A relevância da Segurança da Informação na Internet das Coisas

Rafael T. Bueno
Faculdade de Tecnologia de Americana (FATEC Americana) Curso Superior de Tecnologia em Segurança da Informação
Endereço: Rua Emílio de Menezes, S/N - Gleba B,
Americana/SP, CEP.: 13469-111, Brasil.
Telefone: (19) 3406-3297

***rafaelb096@gmail.com**

RESUMO: Esse artigo apresenta algumas definições de dispositivos IoT, bem como o período que se originou, o funcionamento da tecnologia e suas aplicações. No artigo podem ser encontradas as vulnerabilidades, benefícios e implicações da inclusão desta tecnologia. Ao que é salientado os fundamentos da Segurança da Informação, foi se observado que esta tecnologia pode infringir serviços importantes, deste modo este artigo contém as principais medidas de segurança para o uso adequado desta, e quando bem aplicados contribui de forma positiva para diversos segmentos.

PALAVRAS-CHAVE: Internet das coisas; segurança da informação.

ABSTRACT: This article presents some definitions of IoT devices, as well as the period that originated the operation of the technology and its applications. In the article can be found the vulnerabilities, benefits and implications of the inclusion of this technology. To highlight the fundamentals of Information Security, it has been observed that this technology can infringe important services, so this article contains the main security measures for the proper use of this, and when applied well contributes positively to various segments.

KEYWORDS: Internet of things; information security.

1. INTRODUÇÃO

Este artigo busca salientar a importância da Segurança da Informação em ambientes que possuem objetos inteligentes (IoT) de forma a estas auxiliarem as atividades desenvolvidas nestes espaços sem comprometer a privacidade dos usuários e visando a garantia da preservação dos pilares da Segurança da Informação. Evitando consequentemente o uso indevido dessa tecnologia de modo a dificultar a exploração das vulnerabilidades (suscetíveis) da mesma bem como preservar os usuários de tal tecnologia de possíveis danos.

> A Segurança em redes de sensores sem fio (RSSF) precisa ser considerada em várias aplicações. Por exemplo, se colocarmos sensores em um poço de petróleo para detectar dados da perfuração a fim de executá-la da melhor forma possível. Os responsáveis por coletar os dados irão querer que os dados fossem confiáveis, não existindo nenhum tipo de interferência, alteração ou inclusão de dados falsos. Assim é interessante que uma rede tenha capacidade de prover integridade dos dados, confidencialidade, autenticidade e disponibilidade, além de ser resistente a ataques. (SIQUEIRA GOIS; ANDRADE LIMA; MORENO ORDONEZ, 2015)

2. O QUE É

A Internet das Coisas é uma extensão da Internet atual. Ela proporciona que objetos que tenham capacidade computacional e de comunicação, se conectarem à Internet de forma a solucionar ou possibilitar maior facilidade na execução de tarefas/atividades cotidianas.

A Internet das Coisas (IoT) é um termo criado em setembro de 1999, enquanto trabalhava em identificação por rádio frequência (RFID), Kevin Ashton, um pioneiro tecnológico britânico, concebeu um sistema de sensores omnipresentes que conectava o mundo físico à Internet.

3. ORIGEM

“Internet das Coisas” refere-se à rede de objetos físicos que possuem software para processar dados e com isso, gerarem informações para o mundo externo. A possibilidade de conectar-se com coisas do cotidiano (como geladeiras, máquinas fotográficas, celulares, agendas eletrônicas, sistema de entrega dos correios), não se deu somente da criação de redes sem fio, essa alternativa se originou também da junção de três componentes; a eletrônica (fornecedora dos objetos), a telecomunicações (responsável pela conexão entre Internet-objeto) e a computação (gerência da relação). O que vem se tornando possível devido as redes convergentes disponíveis atualmente.

Figura 1. Internet das Coisas

Fonte:https://www.youtube.com/watch?time_continue=120&v=wZvDZfO13mA

4. PILARES

A IoT incorpora quatro pilares que tornam as conexões em rede mais relevantes e valiosas do que antes: pessoas, processos, dados e coisas. As informações provenientes destas conexões levam a decisões e ações que criam novas capacidades, experiências mais ricas e oportunidades econômicas sem precedentes para indivíduos, empresas e países. O pilar Coisas é composto predominantemente por vários tipos de dispositivos e computadores tradicionais, por exemplo: desktops, laptops, smartphones, tablets, mainframes e clusters de computador. No entanto, a IoT englobará todos os tipos de objetos, inclusive equipamentos e objetos que não estejam conectados de forma convencional. Esses objetos possuem tecnologia integrada para interagir com servidores internos e o ambiente externo. Capazes de trabalhar em rede, tais objetos devem se comunicar por meio de uma plataforma de rede segura, confiável e disponível. Entretanto, a IoT se refere a uma única transição tecnológica: a capacidade de estabelecer conexão com objetos que antes estavam desconectados para que possam se comunicar pela rede e interagir com o usuário. No caso da segurança da informação os pilares são: confidencialidade (diz respeito a informação ser restrita somente aos que possuem autorização para acessa-la), disponibilidade (a informação deve encontrar-se disponível para aqueles que necessitem acessa-la) e integridade (não deve haver alterações indevidas nas informações pertinentes) que devem, neste cenário, harmonizar e cooperar com a tecnologia da IoT.

5. PROPOSTA DA IOT

Baseada nas conexões entre pessoas, processos, dados e coisas a IoT visa: a disponibilidade de dados provenientes de objetos que podem comunicar o que detectam mudar como e onde as decisões serão tomadas, quem decidirá e os processos que os indivíduos e as empresas usarão para tomar essas

decisões. Em como a facilitação de execução de atividades rotineiras desempenhadas pelos usuários.

> A integração de objetos físicos e virtuais em redes conectadas à Internet, permite que “coisas” coletem, troquem e armazenem uma grande quantidade de dados numa nuvem, e uma vez processados e analisados, forneçam informações e serviços em escala sem precedentes. (ALMEIDA, 2015)

A ideia de proteção em vista não é buscar desenvolver um sistema à prova de invasões e sim um mais difícil de ser atacado do que os outros de forma a torná-lo menos atrativo à atacantes em potencial, como é possível observar na imagem a seguir.

Figura 2. Invasões

Fonte: https://www.youtube.com/watch?time_continue=120&v=wZvDZfO13mA

6. COMO PODE AJUDAR

> Há vários setores na sociedade que se beneficiariam com a comunicação entre dispositivos. Uma vez que por mais simples que sejam estes dispositivos eles são capazes de comunicar-se com outros ou até com servidores, pode-se pensar em várias aplicações possíveis que poderiam ajudar a melhorar o ambiente em que as pessoas vivem. Fazendo uma analogia, é como se de repente, as coisas ao redor ganhassem bocas e ouvidos tendo a capacidade de passar informações que antes não podiam ser coletadas por seres humanos ou dava muito trabalho fazê-lo. (TONEZER, 2017)

Em seguida abordaremos como esta tecnologia pode auxiliar tanto as pessoas quanto as empresas que optarem por adquirir e utilizar da mesma.

6.1. Benefícios Para As Pessoas

A IoT representa uma solução em potencial para melhoria na vida das pessoas. Além de trocas de dados entre máquinas, facilitando o acesso às informações, existe ainda a possibilidade de economia de energia, segurança, saúde, educação e outros aspectos do cotidiano. Um exemplo disso é o *smartwatc*h, que monitora a saúde e ainda está conectado à nuvem.

No meio de vida das pessoas, o IoT pode entra como, por exemplo:

1) Organização de uma agenda;
2) Reforço à área médica;
3) Tecnologias de localização,
4) Monitoramentos (como câmeras e sensores de movimento);
5) Comunicação;
6) Compras.

Figura 3. WLAN (Rede residencial sem fio)

Fonte: https://1360665.netacad.com/courses/456510

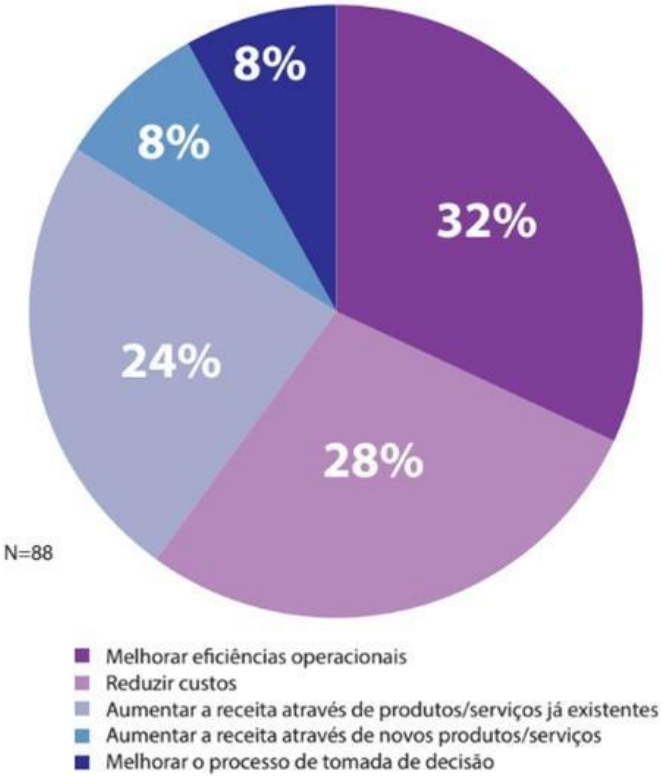
6.2. Benefícios Para As Empresas

Em indústrias e em empresas que se relacionam diretamente com o cliente final, sistemas embarcados intercomunicantes tem o poder de aumentar a produtividade, criar novas estratégias de produção e conhecer melhor o mercado. Esse conceito é chamado de *Smart Industries* ou ainda *Industries 4.0.*

Com a inclusão de Iot nas empresas há pontos importantes que se destacam, como:

1) Economia – possibilita a redução de funcionários, a melhoria da vida útil de equipamentos, à redução do consumo de energia, água e suprimentos;
2) Interação – possibilita maior interação entre os fatores que englobam um processo com um todo. Proporcionando, por exemplo, a criação de uma melhor interação com clientes de maneira a prever e atender suas demandas e expectativas;
3) Erros e falhas – auxilia na prevenção de possíveis erros e falhas;
4) Maior autonomia – as máquinas deixariam de depender 100% da interação humana e dos colaboradores, fazendo com que os funcionários tenham maior disponibilidade para se dedicar às funções mais estratégicas e focadas;
5) Tomada de decisões – O acesso a dados em tempo real possibilita aos gestores informações mais precisas para uma tomada de decisões mais acertada.

Figura 4. Principais benefícios esperados pelas empresas na implementação de soluções da IoT, 2106



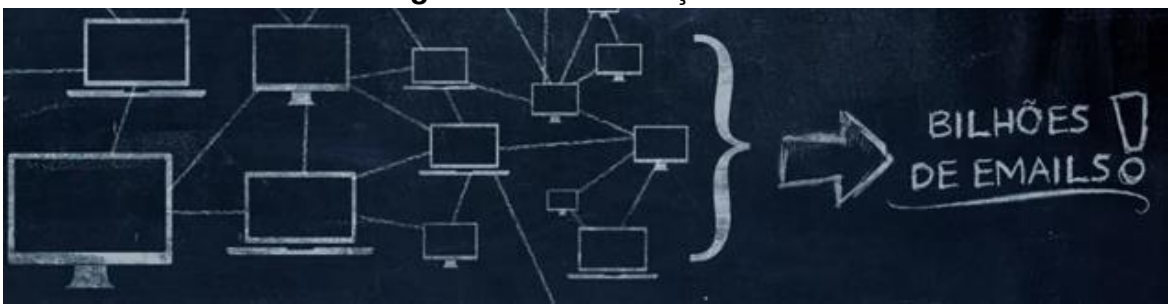
Fonte: http://cio.com.br/tecnologia/2016/11/30/maioria-das-medias-egrandes-empresas-brasileiras-implementara-iot-nos-proximos-12-meses/

7. COMO PODE ATRAPALHAR

Com o advento de novas tecnologias bem como carros, casas e outros aparatos inteligentes (aqueles com conexão à internet) a vida dos hackers foi facilitada, oferecendo a infecção de novos dispositivos devido a menor segurança e pouca atualização, sem mencionar a dificuldade de notar a infecção.

É possível também a expansão de Botnets (máquinas com programa de comando-controle podendo ser acionadas remotamente para obedecer a ordens) através destes dispositivos, que atuam de maneira orquestrada, podendo causar ataques do tipo DDOS (negação de serviço) bem como ataques de SPAM.

Figura 5. Disseminação



Fonte: https://www.youtube.com/watch?time_continue=120&v=wZvDZfO13mA

O avanço da IoT pode representar não só uma ameaça para si mesmo, como perda de privacidade e ou desempenho, mas também uma ameaça aos outros por exemplo a infecção de outros aparelhos e os ataques mencionados anteriormente.

Figura 6. Infecção de outros aparelhos

Fonte: https://www.youtube.com/watch?time_continue=120&v=wZvDZfO13mA

Em um cenário pouco mais futurista onde cidades inteiras dispõem de tais objetos inteligentes é provável que ataques possam danos imensuráveis a empresas e órgãos públicos. Sem mencionar ataques como:

1) Cobrar extorsão;
2) Gerar cliques falsos;
3) Queda de serviço;

> Esses aparelhos têm sido alvos de ataques, muitas vezes, apenas na intenção de transformá-los em zombies, bots, de forma que fiquem à disposição daqueles que infectaram eles, podendo a qualquer momento serem usados em ataques, normalmente de negação de serviço. Além disso, quando um invasor se passa por um usuário legítimo, autorizado, ele pode furtar informações ou mesmo danificar fisicamente e/ou logicamente tais aparelhos.
> Muitos desses aparelhos conectados à Internet, não são apenas de uso caseiro. Em vários casos, possuem uso critico como em

> sistema de controle de radares do espaço aéreo, sensores de medição nível de chuva ou mesmo de controle de temperatura em uma linha de montagem em uma fábrica. Tais aparelhos podem estar submetidos a tarefas que necessitam precisão e disponibilidade, e caso não cumpram corretamente seus objetivos, podem levar a prejuízos ou mesmo riscos a integridade das pessoas.(TONEZER, 2017)

8. QUESTÕES/DILEMAS:

A conexão com a rede mundial de computadores viabilizará controlar remotamente os objetos e permitirá que os próprios objetos sejam acessados como provedores de serviços. Esta nova capacidade dos objetos gerará um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial; entretanto, estas possibilidades apresentam riscos e amplos desafios técnicos e sociais.

Alguns desafios que devem ser elencados são:

1)Segurança;
2)Privacidade;
3)Infraestrutura.

Já com relação a implementação podemos citar:
Como é possível analisar nas imagens à seguir ainda há alguns desafio de implementação assim como:

Figura 7. Principais desafios na implementação de projetos da IoT, 2016

Fonte: http://cio.com.br/tecnologia/2016/11/30/maioria-das-medias-egrandes-empresas-brasileiras-implementara-iot-nos-proximos-12-meses/

Muitos desafios ainda têm que ser superados para que equipamentos conectados passem a ser parte e nosso dia a dia, a internet das coisas ainda está em sua infância e tem vários obstáculos a vencer. Ele cita que o principal desafio são as redes que servem para conectar os sensores ou smartphones aos servidores da internet que prestam estes serviços. “A forma como estas foram construídas não comportam a explosão de volume de conexões e Megabytes previstos”.

Não são poucas as questões que devem ser consideradas, entretanto, a certeza que temos é que a tecnologia não pode, nem deve regredir, sendo assim, nossos esforços devem estar voltados para as soluções dos problemas que a Internet das Coisas pode causar e não permitir que esta tecnologia deixe de nos oferecer sua gama de benefícios.

9. SUGESTÕES DE SOLUÇÕES

Algumas das sugestões elencadas são: manter firmware atualizado, investir em segurança digital, aprimorar o gerenciamento remoto, lançar atualizações frequentes, criar política de acesso entre inúmeras outras que são contempladas pelos fatores a seguir:

1. **Segurança Holística:** diz respeito à proteção integral de uma infraestrutura de rede. O que abrange habilitar tecnologias com capacidade para monitorar as operações de rede e consequentemente detectar de maneira automática, ameaças e reduzi-las. E assegurar paralelamente os pilares da segurança da informação (a confidencialidade, integridade e disponibilidade) de quaisquer dados que sejam enviados pela rede;
2. **Software responsivo:** exige, através de uma abordagem centrada em aplicativos, a ativação da infraestrutura a fim de constatar rápida e automaticamente as demandas de tráfego e fluxos, sem mencionar a adaptação aos mesmos. O que permite que a infraestrutura “reaja” a mudanças nas condições

originais e a problemas potenciais, sem afetar a segurança ou a disponibilidade;

3. **Segurança adaptável e em tempo real:** trata-se de lidar com a segurança de acordo com o crescimento, através da segurança adaptável. Conforme a instituição progride, devem ser estabelecidos os níveis de segurança a fim de minimizar riscos;
4. **Conexões seguras e dinâmicas:** garantem um nível adequado de segurança que perdure em todas as conexões simultaneamente (Cálculos de segurança avançada e os protocolos auxiliam a estar em conformidade com a regulamentação e com a privacidade);
5. **Proteção do cliente e confiança na marca:** redução do impacto e custo de violações de segurança a partir de uma estratégia (de segurança) integral, de forma a detectar, confirmar, limitar e encarar ameaças. Evitando assim a perda de confiança do cliente e asseguram a integridade da marca;
6. **Controle de acesso:** fornece acesso de acordo com políticas para quaisquer dispositivos ou usuários que se conecte a rede. Os mesmos são autorizados e autenticados para verificar conformidade com a política de segurança;
7. **Políticas com reconhecimento de contexto:** utilizam de linguagem comercial descritiva simplificada para estabelecer políticas de segurança fundamentado no cenário completo da organização. Estas políticas alinham-se com as políticas empresariais e mais claras para administrar a empresa como um todo, também assistência a corporação a prover uma segurança mais eficaz e responder aos objetivos de conformidade com maior eficiência operacional e controle.

Outra contramedida que pode ser usada para reduzir as questões de privacidade os dados e o número de ataques bem-sucedidos é o uso de mensagens seguras por meio de medidas criptográficas inclusivamente nas camadas de roteamento

Mensagens que forem criptografadas vão garantir que um invasor não possa ler o conteúdo de uma mensagem sem possuir a chave descriptográfica. Já as mensagens que forem autenticadas de forma correta não podem ser falsificadas. Os dispositivos estrangeiros não poderão adulterar identidades quando a autenticação é necessária.

Outra medida a ser empregada é o projeto de protocolos meticulosos, que contam com políticas de prevenção de ataques além de apenas garantir a comunicação

Estes protocolos também podem permitir que partes confiáveis tenham participação no que diz respeito as decisões de roteamento. Combinando criptografia e protocolos protegidos

> podem também mitigar a análise de tráfego, garantir que todas as mensagens tenham o mesmo tamanho e a transmissão de mensagens falsas entre os dispositivos. (Figueira, 2016)

10. POLÍTICA DE SEGURANÇA

Uma política de segurança define as regras, as normas e os procedimentos que devem ser seguidos para manter uma empresa, seus funcionários e os sistemas seguros. Uma política de segurança pode ser dividida em várias áreas diferentes para solucionar tipos específicos de risco.

Para alguns a parte mais importante de uma política é a educação do usuário. As pessoas regidas pela política de segurança não apenas devem estar cientes dessa política, mas devem entendê-la e segui-la para garantir a segurança das pessoas, dados e coisas.

A harmonia entre a política e o desenvolvimento das atividades de cada “coisa” envolvidas nos processos cotidianos dos usuários são a chave para o sucesso desta tecnologia. Para isso é possível catalogar algumas políticas que podem auxiliar a alcançar esse objetivo:

1. **Política de acesso remoto:** busca definir quem, como, quando e quais dispositivos podem se conectar remotamente a um sistema, sem mencionar que a mesma é responsável por definir quais recursos serão acessíveis pelo usuário remoto;
2. **Política de privacidade:** estabelece os métodos que serão utilizados para preservar as informações de acordo com a sensibilidade e classificação de cada uma (quanto mais confidencial uma informação maior o nível de proteção destinado à mesma);
3. **Política de segurança física:** indica como os recursos físicos serão preservados, por exemplo, o bloqueio de recursos em períodos de não utilização dos mesmos, além de manter estes em área restritas a profissionais competentes e designados para lidar com tais recursos;
4. **Política de segurança dos computadores:** define o modo como usuários são permitidos ou negados a utilizar de um computador, ou seja, quem pode usar qual

computador e quais programas este deve ter acesso a fim de não comprometer dados que não são destinados a um usuário em particular;

5. **Política de senhas:** indica qual senha será empregada para acessar recursos específicos e consequentemente a complexidade desta senha, bem como determinar a periodicidade para a alteração da mesma.

11. NECESSIDADE DE SEGURANÇA ADICIONAL

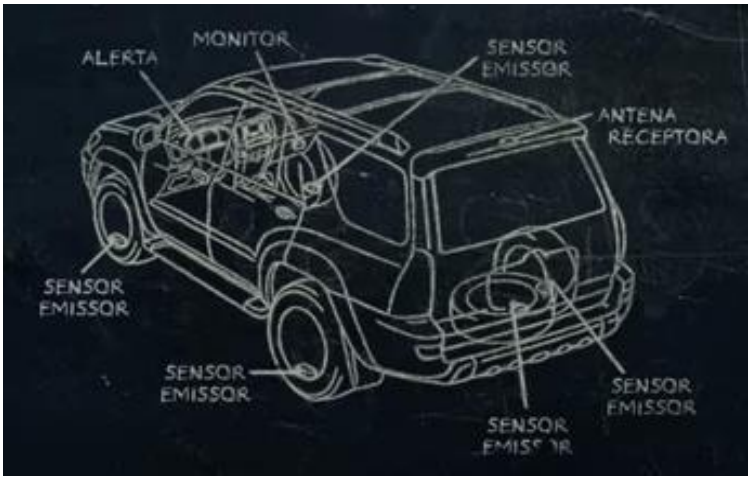
Somado a tudo que foi dito se faz relevante salientar a necessidade de segurança extra, tal como autenticação em dois fatores, biometria, entre tantas outras tendências tecnológicas disponíveis.

Com o número crescente de equipamentos conectados e como resultado a parcela de dados que gerados por estes há o aumento na demanda pela segurança destes dados.

Ataques de hackers ocorrem diariamente e nenhuma pessoa está imune. Como é fácil roubar e usar dados de maneira imprópria no mundo conectado contemporâneo é muito recorrente preocupar-se com esse problema, visto que pessoas, processos, dados e coisas estão conectados na IoT. Basta imaginar as possibilidades que um carro com diversos sensores pode oferecer para um indivíduo mal-intencionado e com a capacidade de invadir tal sistema, sendo possível até mesmo interferir nos freios de um veículo de forma a causar danos ao motorista.

A partir da expansão destes tipos de dispositivos tecnológicos, os riscos que envolvem a sua implantação também se multiplicam, como na figura a seguir.

Figura 8. Equipamentos conectados



Fonte: https://www.youtube.com/watch?time_continue=120&v=wZvDZfO13mA

Para se ter uma ideia dos perigos, podemos exemplificar com um caso ocorrido em janeiro de 2017, onde um hotel da Áustria teve que pagar uma recompensa para um hacker que trancou todos os quartos do estabelecimento através de um ataque cibernético, sem mencionar o *Reveton* (ferramenta maliciosa que sequestra o navegador da vítima a fim de direcionar o computador infectado para sites específicos) “Cryptolocker”, que direcionava o computador da vítima para sites que emitia alertas policiais que exigiam que os usuários pagassem multas além do último ciberataque em massa nos Estados Unidos, que afetou no mínimo 85 serviços como Netflix, Spotify e redes sociais, foi em parte culpa de dispositivos de IoT. A fabricante chinesa Hangzhou Xiongmai Technology reivindicou parte do problema. Suas câmeras conectadas à internet apresentavam uma falha básica em seus códigos, permitindo que hackers conseguissem instalar um vírus chamado Mirai e depois pudessem lançar ataques que sobrecarregavam os servidores de internet.

12. ESTRATÉGIA DE SEGURANÇA

Quanto maior e mais integrada for a solução de IoT, mais descentralizada a rede torna-se. Isso possibilita um maior número de

access points na rede, o que pode conceber um número maior de vulnerabilidades. Um número considerável de aparelhos que se comunicam através da IoT transmitirá dados a partir de locais não confiáveis, mas o transporte deve ser seguro. No entanto, proteger determinada solução pode se mostrar difícil em virtude da quantidade de sensores, “coisas” inteligentes e dispositivas conectadas à rede. O prejuízo potencial causado pela permissão (indevida) de que dispositivos não seguros acessem a rede de uma empresa é um desafio expressivo para os profissionais de segurança, o que nos leva ao seguinte questionamento: Como uma empresa ou um indivíduo pode se beneficiar da IoT enquanto gerenciam riscos?

Figura 9. Possíveis problemas dos dispositivos conectados

Fonte: https://www.youtube.com/watch?time_continue=120&v=wZvDZfO13mA

13. ARQUITETURA DE SEGURANÇA

A segurança de redes da IoT não pode ser sintetizada exclusivamente a dispositivos específicos. Ao invés disso, é preciso programar uma solução de ponta a ponta. Uma solução de segurança que disponibiliza proteção com gerenciamento centralizado e execução distribuída deve ser integrada em toda a rede, a fim de extrair o máximo de eficácia (em termos de segurança) que o sistema

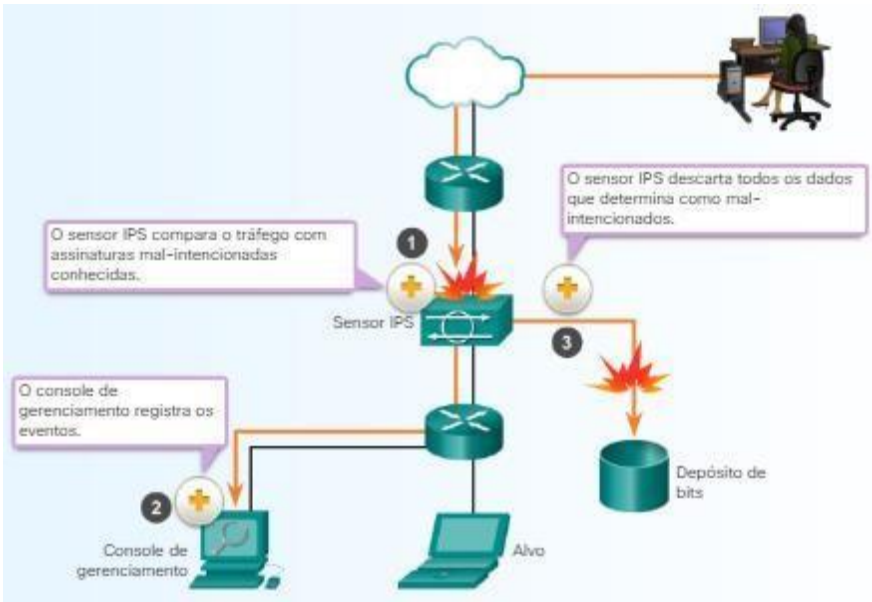
permite. O monitoramento contínuo de atividades na rede é fundamental para agregar e correlacionar dados em todo o ambiente conectado, tirando proveito de informações e agindo, quando necessário (sendo um monitoramento reativo a partir de eventos decorridos no cotidiano).

14. DISPOSITIVOS DE SEGURANÇA

Alguns dos dispositivos são imprescindíveis na arquitetura de segurança por viabilizar ações tais como controle de acesso, inspeção conteúdo e imposição de políticas, entre eles destacaram:

1) **Firewalls:** cria uma barreira entre duas redes, analisa o tráfego de rede para determinar se o tráfego pode navegar entre duas redes em um conjunto de regras predefinidas;
2) **Sistemas de prevenção contra invasões (IPS):** monitora atividades em uma rede e determina se são mal-intencionadas. Um IPS se incumbe de impedir ataques liberando o tráfego de dispositivo ofensivo ou restaurando uma conexão.

Figura 10. Operações do sistema de prevenção de intrusão



Fonte: https://1360665.netacad.com/courses/456510

15. SEGURANÇA PARA CONEXÃO SEM FIO

As dificuldades de manter uma rede com fio segura são expandidas com uma rede sem fio. Uma rede sem fio está vulnerável a qualquer pessoa dentro do alcance de um *Access point* e as devidas credenciais associadas a ela.

A segurança sem fio normalmente é implementada no access point ou no ponto em que a conexão sem fio participa da rede. A segurança sem fio básica inclui:

1. Configuração de protocolos de autenticação fortes com senhas fortes;
2. Configuração da segurança administrativa;
3. Habilitação da criptografia;
4. Alteração de todas as configurações padrão;
5. Manutenção das atualizações do firmware.

No entanto, mesmo com essas configurações, com um equipamento sem fio e conhecimento de técnicas de *hacking*, um invasor pode acessar a rede de uma empresa ou de um indivíduo. Além disso, muitos dispositivos sem fio que se conectam à IoT não são compatíveis com o recurso de segurança sem fio. Por esse motivo, o tráfego de dispositivos móveis inteligentes e sem fio e o tráfego de sensores e objetos incorporados devem passar pelos dispositivos de segurança e pelos aplicativos sensíveis ao contexto da rede.

16. CONCLUSÃO

Mediante as informações expostas anteriormente é notório como os usuários deste tipo de tecnologia se encontram vulneráveis, enquanto obtêm inúmeras facilidades encontram se em um ambiente insuficientemente apto a implementação em largas escalas, sem mencionar o fato de que muitos órgãos públicos estão cada vez mais integrados, se tornando, portanto, alvos em potencial. Caso seja adotado prosseguir com a implementação, é necessário reforçar as medidas de segurança a fim de tornar a experiência o mais agradável e segura possível. Além disto vale salientar a importância de uma transição apropriada para esta tecnologia e consequentemente a minimização de qualquer prejuízo ou outro tipo de problema que possa vir a acontecer neste período. Deste modo, é imprescindível relembrar que como qualquer tecnologia, a IoT não é boa ou ruim, e, sim responsável por auxiliar pessoas, independentemente de suas intenções. Deve-se ressaltar também que, as medidas de segurança devem ser tomadas após avaliar os riscos aos quais estarão sujeitos os usuários do novo sistema na execução de quaisquer tipos de tecnologias, servindo assim a segurança da informação de modo a amparar as tecnologias existentes e vindouras.

17. REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO, Marcio. **IoT – Internet das Coisas: motivação, benefícios e segurança**. Disponível em: <http://www.afrikatec.com.br/iot-internet-das-coisasmotivacao-beneficios-e-seguranca/>. Acesso em 22/05/2018

FIGUEIRA, Vitor Pinheiro. **Internet das Coisas: Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura**. 2016. 66 p. Tese de conclusão de curso (Tecnólogo em Sistemas de Computação)- UNIVERSIDADE FEDERAL FLUMINENSE, Niterói, [2016]. Vol: 1.

GEREMIAS, Thiago et al. **A internet das coisas: será a internet do futuro ou está prestes a se tornar a realidade do presente?** v.1, p.10, 2015. Artigo Científico (Bacharelado em engenharia de telecomunicações) - Faculdade de engenharia e arquitetura - FUMEC, Belo Horizonte, 2015. 1.

LEYDEN, John. **Charlie Miller to tell Vegas how to hack your car.** Disponível em:<www.theregister.co.uk/2013/06/25/miller_car_hacking/>. Acesso: 18/06/2018.

MARTINS, I. R.; ZEM, J. L. Estudo dos Protocolos de Comunicação MQTT e CoAP para Aplicações Machine-to-Machine e Internet das Coisas. **Revista Tecnológica da Fatec Americana**, v. 3, n. 1, p. 24, 2016.

NERDOLOGIA. **Botnets: um exército zumbi pronto para atacar**. 2016. 1 post (5 min 56 s). Postado em: 2016. Disponível em: < https://www.youtube.com/watch?v=fey7JS-1R6Q>. Acesso em: 18/06/2018.

SIQUEIRA, Diego; ANDRADE LIMA, Assis; PAULO, João; MORENO, David. **Segurança em Redes de Sensores sem Fio: Desafios, Tendências e Orientações**. v.13, ed. 1, p 402-411, 2015 [S.l.]: Revista Gestão. Org.

SOPRANA, Paula. **A segurança negligenciada da Internet das Coisas**. 2016. Disponível em: <https://nic.br/noticia/na-midia/a-seguranca-negligenciada-da-internet-das-coisas/>. Acesso em: 18/06 2018.

SMITH, A; Jones, B***. On the complexity of computing. In Advances in Computer Science***, p. 555–566, Editora de Imprensa 1999.

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

Rafael Teodoro Bueno

A relevância da segurança da informação na Internet das Coisas

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Internet das Coisas

Americana, 03 de dezembro de 2018.

Banca Examinadora:

Adriano Cirros Doimo (Presidente)
Pós graduação em Tecnologia na Gestão da Informação
Faculdade de Tecnologia de Americana

José Luis Zem (Membro)
Doutorado em Física Computacional
Faculdade de Tecnologia de Americana

Benedito Aparecido Cruz (Membro)
Bacharelado em Ciencia da Computação
Faculdade de Tecnologia de Americana