTERWORLD. **Cinco fundamentos para elevar a segurança dos dispositivos de IoT.** Disponível em: <https://computerworld.com.br/2016/05/17/cinco-fundamentos-para-elevar-seguranca-do-dispositivos-de-iot/>. Acesso em: 10 agosto 2018.

DIAS, Rafael. **Lista dos melhores programas de criptografia**. Disponível em: <https://www.segurisoft.com.br/criptografia/top-10-software-criptografia/>. Acesso em: 15 setembro 2018.

ITF 365. **O que torna o ransomware tão perigoso para a IoT?** Disponível em: <https://www.itforum365.com.br/seguranca/o-que-torna-o-ransomware-tao-perigoso-para-iot/> Acesso em: 25 julho 2018.

KASPERSKY. **A vulnerável Internet da Coisas**. Disponível em: https://www.kaspersky.com.br/blog/a-vulneravel-internet-das-coisas/10026/. Acesso em: 27 julho 2018.

LAKATOS, Eva Maria; MARCONI, Mariana de Andrade. **Fundamentos de metodologia científica**. 7. ed. Atlas. São Paulo, 2010. 297p.

MACEDO, Diego. **Segurança de Redes de Computadores.** Disponível em: <https://www.diegomacedo.com.br/seguranca-de-redes-de-computadores/>. Acesso em: 05 junho 2018.

MACEDO, Joyce. **5 ferramentas de criptografia fáceis de usar**. Disponível em: <https://canaltech.com.br/seguranca/5-ferramentas-de-criptografia-faceis-de-usar/>. Acesso em: 15 setembro 2018.

MADAKAM, Somayya; RAMASWAMY, R.; TRIPATHI, Siddharth. **Internet of Things (IoT): A Literature Review**. Disponível em: <https://file.scirp.org/pdf/JCC_2015052516013923.pdf>. Acesso em: 07 julho 2018.

MARTINS, Elaine. **O que é World Wide Web?** Disponível em: <https://www.tecmundo.com.br/web/759-o-que-e-world-wide-web-.htm>. Acesso em: 28 junho 2018.

MARTINS, Rodrigo. **Os riscos de segurança na Internet das Coisas.** Disponível em: <https://atitudereflexiva.wordpress.com/2016/01/02/os-riscos-de-seguranca-na-internet-das-coisas/>. Acesso em: 27 julho 2018.

MENEZES, Sérgio Alves. **Segurança da Informação: Um guia de instalação e configuração do sistema de detecção de intrusão *SNORT*.** Floresta-PE, 2018. 58p.

MICROSOFT. **Práticas recomendadas de segurança de Internet das Coisas**. Disponível em: <https://docs.microsoft.com/pt-br/azure/iot-fundamentals/iot-security-best-practices>. Acesso em: 08 agosto 2018.

MIGUEL, Marcelo. **A Internet das Coisas e a transformação das empresas**. Disponível em: <https://canaltech.com.br/negocios/a-internet-das-coisas-e-a-transformacao-das-empresas-92482/>. Acesso em: 30 julho 2018.

NAKAMURA, Emilio Tissato. **SEGURANÇA DE REDES EM AMBIENTES COORPORATIVOS.** Novatec Ed.: São Paulo, 2007. 483 p.

OLHAR DIGITAL. **Internet das Coisas é ameaça para segurança digital em todo mundo**. Disponível em: <https://olhardigital.com.br/fique_seguro/video/internet-das-

coisas-e-ameaca-para-seguranca-digital-em-todo-o-mundo/66418>. Acesso em: 27 julho 2018.

PAIVA, Severino do Ramo de. **SEGURANÇA E AUDITORIA DE SISTEMAS.** Imprel Editora. João Pessoa-PB, 2017. 208 p.

PATEL, Keyur K.; PATEL Sunil M.. **Internet of Things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges.** Disponível em: <http://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857.Internet%20of%20Things-IOT%20Definition,%20Characteristics,%20Architecture,%20Enabling%20Technologies,%20Application%20&%20Future%20Challenges.pdf>. Acesso em: 01 julho 2018.

PEREKALIN, Alex. **Kaspersky IoT Scanner: How to keep your home network and its smart devices safe**. Disponível em: <https://www.kaspersky.com/blog/kaspersky-iot-scanner/18449/>. Acesso em: 27 julho 2018.

PESSOA, Cláudio Roberto Magalhães; JAMIL, George Leal; JUNIOR, Manuel Rocha Fiuza Branco. **A Internet das Coisas: Conceitos, aplicações, desafios e tendências**. Disponível em: <https://www.researchgate.net/publication/305805347_INTERNET_OF_THINGS_CONCEPTS_APPLICATIONS_CHALLENGES_AND_TRENDS>. Acesso em 07 julho 2018.

PROOF. **Internet das Coisas e seus desafios de Segurança**. Disponível em: <https://www.proof.com.br/blog/iot-internet-das-coisas/>. Acesso em: 06 agosto 2018.

RAJPUT, Dharmendra Singh; GOUR, Rakesh. **An IoT Framework for Healthcare Monitoring Systems.** Disponível em: <https://www.researchgate.net/publication/303923009_An_IoT_Framework_for_Healthcare_Monitoring_Systems>. Acesso em: 01.07.2018.

RODRIGUES, Marcelo. **Ataques DDoS crescem 138% no Brasil, dispositivos IoT seriam os culpado**. Disponível em: <https://www.tecmundo.com.br/seguranca/119605-ataques-ddos-crescem-138-brasil-dispositivos-iot-culpados.htm> Acesso em: 26 julho 2018

ROHR, Altieres. Aumento de ataques para tirar sites do ar confirma despreparo do Brasil. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/aumento-de-ataques-para-tirar-sites-do-ar-confirma-despreparo-do-brasil.html> Acesso em: 26 julho 2018.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23. ed. Cortez. São Paulo, 2007. 304p.

SILVA, Leonardo Werner. **Internet foi criada em 1969 com o nome de "ARPANET" nos EUA.** Disponível em: <https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml>. Acesso em: 28 junho 2018.

SNORT. **Snort FAQ**. Disponível em: <https://www.snort.org/faq>. Acesso em: 16 agosto 2018

STALLINGS, William. **Criptografia e segurança de redes**: **Princípios e práticas**. 4. ed. Pearson Prentice Hall. São Paulo, 2008. 492 p.

TANENBAUM, Andrew S.; WETHEREALL, David. **Redes de computadores**. Pearson Prenttice Hall. São Paulo. 2011.

TANENBAUM, Andrew S.. **Redes de Computadores.** Disponível em: <https://books.google.com.br/books?id=0tjB8FbV590C&printsec=frontcover&dq=inauthor:%22Andrew+S.+Tanenbaum%22&hl=pt-BR&sa=X&ved=0ahUKEwj-j-ye8sHcAhXHEZAKHdCDBGcQ6AEIKjAA#v=onepage&q&f=false>. Acesso em 24 maio 2018.

TECMUNDO. **O que são wearables e por que você vai querer usar um em breve**. Disponível em: <https://www.tecmundo.com.br/wearables/117937-samsung-wearables-dispositivos-vestiveis-realidade-virtual-camera-360.htm>. Acesso em: 10 julho 2018.

VERMESAN, Ovidiu; FRIESS, Peter. **Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems**. Disponível em: <http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf>. Acesso em: 03 julho 2018.

VLCEK, Ondrej. **CyberCapture: Proteção contra os ataques zero-segundos.** Disponível em: <https://blog.avast.com/pt-br/cybercapture-protection-against-zero-second-attacks-0> Acesso em: 08 setembro 2018.