FACULDADE DE TECNOLOGIA DE SÃO PAULO

FRANCIELLY NASCIMENTO PEREIRA

A indústria 4.0: Vulnerabilidades Causadas por redes IoT

SÃO PAULO

2021

FACULDADE DE TECNOLOGIA DE SÃO PAULO

FRANCIELLY NASCIMENTO PEREIRA

A indústria 4.0: Vulnerabilidades causadas por redes IoT

Trabalho submetido como exigência parcial
para a obtenção do Grau de Tecnólogo em
Análise e Desenvolvimento de Sistemas
Orientador: Prof. Valter Yogui

SÃO PAULO
2021

FACULDADE DE TECNOLOGIA DE SÃO PAULO

FRANCIELLY NASCIMENTO PEREIRA

A indústria 4.0: Vulnerabilidades causadas por redes IoT

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador
_____
_____
_____

Conceito/Nota Final: _____

Atesto o conteúdo contido na postagem do ambiente TEAMS pelo aluno e assinada por mim para avaliação do TCC.

Orientador: Prof. Valter Yogui

SÃO PAULO, ____ de _____ de 2021.

Assinatura do Orientador

Assinatura do aluno

Dedicatória

Dedico esta monografia à minha família, que deu todo o incentivo para sempre continuar com meus estudos e aos meus professores, que foram muito além de seus deveres para fornecer insumos e fomentar minha curiosidade.

Agradecimentos

A Deus, que pela fé me deu forças para atravessar os períodos mais complicados da vida.

A minha família, que com muito carinho e esforço, permitiu que eu tivesse a melhor educação possível.

Aos meus professores, que com todo trabalho empregado, me ajudaram a seguir meu próprio caminho.

Aos meus amigos, que me incentivaram a continuar.

Resumo

A 4ª revolução industrial está atualizando o mercado e transformando pelo uso da tecnologia, processamento e análise de dados a forma que as empresas trabalham. Para isso, a própria existência da indústria 4.0 se mescla com a utilização da IoT que permite a coleta de dados, processamento, análise e atuação sobre a produção, muitas vezes, sem a necessidade de que haja interferência humana. No entanto, o funcionamento da IoT também exige um grande tráfego de dados e informações que, quando utilizados indevidamente, podem ocasionar grandes problemas, desde questões financeiras, até questões de risco à saúde. A aplicação de objetos conectados é muito ampla e tais tecnologias, muitas vezes, não possuem protocolos apropriados para proteção da rede em que estão inseridos. O presente trabalho disserta sobre a indústria 4.0, a internet das coisas e sua inserção na indústria, na vida das pessoas e problemas que pode causar se não assegurada devidamente.

Palavras-Chave: Indústria 4.0, Internet das coisas, vulnerabilidades, IOT, segurança.

Abstract

The 4ª industrial revolution is updating the job market and changing through the use of technology, processing and data analysis the way companies work. To do this, the own industry 4.0's existence mixes with the use of IoT which allows collecting data, processing, analysis and acting on production, oftenly, without the need for human interference. However, the functioning of the IoT also requires a large amount of data and information traffic that, when misused, can cause major problems, from financial issues to health issues. The application of connected objects is very wide and such technologies often do not have appropriate protocols for protecting the network in which they are inserted. This work discusses industry 4.0, the internet of things and its insertion in the industry, in people's lives and problems it can cause if not properly ensured.

Keywords: industry 4.0, internet of things, vulnerabilities, IOT, security.

Sumário

1.Introdução

Em 1760 iniciava-se na Inglaterra a primeira revolução industrial, na qual os antigos processos que eram feitos manualmente por artesãos passaram a ser desenvolvidos dentro de fábricas, com a divisão do trabalho e com o auxílio de máquinas a vapor.

Entre 1850 e 1870 iniciou-se a segunda revolução industrial. A industrialização, que se concentrava na Inglaterra, passou a se espalhar por outros países como Estados Unidos, França, Rússia, Japão e Alemanha. A energia a vapor passou a ser substituída pela energia elétrica e o carvão passou a ser substituído pelo petróleo.

Após o fim da Segunda Guerra Mundial a indústria passou por sua terceira revolução, também conhecida como revolução técnico-científica-informacional. Nessa fase, indústrias de metalurgia, siderurgia e de automóveis, que foram altamente desenvolvidas nas revoluções anteriores, se viram em desvantagem em relação a outras indústrias que passaram a investir em alta tecnologia como robótica, genética, informática, telecomunicações e eletrônica.

Já em 2011, na feira de Hannover Messer, principal feira de tecnologia industrial do mundo, o governo alemão, vendo a necessidade de dar um rumo para o desenvolvimento da indústria do país, lançou um programa chamado Plattform Industrie 4.0. O intuito era desenvolver alta tecnologia, de forma que, as empresas, já automatizadas, conseguissem criar uma rede de sistemas que pudessem conversar entre si, trocando informações entre máquinas e humanos, para otimizar a produção. Na época, criou-se uma parceria público-privada, que em 2013, lançou a plataforma Indústria 4.0, divulgada por empresas, academias e associações.

Nesse momento o mundo passa por sua quarta revolução industrial, a fim de elevar ao máximo o potencial da automação, de forma que robôs desempenhem funções cada vez mais complexas. Sendo assim, a indústria pretende se tornar cada vez mais rápida, inteligente e precisa.

Em 2015, um estudo apresentado pela consultoria PwC Strategy&, já mostrava o potencial da indústria. Empresas alemãs indicavam que pretendiam investir cerca de 3.3% de seus faturamentos anuais em soluções da indústria 4.0, indicando assim um investimento de 40 bilhões de euros anuais até o ano de 2020.

Esse investimento seria refletido em um aumento de aproximadamente 20% da eficiência da produção e uma redução de custos de até 2,6%.

Um dos pilares da indústria 4.0, sem dúvida, é a internet das coisas (IoT). Pode-se dizer que, de forma geral, a IoT pode ser entendida como "(...) um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua) (...)" (MAGRANI, 2018).

Pesquisas da Gartner Research indicaram que o número de coisas conectadas à internet chegariam a 20,4 bilhões em 2020 e esse valor seria elevado para 25 bilhões em 2021.

Com um grande número de dispositivos conectados, coletando quantidades massivas de dados a todo momento, é natural que a segurança sobre o tráfego, armazenamento e tratamento de tais dados deva ser tratada com grande relevância.
Pode-se citar o caso do botnet Mirai, que é voltado para atacar especificamente equipamentos IoT. Em 2016, esse botnet fez uma ataque massivo que deixou mais de 1 milhão de alemães sem acesso à internet.

Dessa maneira, o presente trabalho pretende fazer um estudo sobre as vulnerabilidades que a internet das coisas pode causar na indústria 4.0.

2.A indústria 4.0

2.1.Contexto histórico

A humanidade passou por diversas revoluções ao longo de seu desenvolvimento para chegar ao ponto que está. Embora o termo “revolução” denote um processo abrupto e violento, a primeira pela qual a humanidade passou foi a transição de uma vida nômade, de forrageamento, para a produção agrícola. Essa mudança ocorreu há cerca de 10.000 anos atrás e levou muito tempo para ocorrer completamente.

Com ela, no entanto, foi possível o crescimento populacional e a criação de assentamentos maiores da nossa espécie, levando à criação da urbanização e de

grandes cidades. Sendo assim, ela acabou permitindo também que outras revoluções ocorressem posteriormente, como as revoluções industriais.

A primeira revolução industrial ocorreu aproximadamente entre 1760 e 1840. A construção de ferrovias e a invenção de máquinas a vapor permitiu que a produção, que antes era manual e feita por artesãos, ou seja, o processo produtivo era feito do começo ao fim por uma pessoa que detinha todo o conhecimento, passou a ser dividido.

A segunda revolução industrial iniciou aproximadamente ao final do século XIX, substituindo o vapor pela eletricidade. As linhas de montagem da época passaram a permitir que a produção fosse feita em massa e a industrialização, que até então se concentrava na Inglaterra, passou a se espalhar pelo mundo.

A terceira revolução industrial começou na década de 1960 e ficou conhecida como a revolução digital, uma vez que tenha sido impulsionada pelo desenvolvimento dos semicondutores, dos mainframes (nos anos 60), computadores pessoais (entre os anos 70 e 80) e por fim da internet (nos anos 90).

A quarta revolução industrial se deu início na virada do século, e “É caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina).” (SCHWAB, 2016).

Embora as tecnologias relativas aos computadores não sejam novas, como softwares e redes, estas estão cada vez mais sofisticadas e alterando consideravelmente o modo de produção instaurado pela terceira revolução por meio da automação.

A Alemanha, na feira de Hannover de 2011, cunhou o termo “indústria 4.0”, onde iniciaram-se as discussões de como poderia ser conduzido o andamento dessa nova fase da indústria, que está vendo a organização das cadeias globais de valor serem alteradas.

2.2.O que é a Indústria 4.0

A indústria 4.0 refere-se à quarta revolução industrial e engloba avançadas tecnologias de produção que captam, processam e enviam dados. Pode-se dizer que tudo que está dentro e fora de uma planta industrial está conectado digitalmente, permitindo que a cadeia de valor seja altamente integrada e automatizada.

Nesse tipo de indústria, é comum que ocorra a descentralização do controle dos processos. Isso ocorre porque, com a alta integração entre as máquinas e maior poder de processamento e análise de dados, não há a necessidade de que um humano tenha que interagir com o processo e o próprio maquinário pode se auto ajustar, prevendo assim falhas e a necessidade de manutenção.

Segundo o Sebrae (2018), uma das vantagens da indústria 4.0 é a capacidade de aproximar o consumidor da indústria, uma vez que, com máquinas “inteligentes” e automação, a produtividade cresce, atendendo ao volume solicitado pelo mercado, em um tempo menor. Isso permite que nichos mais específicos também possam ser atendidos, com produtos customizados de maior valor agregado.

Outros diferenciais que esta indústria pode apresentar:

- Operação em tempo real: coleta em análise de dados permite que tomadas de decisão sejam tomadas com mais assertividade;
- Descentralização: a própria máquina possui capacidade de tomar decisões;
- Modulação da produção: a produção pode ser customizada e se adaptar automaticamente à demanda do mercado;
- Rastreabilidade e Monitoramento: com diversas câmeras e sensores, o controle da linha de produção pode ser feita remotamente;
- Maior segurança: o processo pode ser rastreado a todo momento, aumentando a segurança e permitindo maior transparência no processo;
- Menos custos: a produção fica mais barata com a redução da mão de obra, automatização do processo e auto regulagem das máquinas.

Para providenciar tais benefícios, segundo o Boston Consulting Group (BCG), a Indústria 4.0 utiliza-se de 9 tecnologias que impulsionam seu funcionamento.

2.2.1.Manufatura aditiva

A manufatura aditiva, segundo a 3DLAB (maior empresa de soluções em impressão 3D do Brasil), utiliza-se de tecnologias que permitam a impressão 3D, ou seja, a produção é feita a partir de modelos digitais.

Tais tecnologias trazem algumas vantagens para a indústria.

- Custo: peças podem ser produzidas em quantidades menores, reduzindo o custo unitário;
- Rapidez: a transição do modelo digital para o físico é eficiente e rápido, possibilitando que protótipos sejam criados em menor tempo;
- Complexidade: peças geometricamente complexas podem ser criadas;
- Customização: permite a produção de peças variadas, de acordo com a solicitação do cliente;
- Economia/Sustentabilidade: essa tecnologia permite que as peças sejam produzidas sem o desperdício de materiais, economizando energia e gerando menos refugo.

Figura 1 - Impressora 3D

Fonte: 3dlab (2019)

Sendo a manufatura aditiva um conjunto de tecnologias que produzem objetos físicos a partir de um modelo digital, na Figura 1 temos um exemplo de impressora 3D que pode produzir peças utilizando resina líquida. De forma geral essa impressão 3D pode ser dividida em 3 etapas. A primeira delas é a modelagem digital, na qual o objeto a ser produzido é criado primeiramente através de software. Na segunda etapa, o modelo criado anteriormente é dividido em camadas, os parâmetros são estabelecidos e o arquivo é criado. Por fim, a terceira etapa é constituída pelo envio do arquivo gerado na etapa anterior para a impressora 3D, que iniciará a produção da peça, depositando a matéria prima em camadas (que pode ser polímero em forma de filamento, ou resina líquida, dependendo do tipo de impressora). O tempo para a produção da peça vai variar conforme sua complexidade, podendo ser de algumas horas ou até mesmo alguns dias.

2.2.2. Realidade aumentada

A realidade aumentada (RA) na indústria 4.0 permite que cenários virtuais sejam projetados sobre o mundo físico. Considerando a coleta de dados através dos sistemas industriais, GPS, câmeras e internet, integrados a um aparelho móvel, é possível fazer o acompanhamento virtual de diversos processos da indústria. Gestores podem fazer o acompanhamento da produção, operários podem controlar máquinas à distância e até mesmo a manutenção e segurança do ambiente podem ser orientadas remotamente por especialistas.

As vantagens na utilização dessa tecnologia são diversas. Suas projeções permitem que detalhes em tempo real sejam observados, quando, em um processo comum, não seria possível fazer o mesmo, o que poderia prejudicar a eficiência produtiva. Quando associada com uma inteligência artificial, a realidade aumentada permite que falhas e desvios operacionais sejam percebidos antes que eles ocorram, permitindo que técnicos façam ajustes sem a necessidade de paralisar a produção.

A RA também permite que modelos de CAD (Computer-Aided Design) e dados provenientes de sistemas de gestão industrial como SCADA, PIMS e MES sejam utilizados como base para a experiência, de forma que, seja possível fazer o controle de processos complexos com grande assertividade, evitando perdas monetárias consideráveis.

Na segurança do trabalho, tal tecnologia permite que gestores monitorem à distância as condições das máquinas, se o operador está utilizando os equipamentos exigidos e as condições do ambiente em geral. Isso permite que processos que exijam manuseio de materiais perigosos, ou em ambientes perigosos (trabalho em altura ou em profundidade), possam ser observados com muito mais detalhes, prevenindo acidentes.

Na questão dos treinamentos, pode-se dizer que os benefícios são trazidos desde a questão monetária, até o aprendizado. Os funcionários conseguem absorver mais informações, podendo compreender, por exemplo, o funcionamento e a montagem da peça de uma máquina, através de modelos 3D, ao passo que, recebem informações e instruções de especialistas que podem estar em uma localidade completamente diferente de onde o treinamento está ocorrendo.

Tais treinamentos influenciam na manutenção também. Funcionários do chão de fábrica podem receber animações que ilustram a forma correta de se trocar uma peça específica da máquina. Diminuindo o tempo levado para compreender como o processo deve ser feito e, consequentemente, diminuindo a chances de se ter problemas durante a manutenção e diminuindo o tempo necessário de parada da máquina.

2.2.3.Robôs autônomos

Robôs autônomos são robôs que podem interagir uns com os outros e com humanos com segurança. Eles são estruturados de forma que atendam ao nível de automação desejada para o trabalho que devem empreender, ou seja, captando dados do ambiente e fazendo suas tarefas sem a necessidade que um humano interfira no processo, podendo, inclusive, realizar sua própria auto-manutenção e alterar a estratégia de ação, se adaptando a diferentes situações.

Eles apresentam 3 grandes habilidades:

- Propriocepção: de forma geral, é a habilidade do robô de compreender sua própria situação, por exemplo, se estão molhados, se desequilibrando, em perigo ou acabando a bateria.
- Realizar tarefas: possuem a habilidade de fazer tarefas repetitivas, perigosas ou inviáveis para os humanos, como o transporte de cargas pesadas no chão de fábrica.

- Localização: conseguem identificar sua localização e mapear a região, para que possam executar suas tarefas corretamente. Muitas empresas utilizam sistemas de faixas no chão para que possam guiar tais robôs. Esse processo utiliza sensores, lasers e câmeras para que a máquina identifique o ambiente ao seu redor.

Essa tecnologia conta com o desenvolvimento de inteligências artificiais, que permitirão que os robôs possuam cada vez mais comportamentos mais complexos. Em São Francisco (EUA), por exemplo, robôs já estão sendo utilizados no combate ao crime, auxiliando nas patrulhas de estacionamentos, arenas esportivas e empresas de tecnologia.

2.2.4. Big Data Analytics

Atualmente, entende-se que a informação é um insumo de grande valor para a indústria uma vez que o entendimento do mercado faz com que as empresas possam ser mais competitivas. Em 2018, a Google já estimava que a internet produzia em torno de 5 exabytes de informação a cada dois dias. Comparativamente, esse volume de dados equivale a mesma quantidade de informação gerada por toda a civilização até o ano de 2003.

A coleta de grande quantidade de dados permite a análise de padrões e, consequentemente, os resultados dessas análises permitem que tomadas de decisão sejam feitas com mais assertividade, no entanto, com o grande volume criado todos os dias, novas ferramentas que comportem o volume, velocidade e variedade de informações passaram a ser necessárias. Big Data, de forma geral, são soluções que conseguem trabalhar sob essas três condições.

Na indústria 4.0 entende-se que a produção tende naturalmente a uma automatização, sendo assim, tal tecnologia está diretamente conectada a IIoT (Industrial Internet of Things), dessa maneira, do fornecedor até o consumidor final, diferentes tipos de informações são coletadas a todo momento por diversos sensores e sistemas diferentes.

Apenas coletá-los não traz vantagens para a produção, no entanto, quando são reunidos e analisados, pode-se compreender padrões e tomar medidas em tempo real de produção. No chão de fábrica, por exemplo, pode-se fazer a análise da qualidade dos

produtos, podendo alterar os parâmetros da produção caso uma anomalia seja detectada. Já nas vendas, pode-se analisar o padrão de consumo, permitindo ações no próprio setor, caso as previsões não sejam satisfatórias, mas também, tomar decisões para outras áreas, como reduzir custos com estoques e comprar com mais precisão os insumos necessários.

2.2.5.Nuvem

Para manter um sistema computacional em funcionamento, é necessário que se mantenha toda uma infraestrutura que o suporte. Geralmente, adquirir, manter e, eventualmente, expandir, exige grande investimento, de tempo, dinheiro e mão de obra.

A computação em nuvem é a oferta de infraestrutura como um serviço, ou seja, a empresa interessada pode contratar a infraestrutura de um provedor, não precisando armazenar seus arquivos em uma estrutura local.

Como benefícios, pode-se economizar com equipamentos e tudo que abrangeria manter um sistema físico (espaço, manutenção, equipamentos, mão-de-obra e etc), há a facilidade de acesso aos dados, que estão sempre disponíveis pela internet e a segurança, uma vez que provedores fazem grandes investimentos na proteção dos dados de seus clientes.

Na indústria 4.0 o armazenamento em nuvem vem ganhando cada vez mais importância, uma vez que uma produção mais inteligente inevitavelmente criará mais dados e necessitará manter o fluxo deles para dar sequência ao trabalho, que poderá ser gerenciado por um funcionário através do software fornecido pelo provedor do serviço.

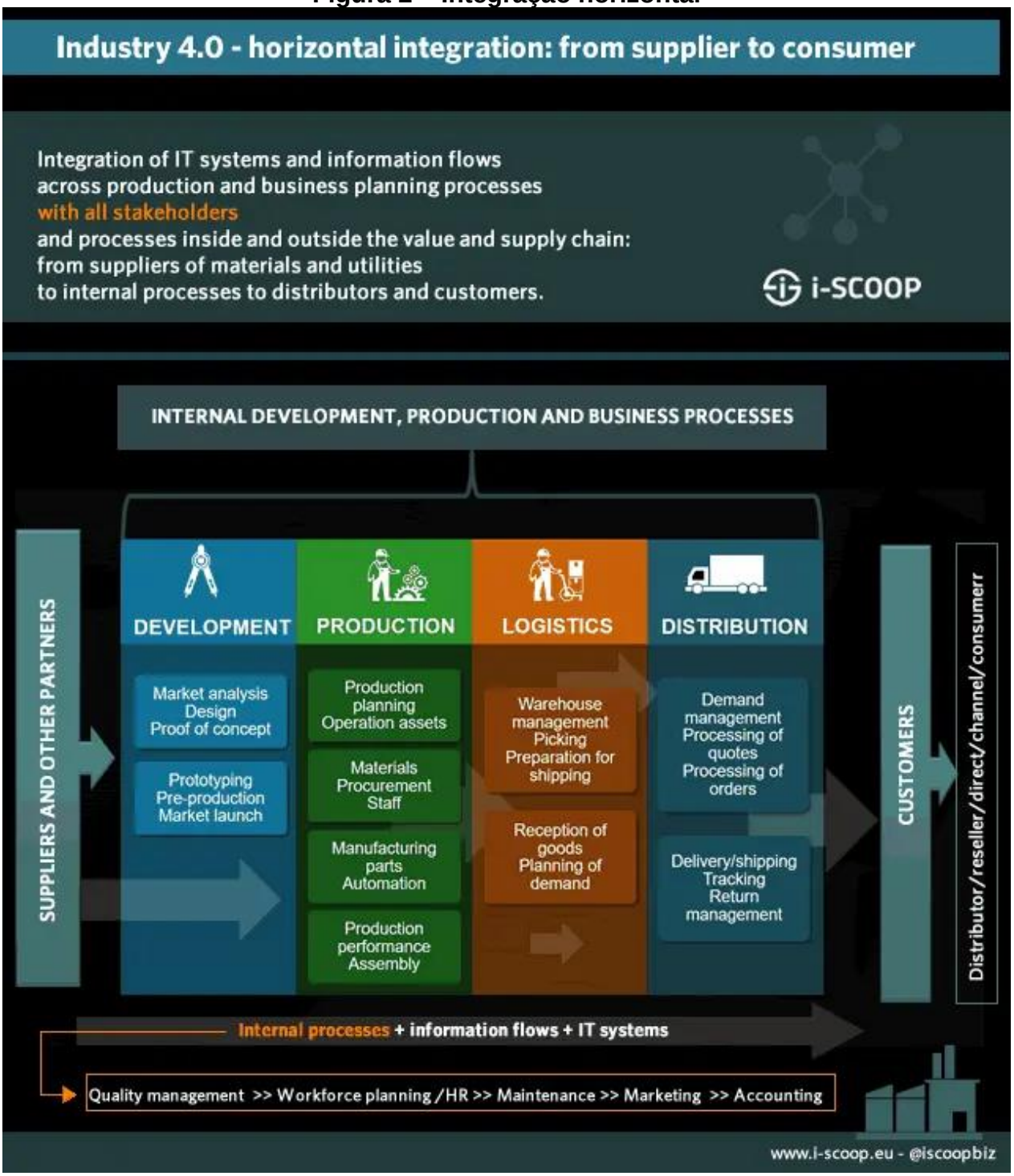
Outro ponto que a Nuvem pode auxiliar é na disponibilização de dados. A informação pode ser segmentada e distribuída para diferentes pontos de produção, levando em consideração o nível de acesso que cada local ou pessoa pode ter.

2.2.6.Integração horizontal e vertical de sistema

Na indústria 4.0, a integração entre equipamentos dentro de fábrica é essencial para que todo processo possa ser monitorado e controlado. Essa ligação entre equipamentos pode ser feita gradativamente, de forma que, uma mesma empresa possua elementos da indústria 4.0 em algumas áreas e trabalhe com elementos menos

conectados em outras. Com a integração vertical/horizontal do sistema o objetivo é que toda empresa passe a trabalhar conectada.

Figura 2 – Integração horizontal



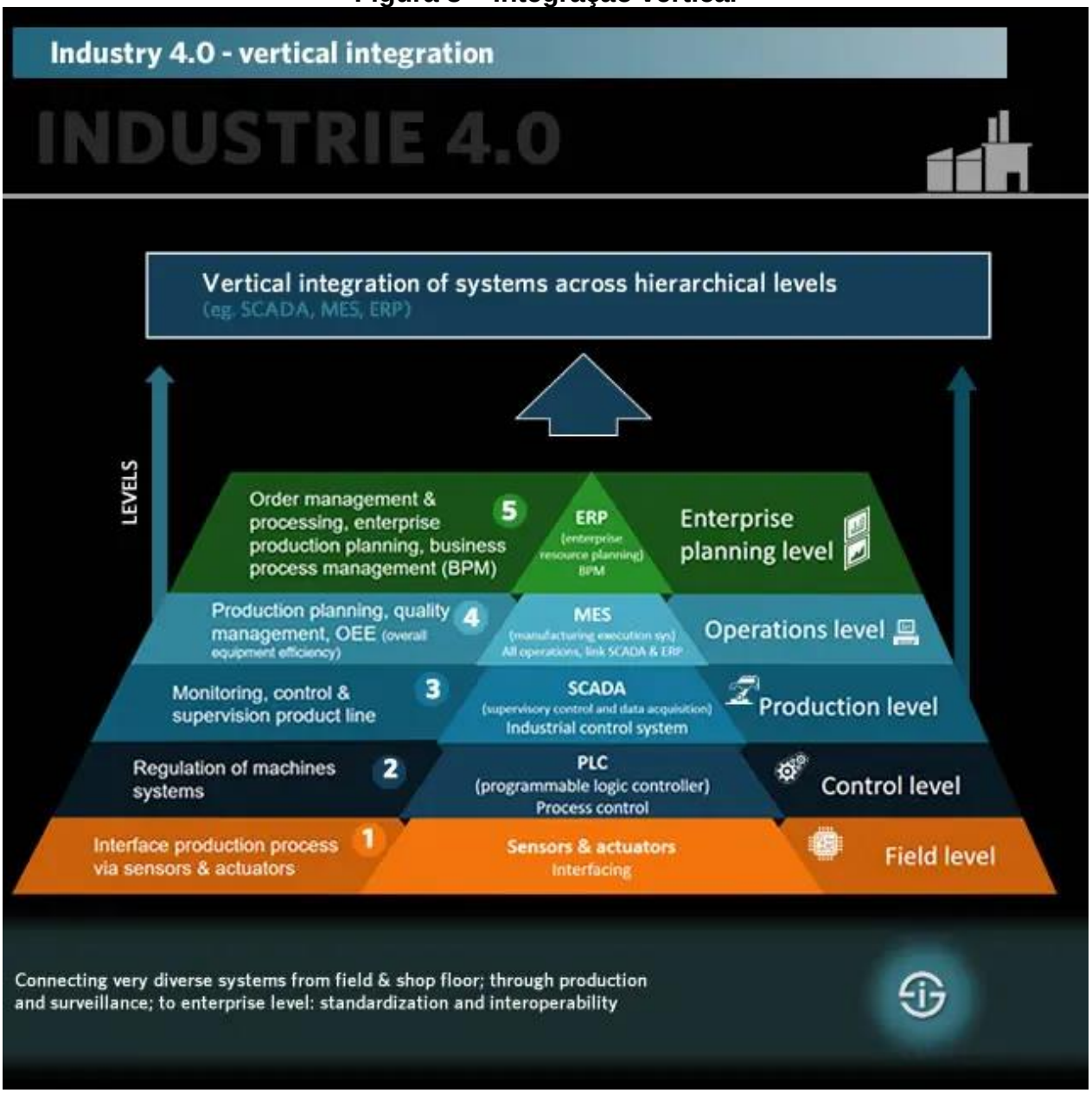
Fonte: i-scoop (2020)

Na Figura 2, exemplifica-se áreas que podem ser impactadas pela integração horizontal de uma empresa. Por fazerem parte de um fluxo, ocorrências que impactem em uma etapa, poderão afetar as anteriores e posteriores, como exemplo, pode-se pensar em um problema na linha de produção que interrompa a fabricação de um produto. A interrupção afeta tanto fornecedores, que fazem uma estimativa de vendas, que não serão alcançadas e, ao mesmo tempo, consumidores podem ser afetados por eventualmente não encontrarem os produtos desejados nas prateleiras das lojas.

Tal integração se trata da digitalização de toda a cadeia de valor da produção, de forma que todos os processos necessários para a produção, incluindo processos externos, como fornecedores, sejam integrados digitalmente, permitindo assim que todo o fluxo seja monitorado em tempo real, podendo-se compreender como a produção está ocorrendo.

Ela permite que seja feito um monitoramento constante de todos os elementos que permitirão a entrega do produto ao cliente, dessa maneira é possível que planejamentos sejam feitos mais assertivamente, que seja aumentada a velocidade da produção, melhorada a qualidade do produto e, consequentemente, a satisfação dos clientes.

Figura 3 – Integração vertical



Fonte: i-scoop (2020)

A integração vertical (ilustrada pela Figura 3), por sua vez, se preocupa em fazer a integração dos sistemas entre diferentes níveis hierárquicos dentro da própria empresa. Dessa maneira, é criada uma integração do chão de fábrica até o nível executivo. Os sensores instalados no chão de fábrica produzem dados que serão passados e acompanhados para níveis acima, sendo transformados em informações que eventualmente poderão ser utilizadas por outros níveis da empresa, para tomadas de

decisão. Dados que, por vezes, são registrados manualmente e atualizados em uma determinada periodicidade passam a ser disponibilizados imediatamente para diferentes lugares, que não precisam necessariamente estar na mesma região da coleta, ou seja, isso permite que escritórios que estejam a grandes distâncias das áreas de produção possam receber rapidamente informações da produção.

2.2.7. Simulação

A simulação na indústria 4.0 une uma série de tecnologias diferentes que permitem a reprodução virtual de processos para compreender pontos de melhoria da manufatura, propor soluções, testar hipóteses, aplicar e metrificar mudanças.

Utilizando softwares e, dependendo do processo, hardwares específicos, a empresa pode reproduzir virtualmente o andamento de um processo, de forma que ele possa ser analisado e possam ser feitas mudanças e aperfeiçoamentos em um ambiente de testes antes de aplicá-los em produção.

Para isso, a qualidade dos dados aplicados na simulação ditará o grau de similaridade entre o virtual e o real, de forma que, quanto melhor os dados inseridos, mais próxima à realidade será a simulação e, consequentemente, os resultados mais parecidos serão com o que ocorreria na realidade. Sendo assim, para a utilização da simulação, é necessário que a empresa já tenha adotado uma estrutura de dados organizada, para que ela possa alimentar os testes.

O processo de simulação ocorre em 5 passos:

Definição de problemas: o primeiro passo é o entendimento de que a indústria precisa ou pode ser melhorada em algum ponto. Com a simulação, é possível compreender como os processos ocorrem durante seu funcionamento e analisar possíveis locais de gargalo, pontos que estejam apresentando problemas, processos que podem ser rearranjados e etc;

Validação: Com o problema encontrado, testa-se as diferentes soluções que podem ser aplicadas, de forma que se possa definir a melhor tomada de ação;

Melhoria: Nesse momento, além da solução pensada, pode-se verificar recursos internos e do mercado, de forma que seja possível validar o processo e, até mesmo, inserir melhorias na solução anteriormente apresentada;

Implementação: Os dados inseridos na simulação retornarão resultados que permitirão avaliar a viabilidade da solução apresentada e melhorada. Dessa maneira, a implantação pode ser feita com maior assertividade;

Metrificação: Uma vez implantada, a solução pode ser passada novamente pela simulação, para que assim possa-se analisar dados mais novos, permitindo que a solução seja constantemente aprimorada.

De forma geral, a simulação traz diversas vantagens para a indústria, permitindo que alterações, novas soluções e até mesmo treinamentos sejam feitos em ambientes virtuais, de forma que diferentes medidas sejam tomadas, sem que eventuais erros causem reais prejuízos ou perigos para a empresa.

2.2.8. Internet das coisas

Nascida em 1980, a internet das coisas (internet of things) pode ser definida como uma rede de objetos conectados à internet responsáveis por captar diferentes grandezas do ambiente em que se encontram. Na época, o estudante de ciências da computação David Nichols, da Universidade de Carnegie Mellon, criou o primeiro objeto ligado à uma rede de computadores local, para saber se a única máquina de refrigerantes do campus estava carregada de latas geladas sem que tivesse que sair de seu laboratório.

O termo “internet of things”, no entanto, foi cunhado apenas em 1999, por Kevin Ashton, que utilizando tecnologia RFID, teve a ideia de colocar sensores nos produtos da P&G para receber informações sobre as vendas, de forma que, fosse possível saber caso algum produto estivesse faltando nas prateleiras das lojas.

Hoje, a IoT pode ser aplicada em várias áreas do cotidiano e está relacionada ao conceito da computação ubíqua, ou seja, aparelhos super conectados, que captam diversas informações do ambiente, no entanto, quase não são perceptíveis aos humanos, tornando-se “transparentes” no local. Esses objetos possuem capacidade de capturar uma grande quantidade de dados que são transmitidos pela internet. Uma vez processados, tornam-se informações que podem ser utilizadas para retornar comandos para os objetos em campo, para que atuem automaticamente dependendo da resposta recebida. Isso torna possível, por exemplo, a existência de casas inteligentes que a partir de dados extraídos em tempo real podem ligar, desligar ou controlar uma série de

aparelhos para diferentes fins, podendo economizar energia, proporcionar comodidade aos seus proprietários ou, até mesmo, auxiliar na segurança do local.

No entanto, mais do que a aplicação residencial, essa conectividade é utilizada na indústria também. Conhecida como internet das coisas industrial (IIoT), o conceito de IIoT e a própria indústria 4.0 se mesclam, uma vez que ambas tratam da conexão de atuadores com a rede de forma que possam gerar grandes quantidades de dados que possam ser utilizados para gerar informações e deixar a linha de produção mais inteligente, de forma que, muitas vezes, o próprio maquinário possa fazer um ajuste da configuração sem a necessidade de uma intervenção humana.

2.2.9. Cibersegurança

Com uma quantidade maior de armazenamento e tráfego de dados, é normal que a preocupação com a segurança de tais dados deva ser levada em consideração. Segundo a empresa de segurança Fortinet, somente no primeiro trimestre de 2021, o Brasil sofreu mais de 3,2 bilhões de tentativas de ataques cibernéticos dos 7 bilhões ocorridos na América Latina no mesmo período, liderando o ranking, seguido pelo México, Peru e Colômbia que tiveram cerca de 1 bilhão de ataques cada.

A cibersegurança é um conjunto de práticas, procedimentos e tecnologias que visam proteger computadores, redes, programas e dados de ataques.

Tais ataques podem provocar diferentes níveis de danos, podendo-se citar como exemplos a perda parcial de dados, roubo de senhas, sequestro de computadores para exigir pagamento de resgate, espionagem e disseminação de SPAM.

Para evitar esse tipo de problema, os usuários podem se utilizar de algumas medidas de proteção, como a utilização de softwares atualizados e originais, a utilização de firewall, antispam e antivírus, fazer frequentemente backups de seus dados e utilizar senhas fortes e diferentes para cada serviço.

Na indústria 4.0, no entanto, a proteção de dados é fundamental, uma vez que a conectividade que faz prosperar o sistema, quando invadida, pode provocar danos irreversíveis. Em fevereiro de 2021, a cidade da Flórida, Oldsmar, registrou um caso em que um hacker invadiu os computadores da planta de distribuição de água da cidade para alterar o teor de soda cáustica aplicada na água. O ataque só não causou grandes

problemas porque um dos funcionários verificou que o cursor indicativo da máquina estava se alterando sozinho ao longo do dia, então cancelou a operação antes que quantidades insalubres de soda cáustica fossem aplicadas na água a ser distribuída.

Para fazer a proteção de um sistema empresarial ou industrial, a cibersegurança se depara com uma série de obstáculos. Cada dispositivo conectado representa um risco potencial de invasão. Considerando que com a IIoT, sistemas que antes eram isolados, hoje, fazem parte de uma rede, aumenta-se a “superfície” passível de ataques. Outro problema comumente encontrado na indústria moderna são as características únicas de cada sistema de controle industrial, o que também tornam suas vulnerabilidades únicas. Upgrades, que podem melhorar as barreiras de defesa, são feitos aos poucos, por conta da complexidade dos sistemas e suas integrações.

A implementação de boas práticas auxilia empresas a reduzir problemas com ataques mais comuns. Uma delas é o controle de acesso, com a devida identificação dos usuários e a restrição de permissões, de forma que apenas pessoas que realmente necessitem alterar registros possam fazê-lo, ao passo que outros usuários tenham condições para fazer apenas a leitura dos arquivos. Outra boa prática é o nível de integração entre sistemas da TI e os sistemas das máquinas, de forma que, além de identificáveis, os sistemas também devem ter apenas o nível ideal de troca de informações. Também pode-se citar a desativação de serviços e dispositivos que não tenham mais utilidade para o trabalho, uma vez que eles também podem ser utilizados como fonte de exploração para ataques.

2.3.A indústria 4.0 no Brasil

O cenário industrial no Brasil não é bom. Nos anos 80, sua participação no PIB brasileiro passava dos 20%, no entanto, em 2021, sua participação gira em torno de 11%, retrato de uma economia que já via a redução de sua indústria quando a pandemia abalou o mercado de forma geral.

Além do baixo desempenho na economia do país, a indústria brasileira vem caindo no índice global de inovação que avalia como está o desenvolvimento das nações em

áreas como crescimento da produtividade, investimentos em P&D, educação, dentre outras categorias.

No índice global de competitividade de manufatura o país também não vai bem, caindo do 5º lugar que ocupava em 2010 para o 29º em 2016 (dentre 40 países avaliados).

De forma geral o país apresenta baixa complexidade no setor, sendo um dos maiores produtores de commodities do mundo, e dentre os países do G20, tem baixos indicadores de preparo, comparáveis aos da Argentina e da África do Sul.

Embora as notícias pareçam ruins, segundo o relatório Readiness for the future of production report, elaborado pelo Fórum Econômico Mundial, o Brasil possui uma boa tendência para a indústria 4.0.

O país ainda é um grande atrativo para investimento estrangeiros e, por possuir boas relações com outros países, pode ter mais facilidade para fazer transferências de conhecimento e tecnologias.

Também pode-se citar que alguns setores específicos do país já possuem alto nível de inovação digital, como a indústria farmacêutica, automobilística e de bebidas e alimentos. O agronegócio ainda precisa de aprimoramento, no entanto, e é um setor que também apresenta com frequência a utilização de tecnologias de ponta.

O desenvolvimento da indústria do país não pode ocorrer repentinamente. A indústria 4.0 deve ser implantada gradualmente e apresenta uma série de obstáculos a serem transpostos, como:

Fornecedores: A indústria 4.0 extrapola os limites da própria empresa para que o produto final chegue com mais qualidade e mais eficientemente para o consumidor. Isso exige que toda a cadeia de produção seja atualizada, no entanto, alguns setores se desenvolvem mais rapidamente que outros.

Investimentos: O investimento em novas tecnologias é de alto custo e a economia brasileira, de forma geral, não está muito bem, principalmente com os efeitos da

pandemia. Embora a indústria 4.0 apresente uma série de vantagens, empresas que possuem mais recursos ainda fazem investimentos com muita cautela.

Cultura: A alteração na forma de produzir impacta diretamente na cultura das empresas e pode causar grande resistência por parte dos colaboradores.

Com tais dificuldades para impulsionar a indústria, o ministério da Economia criou em 2017 o grupo de Trabalho para a Indústria 4.0 (GTI 4.0) juntando mais de 50 instituições do governo, empresas, sociedade civil, startups e outros.

O intuito do grupo é fomentar a indústria, difundindo conhecimento e facilitando financiamentos, para que ela possa ficar mais competitiva. Essa ação converge com as premissas da Agência Brasileira de Desenvolvimento Industrial (ABDI) que indicam como o impulso do setor deve ser feito.

Segundo a ABDI deve-se incentivar iniciativas que auxiliem empresas a investirem em tecnologia, facilitar o acesso às novas tecnologias, testar e debater projetos pilotos e experimentos referentes a áreas que não utilizam tecnologia atualmente e equilibrar os incentivos dados entre pequenas e médias empresas em comparação com grandes empresas.

3.Internet das coisas

3.1.O que é IoT e IIoT?

Como mencionado anteriormente, a internet das coisas (internet of things) são redes de aparelhos dotados de sensores que podem fazer uma leitura de diferentes grandezas do ambiente, enviar os dados coletados pela internet e receber da rede uma resposta de como tal aparelho pode atuar, dependendo da leitura feita dos dados.

Ela pode ser empregada em diversos setores e hoje, pode-se encontrar aparelhos inteligentes e conectados para diversos públicos, a exemplo disso, tem-se os mais diversos aparelhos e eletrodomésticos que podem transformar uma casa comum em uma casa inteligente.

Na indústria não é diferente, a internet das coisas tem um papel fundamental na 4ª revolução industrial, de tal forma que é difícil separar a IoT da revolução, uma vez que ambas tratam da leitura de dados, processamento e resposta automática das máquinas, com intervenção mínima de seres humanos.

Assim como a automação industrial passou a substituir o trabalho manual repetitivo e perigoso, a internet das coisas pode auxiliar na substituição da necessidade de trabalhos intelectuais repetitivos, podendo tornar a indústria mais rápida e segura. Dessa maneira, pode-se mencionar a IIoT (Industrial Internet of Things), que seria uma categoria da IoT voltada para a indústria.

3.2.História

A ideia de dispositivos super conectados surgiu cerca de 40 anos atrás, na Universidade Carnegie Mellon em 1980, quando o estudante de ciências da computação, David Nichols, cansado de andar todo o campus da faculdade para descobrir que a máquina de refrigerante estava vazia, criou um dispositivo que adaptava os sinais de luz já existentes no equipamento para saber se havia latas de refrigerante disponíveis e até mesmo se estavam geladas. Os sinais eram enviados para a ARPANET, que na época, comportava cerca de 300 computadores na rede.

Onze anos depois, em 1991, Mark Weiser lançou o artigo “O computador para o século XXI”, onde cunhou o termo “computação ubíqua”. Nesse artigo descreveu que a tecnologia seria cada vez menos perceptível aos olhos humanos, de forma que, dispositivos tecnológicos seriam integrados a objetos comuns, do dia a dia, colhendo dados sobre o cotidiano e poderiam oferecer informações em tempo real, sem a necessidade de acessar terminais específicos para isso, como um computador ou uma televisão.

No entanto, somente em 1999, Kevin Ashton, funcionário da P&G, idealizou um sistema que conectaria produtos físicos ao mundo digital. Na época, a empresa se deparava com um problema, uma vez que, ao venderem seus produtos para lojas, perdiam a noção de como estavam as vendas diretamente para o consumidor final, ou seja, não sabiam o que ficava mais tempo nas prateleiras e o que era vendido mais

rápido. Para solucionar a questão, Ashton pensou em colocar sensores em seus produtos, para que assim a P&G pudesse saber como estavam as vendas.

Mais especificamente para a área da indústria, a IIoT nasceu a partir de uma série de criações que vieram muito antes e foram se desenvolvendo com o tempo. Pode-se dizer que tudo começou com a criação de Computadores Lógicos Programáveis (CLP) em 1986 por Dick Morley.

Já em 1973, Theodore Paraskevakos , patenteou a tecnologia máquina a máquina (Machine to Machine - M2M) que utiliza computação e telefonia para fazer conexão entre máquinas.

A padronização da ethernet em 1983 também foi de grande importância, uma vez que permitiu que transferências de dados pudessem ser feitas a uma taxa de 2.94 megabits por segundo.

Outro passo importante que ocorreu e que hoje é muito importante na utilização da indústria, foi a criação e popularização da World Wide Web (WWW) em 1990. Bem como a disseminação de tecnologias wireless em 1997.

Por fim, veio o cunho do termo “Internet of Things” pelo Kevin Ashton em 1999 e o lançamento dos serviços em nuvem pela Amazon em 2002.

A IIoT veio junto com a 4ª revolução industrial, utilizando-se de diversas tecnologias desenvolvidas ao longo dos anos.

3.3.Futuro da IoT

O futuro da IoT é promissor. Uma das dificuldades que podem ser encontradas na implantação de redes IoT é a falta de redes de dados móveis rápidas e estáveis em algumas regiões. Com a implantação do 5G, locais que antes não possuíam sinal, passarão a receber, permitindo assim que mais empresas e pessoas passem a utilizar internet das coisas.

Na medicina, sensores poderão monitorar continuamente usuários, enviando automaticamente mensagens para médicos e pacientes assim que parâmetros anormais

forem detectados, acelerando o atendimento em caso de emergência. Lentes de contato, sensores ingeríveis e smartwatches detectores de hormônios da depressão são alguns dos futuros equipamentos médicos que poderão estar disponíveis no mercado em um futuro próximo.

A agricultura é um dos setores que mais poderão se beneficiar, uma vez que sensores poderão prever mudanças climáticas, aferir a qualidade do ar, temperatura e humidade, quantidade de elementos químicos aplicados na lavoura e água, permitindo que plantio e colheita sejam feitos nos momentos mais ideias, aumentado a produtividade e reduzindo desperdícios.

No setor alimentício, geladeiras, congeladores e termostatos inteligentes auxiliarão lojas, restaurantes e indústria a manter os estoques em condições adequadas, evitando que alimentos sejam perdidos por passar da validade e alertando em casos de possíveis contaminações.

Com a implementação da IoT em diversos setores e das formas mais variadas, é natural que a cibersegurança também esteja atrelada ao futuro. Com mais dispositivos conectados e transmitindo grandes quantidades de dados, ataques a redes de objetos conectados já são uma realidade e a tendência é piorar. Portanto, o investimento em criptografia deve ser prioridade enquanto diferentes camadas de segurança possam ser estudadas e implantadas em diferentes sistemas.

Na indústria a IIoT já tem seu efeito no desenvolvimento de produtos, uma vez que auxilia empresas a melhorar custos operacionais, aumentar a eficiência da produção e otimizar processos existentes.

A tendência da indústria será a IIoT vendida como serviço. Empresas especializadas fornecerão API’s, serviços de análise avançadas, updates de sistema, controle de segurança e gerenciamento de dispositivos, permitindo que sistemas complexos sejam rapidamente instalados e passem a gerar dados imediatamente, exigindo conhecimento mínimo do cliente e assemelhando-se a uma solução “plug-and-play”.

A manutenção preditiva também está sendo alterada pela IIoT, em conjunto com a inteligência artificial, realidade aumentada e gêmeos digitais. Com a utilização de dados fornecidos por sensores IoT, empresas podem criar modelos digitais muito semelhantes

a equipamentos físicos, rodar testes e direcionar manutenções seguindo os dados gerados em campo, podendo compreender áreas mais suscetíveis a desgaste sem a necessidade de avaliar fisicamente um equipamento previamente.

3.4.Aplicações

Uma das mais populares utilizações da IoT são as casas inteligentes. Nesse segmento, proprietários podem utilizar uma série de sensores e atuadores para fazer o controle e gerenciamento de suas residências à distância. Podendo utilizar desde câmeras e sensores de presença para identificar possíveis invasões, até o controle de aparelhos domésticos e luzes, para fazer um consumo mais inteligente de energia e tornar o ambiente mais confortável.

Os wearables, são equipamentos “vestíveis” ou de fácil transporte, como smartwatches, smartphones e rastreadores de saúde que também fazem parte do ecossistema da IoT. São dispositivos que captam e transmitem preferências do usuário, de maneira que possam facilitar a busca por informações. Hoje são muito comuns no campo da saúde e para pessoas que procuram manter uma boa forma física, no entanto a indústria já vê nesse segmento uma forma de melhorar a cadeia de fornecimento e logística.

Na questão urbana, a IoT pode ajudar governos a transformar centros urbanos em cidades inteligentes. Sensores podem auxiliar no controle e vigilância do tráfego, fazer gerenciamento de energia, gerenciamento de resíduos e auxiliar na segurança pública.

Na agricultura, sensores podem ser utilizados para verificar a saúde do solo, umidade e concentração de nutrientes. Dessa maneira, a distribuição de água e fertilizantes pode ser personalizada para diferentes áreas de uma mesma lavoura. Já na pecuária, instrumentos podem ser utilizados para verificar a saúde do gado, auxiliando a identificar animais doentes ou em risco, permitindo uma intervenção humana preventivamente.

4.Segurança na indústria 4.0

As redes IoT são compostas por uma série de dispositivos conectados à internet. Dessa maneira, quando um ou mais deles é infectado por um malware, podem se tornar entrada para uma infecção dos outros dispositivos existentes na mesma rede, podendo afetar, assim, infraestruturas críticas.

Vulnerabilidades encontradas nos softwares de comunicação dos dispositivos podem variar desde o manejo e acesso dado aos computadores pessoais (PC) até os sistemas de vigilância de câmeras, de forma que, há registros de invasões através desses dispositivos que acabaram permitindo o acesso remoto de pessoas não autorizadas a áreas restritas.

Dispositivos que eram normalmente utilizados offline passaram a trabalhar conectados à internet, coletando grandes quantidades de dados, que, ao serem analisados juntamente a informações obtidas ao longo do tempo ou de outros dispositivos, tornam-se conhecimento.

Tal conhecimento é de grande importância para o crescimento da eficiência e diminuição de custos da indústria. No entanto, segundo o IoT Acceleration Consortium, programa colaborativo de representantes da academia, governo e indústria japonesa, pode-se considerar que em relação às ameaças que redes IoT podem oferecer, 3 questões foram subestimadas: (1) o número crescente de dispositivos sendo conectados à internet, (2) os ciclos de longa vida e (3) dificuldade de vigilância manual perfeita.

O número crescente de coisas conectadas, embora demonstre o potencial e a eficiência das redes, acaba apresentando uma gama muito grande de alvos a serem atacados, ou seja, quanto mais dispositivos uma rede apresenta, maior a necessidade de protegê-los, por serem portas de entrada em potencial.

Ciclos de longa vida se referem a sistemas que coletam dados por muito tempo, podendo ser até mais de 10 anos, antes de se fazer um estudo sobre eles. Por levar tanto tempo para serem analisados, correm o risco de serem atacados, e em alguns casos, os

ataques podem ocorrer por longos períodos, de forma que, o problema possa ser identificado muito tardiamente.

A terceira questão, além de um problema por si só, pode ser um agravante para a segunda, porque, uma vez que a indústria 4.0 e as redes IoT possam apresentar grande independência e exijam pouca interferência humana, isso implica em poucos profissionais cuidando de tais redes, e consequentemente, dificulta a identificação de eventuais anormalidades.

A redução da necessidade de profissionais na cadeia produtiva, consequentemente, eleva a necessidade de melhorar a qualidade da mão-de-obra empregada em tais empresas. Funcionários que não estejam bem preparados e que não tenham um bom conhecimento e entendimento das tecnologias empregadas podem levar a vulnerabilidades, como a má configuração de aparelhos e desconsideração na hora de seguir protocolos.

Em 2017, a empresa Inmarsat (provedor global de comunicações por satélite), fez uma pesquisa com 500 decisores em TI de grandes organizações em diversos países da América, Europa, Oriente Médio, África e Ásia. A pesquisa revelou que 94% dos entrevistados brasileiros precisavam de profissionais voltados para a implantação de soluções com internet das coisas de nível sênior. O problema se estende para a América Latina, uma vez que 86% dos entrevistados da região revelaram ter o mesmo problema. A média global para esse caso é de 76%.

A mesma pesquisa também identificou que 72% dos entrevistados indicaram que falta mão de obra experiente para gerenciar a implantação de soluções IoT e 80% indicaram que faltam habilidades na entrega prática de soluções IoT de forma que elas funcionem adequadamente da forma pretendida.

4.1.Shodan

Assim como a Google, Shodan é uma ferramenta online de pesquisa, no entanto, ao invés de pesquisar sites, seu propósito é encontrar dispositivos conectados à internet. Seu criador Jhon Matherly, originalmente criou a ferramenta (lançada em 2009) para que fosse utilizada por grandes empresas, como a Cisco, Juniper e Microsoft, de modo que pudessem mapear os produtos de seus concorrentes. No entanto, a mesma passou a ser utilizada principalmente por pesquisadores de segurança, acadêmicos, polícia e hackers, de modo geral, pessoas que estejam procurando dispositivos que possam estar desprotegidos na internet.

Através do Shodan (nomeado em homenagem ao vilão do jogo System Shock, que é um computador senciente), milhares de dispositivos podem ser encontrados. No ano de 2013, o site registrava cerca de 48.000 câmeras para vigiar bebês, todas elas nos Estados Unidos, todas da empresa Foscam, que apresentavam sérios problemas de segurança e poderiam ser facilmente invadidas. A ferramenta também apresentava que haviam mais 400.000 câmeras do mesmo tipo espalhadas pelo mundo.

Muito além das câmeras de babás eletrônicas, Shodan pode encontrar diversos tipos de dispositivos, dentre eles: carros, monitores cardíacos de fetos, sistemas de controle de aquecimento de prédios comerciais, empresas de tratamento de água, controles de usinas de energia, semáforos e sensores de glicose.

4.2.MOZI

Criado em 2019, Mozi é um botnet que se aproveita das configurações padrão ou incorretas de alguns equipamentos IoT para executar comandos CMDi, permitindo assim acesso aos equipamentos infectados, ataques DDoS, roubo de dados e envio de spams. Segundo informações da IBM, entre outubro de 2019 e Junho de 2020, 90% do tráfego de redes IoT foram causados pelo Mozi.

Por utilizar estrutura P2P (ponto a ponto), o botnet tem uma vantagem natural para se espalhar porque, mesmo que um dos nodes infectados da rede em que se encontra seja derrubado, os outros compensam sua ausência e continuam a infectar dispositivos vulneráveis. Estima-se que a infecção passou de 323 nodes registrados em dezembro

de 2019 para 1.5 milhões em Abril de 2020, sendo a maioria encontrados na China e na Índia.

A grande quantidade de ataques desse período pode ser atrelada também à expansão da rede de “coisas”, uma vez que, na época, existiam cerca de 31 bilhões de dispositivos ativos no mercado, e uma taxa de 127 novos dispositivos sendo implantados na rede por segundo.

Os hackers responsáveis pelo Mozi foram presos por autoridades chinesas em 2021 e ele não recebe novas atualizações há algum tempo, no entanto, sua rede ainda está ativa e dispositivos continuam a ser infectados todos os dias, dessa forma a principal orientação é que as configurações padrão dos dispositivos sejam alteradas e testes de penetração sejam feitos para identificar possíveis lacunas na defesa do sistema.

4.3. Cases

4.3.1. Caso Foscam e as câmeras para vigiar bebês

Em Agosto de 2013, Marc Gilbert do Texas, teve o aparelho de vigilância do seu bebê (Figura 4) invadido por um hacker. No caso, Gilbert estava em casa quando percebeu que uma barulho estranho estava vindo do quarto de sua filha, de 2 anos. A menina, estava dormindo tranquilamente em seu berço, no entanto o invasor da babá eletrônica estava tentando acordá-la com termos extremamente pesados, sem saber que o bebê é surdo e que o aparelho auditivo da menina, por sorte, estava desligado naquele momento.

O pai imediatamente desligou a babá eletrônica, composta por microfone, saídas de som e câmera.

Figura 4 – Babá eletrônica Foscam

Fonte: Foscam (2021)

Naquele momento, Gilbert ficou muito confuso com o ocorrido, pois havia tomado as medidas básicas de segurança, alterando as senhas padrão do roteador e da babá eletrônica e deixando ativado o firewall da rede, no entanto, não foi suficiente para impedir a invasão.

O problema, na verdade, estava no aparelho. Alguns poucos meses antes do ocorrido, os pesquisadores de segurança Sergey Shekyan e Artem Harutyunyan da Qualys já haviam apontado problemas nas câmeras da Foscam, em uma apresentação chamada "To watch or to be watched: Turning your surveillance camera against you." (Assistir ou ser assistido: voltando suas câmeras de segurança contra você, em tradução livre).

Na apresentação, Shekyan e Harutyunyan indicaram que a cada 10 aparelhos do modelo ‘Netwave IP Camera’ retornados pelo site Shodan, 2 poderiam ser invadidos, pois os mesmos fariam a autenticação do usuário, mesmo sem a senha, caso fosse utilizado o login “admin”.

Com a invasão, o hacker poderia coletar dados como vídeos, e-mails, ftp, MSN e credenciais do wi-fi.

Na época, a apresentação dos dois pesquisadores não chamou muita atenção porque eles se referiram aos aparelhos como “IP Cams”, o que acabou não alarmando muito as pessoas.

Em Junho do ano anterior (2012) a empresa Foster já havia liberado uma atualização do firmware que poderia resolver esse problema, uma vez que os usuários seriam incentivados a alterar a senha e o login do aparelho passaria a poder ser alterado, extinguindo assim, o login “admin”. No entanto, a pesquisa feita em abril, por Shekyan e Harutyunyan, indicou que 99% dos aparelhos ainda estavam com o firmware antigo.

4.3.2. Caso ThroughTek

Em 2021 foi identificado que milhões de aparelhos IoT, incluindo câmeras de segurança, monitores de bebês e outros equipamentos de gravação de vídeo, apresentam uma vulnerabilidade que possibilita que criminosos invadam o equipamento e possam assistir e ouvir os vídeos ao vivo, bem como utilizar os aparelhos para preparar ataques maiores.

Tal vulnerabilidade foi encontrada em dispositivos que utilizam a rede ThroughTek Kalay e divulgada pela empresa de cibersegurança Mandiant em conjunto com Agência de Segurança Cibernética e Infraestrutura (CISA).

A vulnerabilidade recebeu uma nota de 9.6, considerada crítica, e pode ser mitigada com a atualização do protocolo Kalay (3.1.1.0). A Mandiant não compilou uma lista com todos os objetos vulneráveis, mas a própria ThroughTek indica que 83 milhões de aparelhos estariam ligados à rede em questão.

Pesquisadores conseguiram combinar bibliotecas da ThroughTek através de aplicativos oficiais disponíveis no Google Play e na Apple Store com uma implantação funcional do protocolo Kalay. Isso permitiu a descoberta de dispositivos, registro de novos dispositivos, conexões remotas de clientes, autenticação e processamento de áudio e vídeos.

Com isso, cibercriminosos conseguiram sobrescrever registros, redirecionando a conexão dos equipamentos para os aparelhos dos criminosos, conseguindo login e senha dos usuários verdadeiros.

Além de comprometer a privacidade de milhares de casas, criminosos poderiam coletar dados sensíveis de empresas e, até mesmo, utilizar os equipamentos invadidos como bots para ataques DDoS.

Até então não foram identificados ataques e explorar essa vulnerabilidade é um esquema complexo, que demandaria tempo e esforço de possíveis agentes maliciosos, mas não está descartado o perigo, que continua sendo considerado crítico pela CISA.

4.3.3. Dispositivos IoT em hospitais

A empresa de tecnologia em saúde Philips em conjunto com a empresa de cibersegurança CyberMDX liberaram em 2021 um relatório abordando os gastos em cibersegurança e as tendências em hospitais de médio e grande porte.

Pesquisadores entrevistaram 130 pessoas responsáveis por tomadas de decisão relacionadas à TI de hospitais para descobrir como esses profissionais estavam lidando com os milhares de dispositivos que são utilizados em hospitais atualmente.

Identificaram que aproximadamente 31% dos entrevistados precisam gerenciar menos de 10.000 aparelhos, ao passo que 29% são responsáveis por menos de 25.000 aparelhos e 20% lidam com menos de 50.000. Embora uma grande parte dos entrevistados tivesse uma boa noção de quantos aparelhos possuem sob seu gerenciamento, 15% dos profissionais de hospitais de médio porte e 13% de grande porte não sabiam a quantidade de dispositivos conectados à sua rede.

Quase metade dos entrevistados relataram que a segurança e a quantidade de profissionais que lidam com tais aparelhos são “inadequados”. 40% dos grandes hospitais contratam soluções de segurança voltadas para IoT, mas 16% deles utilizam apenas a segurança oferecida pelo fornecedor do equipamento. Os números não diferem muito para os de médio porte. Os entrevistados revelaram também que a média anual gasta em dispositivos IoT gira em torno de US$300.000.

A cibersegurança de hospitais possui alta crucialidade. Até meados de 2021, um relatório do departamento de saúde e serviços humanos americano (HHS) indicou que houveram 82 incidentes envolvendo ransomware no mundo todo, sendo 60% deles voltados especificamente para os Estados Unidos.

Metade dos executivos entrevistados também revelaram que já tiveram que forçar a parada de dispositivos por ataques nos últimos seis meses. Os hospitais maiores indicaram que tiveram uma média de parada de 6.2 horas de seus dispositivos, tendo um custo de US$21.500 por hora. Os hospitais de médio porte passaram por problemas maiores, tendo uma média de parada de 10 horas, custando US$45.700 por hora.

5.Conclusão

A 4ª revolução industrial já é uma realidade e está alterando a forma como as empresas conduzem seus negócios. Hoje, sabe-se que a informação é um bem precioso e quando utilizada corretamente pode gerar diversas vantagens na competição do mercado, reduzir custos, aumentar a qualidade do produto, melhorar relacionamento com cliente entre outras tantas vantagens.

Para que isso possa ocorrer, a existência da indústria 4.0 está intimamente ligada à utilização da internet das coisas, pois é ela quem faz a ponte entre o mundo real e o mundo digital, ou seja, é a IoT que faz o trabalho de coletar os dados do mundo físico através de sensores e enviá-los pela internet para um lugar que poderão ser armazenados e, no devido tempo, serem processados e transformados em informação.

Como tantas outras coisas, quando algo torna-se valioso, ele tende a ser cobiçado e a informação não é uma exceção. A implantação de dispositivos IoT podem ser extremamente simples, necessitando apenas ligá-los na tomada e fazer uma conexão rápida do equipamento com um aparelho supervisório, que hoje em dia, pode ser um celular. Com essa facilidade de utilização e as vantagens e comodidades trazidas por essa rede, é compreensível que a expansão de objetos conectados à internet esteja ocorrendo tão rapidamente. No entanto, nem sempre são considerados os perigos trazidos por esses itens quando não são bem protegidos.

No âmbito doméstico, há pouca consciência das pessoas da necessidade de proteger seus aparelhos conectados à internet. Se para antigas questões ainda encontram-se problemas porque os usuários não tomam medidas simples como alterar periodicamente suas senhas, manter senhas diferentes para sistemas diferentes e não informar a senha para outras partes, a preocupação e o entendimento da necessidade de tomar precauções com aparelhos que antes não requeriam esse tipo de conduta (televisores, relógios, computadores, celulares, babás eletrônicas e etc) ainda é muito baixa e ataques aos aparelhos smart estão ficando cada vez mais sofisticados.

Na indústria a preocupação com esse tipo de ataque é grande, uma vez que, dependendo do tipo de invasão, pode-se sofrer desde problemas financeiros com o sequestro de dados e parada da produção, até problemas mais sérios que podem

envolver a segurança dos trabalhadores, bem como dos consumidores quando o ataque acaba por alterar a qualidade de um produto ou o funcionamento de um equipamento. No entanto, a internet das coisas embora já amplamente aplicada, seja em maior ou em menor escala, é uma solução nova para as empresas e altamente adaptável, de forma que as vulnerabilidades causadas em um sistema podem ser diferentes das vulnerabilidades causadas em outro sistema que também utilize objetos conectados. Outro agravante dessa situação é a falta de profissionais experientes no mercado.

Sendo assim, a cibersegurança, é um dos pilares da indústria 4.0, no entanto, ainda um objeto de estudo, pois com as mais variadas aplicações existentes, é necessário que diversos testes de segurança sejam feitos e voltados para cada caso, bem como o treinamento das pessoas e a restrição de funcionários envolvidos com esses equipamentos e a criação de diferentes camadas de proteção que possam impedir a invasão desses sistemas.

6.Referências Bibliográficas

3DLAB Industria. Manufatura aditiva: saiba o que é e o que ela representa. *In:* 3D Lab Industria. **3DLAB Soluções em impressão 3D.** *[S.l.].* [2019]. Disponível em: https://3dlab.com.br/o-que-e-manufatura-aditiva/. Acesso em: 19 mai. 2021.

BUSINESS Tech Multimídia. Internet das coisas e a falta de mão-de-obra especializada. *In:* Business Tech Multimídia. **Business Tech Multimídia.** *[S.l.].* 11 set. 2017. Disponível em: https://www.businesstech.net.br/site/2017/09/internet-das-coisas-e-a-falta-de-mao-de-obra-especializada/. Acesso em: 14 mai. 2021.

CICLO Consultoria. Big Data Analytics e Indústria 4.0: o uso de dados para transformar a realidade industrial. *In:* Ciclo Consultoria. **Ciclo consultoria.** *[S.l.].* 14 mai. 2020. Disponível em: https://www.cicloconsultoria.org.br/post/big-data-analytics-e-ind%C3%BAstria-4-0-o-uso-de-dados-para-transformar-a-realidade-industrial. Acesso em: 12 jun. 2021.

CIZO Advisor. Botnet Mozi é responsável pela maioria dos ataques a redes IoT. *In:* CISO Advisor. **CISO Advisor.** *[S.l.].* 21 set. 2020. Disponível em: https://www.cisoadvisor.com.br/botnet-mozi-e-responsavel-pela-maioria-dos-ataques-a-redes-iot/. Acesso em: 30 out. 2021.

COZER, Carolina. Tendências e o futuro da Internet das Coisas. *In:* Grupo Padrão. **Whow! Empreendedorismo para a vida real.** *[S.l.].* 15 out. 2019. Disponível em: https://www.whow.com.br/tecnologia/tendencias-e-o-futuro-da-internet-das-coisas/. Acesso em: 6 abr. 2021.

DEUTSCHLAND.DE. A indústria integrada. In: deutschland.de. **deutschland.de**. [S.l.]. 8 abr. 2015. Disponível em: https://www.deutschland.de/pt-br/taxonomy/term/40/a-industria-integrada. Acesso em: 11 mai. 2021.

ENDRESS + Hauser. History of IIoT. *In:* Endress + Hauser. **Endress + Hauser.** *[S.l.].* [201-?]. Disponível em: https://www.processpioneers.com/iiot-potential/history-of-iiot/#top. Acesso em: 7 nov. 2021.

FIA - Fundação Instituto de Administração. Indústria 4.0: o que é, consequências, impactos positivos e negativos [Guia Completo]. *In:* FIA Business School. **FIA - Fundação Instituto de Administração.** *[S.l.].* 23 ago. 2021. Disponível em: https://fia.com.br/blog/industria-4-0/. Acesso em: 2 dez. 2021.

FONTES, Aléxia. Robôs autônomos: qual sua importância dentro da Indústria 4.0?. *In:* Grupo Voitto. **Voitto.** *[S.l.].* 4 ago. 2020. Disponível em: https://www.voitto.com.br/blog/artigo/robos-autonomos. Acesso em: 12 jun. 2021.
FOSCAM DIGITAL TECHNOLOGIES. **Foscam Digital Technologies.** *[S.l.].* Foscam Digital Technologies, [201-?]. Disponível em: http://foscam.us/products/foscam-fi8910w-white-wireless-ip-camera.html. Acesso em: 14 mai. 2021.

GREIG, Jonathan. Philips study finds hospitals struggling to manage thousands of IoT devices. *In:* ZDNET, A RED VENTURES COMPANY. **ZDNet.** *[S.l.].* 13 ago. 2021. Disponível em: https://www.zdnet.com/article/philips-study-finds-hospitals-struggling-to-manage-thousands-of-devices/. Acesso em: 15 nov. 2021.

HILL, Kashmir. How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old. *In:* Forbes. **Forbes.** *[S.l.].* 13 ago. 2013. Disponível em: https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/?sh=283463bfaad6. Acesso em: 14 mai. 2021.

HILL, Kashmir. How The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors And Power Plants. *In:* Forbes. **Forbes.** *[S.l.].* 04 set. 2013. Disponível em: https://www.forbes.com/sites/kashmirhill/2013/09/04/shodan-terrifying-search-engine/?sh=a3b63e525de4. Acesso em: 14 mai. 2021.

INDUSTRIA 4.0. As aplicações de Realidade Aumentada na Indústria 4.0. *In:* Industria4.0. **Ind4.0.** *[S.l.].* 23 mai. 2019. Disponível em: https://www.industria40.ind.br/noticias/18218-as-aplicacoes-de-realidade-aumentada-na-industria-40. Acesso em: 22 mai. 2021.

I-SCOOP. Industry 4.0 and the fourth industrial revolution explained. *In:* I-SCOOP. **I-SCOOP.** *[S.l.].*2020. Disponível em: https://www.i-scoop.eu/industry-4-0/. Acesso em: 10 out. 2021.

LAKSHMANAN, Ravie. Chinese Authorities Arrest Hackers Behind Mozi IoT Botnet Attacks. *In:* The Hacker News. **The Hacker News .** *[S.l.].* 2 set. 2021. Disponível em: https://amp-thehackernews-com.cdn.ampproject.org/v/s/amp.thehackernews.com/thn/2021/09/chinese-authorities-arrest-hackers.html?amp_js_v=a6&_gsa=1&usqp=mq331AQIKAGwASCAAgM=#amp_tf=De%20%251%24s&aoh=16306045743049&csi=0&referrer=https%3A%2F%2Fwww.google.com&share=https%3A%2F%2Fthehackernews.com%2F2021%2F09%2Fchinese-authorities-arrest-hackers.html. Acesso em: 30 nov. 2021.

MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: Fgv Editora, 2018. *E-book* (192p.) ISBN: 978-85-225-2006-0. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=qYtlDwAAQBAJ&oi=fnd&pg=PA1&dq=internet+das+coisas+e+a+industria+4.0&ots=rgQmEzh985&sig=rUjheeF7Tfdx6MRC6EAzTmrKqZE#v=onepage&q&f=false. Acesso em: 11 mai. 2021.

NARCISO FILHO, PAULO. Qual é o papel do Big Data na Indústria 4.0?. *In:* Harbor Informatica Industrial. **HarboR Informática Industrial.** *[S.l.].* 2 ago. 2018. Disponível em: https://www.harbor.com.br/harbor-blog/2018/08/02/qual-e-o-papel-do-big-data-na-industria-4-0/. Acesso em: 12 jun. 2021.

OTÁVIO, Luis. IoT: 9 Exemplos de aplicativos bem-sucedidos. *In:* Usemobile Soluções em Tecnologia. **Usemobile.** *[S.l.].* 7 jan. 2019. Disponível em: https://usemobile.com.br/iot-9-exemplos-de-aplicativos/. Acesso em: 15 nov. 2021.

PALMER, Danny. Critical IoT security camera vulnerability allows attackers to remotely watch live video - and gain access to networks. *In:* ZDNET, A RED VENTURES COMPANY. **ZDNet.** *[S.l.].* 17 ago. 2021. Disponível em: https://www.zdnet.com/article/critical-iot-security-camera-vulnerability-allows-attackers-to-remotely-watch-live-video-and-gain-access-to-networks/. Acesso em: 15 nov. 2021.

PEDERNEIRAS, Gabriela. Cloud, ou computação em nuvem, na indústria 4.0. *In:* Canal Indústria 4.0. **Ind4.0.** *[S.l.].* 7 abr. 2019. Disponível em: https://www.industria40.ind.br/artigo/17984-cloud-ou-computacao-em-nuvem-na-industria-40. Acesso em: 20 set. 2021.

RODRIGUES, Guilherme Valença Silva. O que falta para o desenvolvimento da indústria 4.0 no Brasil?. *In:* CERTI Insights. **CERTI Insights.** *[S.l.].* 13 abr. 2021. Disponível em: https://certi.org.br/blog/industria-4-0-no-brasil/. Acesso em: 1 nov. 2021.

SACOMANO, José Benedito. **Indústria 4.0**: conceitos e fundamentos. São Paulo: Edgard Blücher Ltda., 2018. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=PNCuDwAAQBAJ&oi=fnd&pg=PA17&dq=in%C3%ADcio+da+ind%C3%BAstria+4.0+&ots=o0PXzyMK_d&sig=ToF01zPcrCj7WzuEk5kJ3BcAAV8#v=onepage&q&f=false. Acesso em: 10 maio 2021.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016. Tradução de: Daniel Moreira Miranda. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=XZSWDwAAQBAJ&oi=fnd&pg=PT161&dq=livro+a+quarta+revolu%C3%A7%C3%A3o+industrial+&ots=Y98aYyMBj7&sig=xEjj7Rwrkt2b0JJ-3hWCdtWeTkw#v=onepage&q&f=false. Acesso em: 15 maio 2021.

SCOLA, Alvaro. A botnet Mirai está de volta e ameaça a internet. Saiba como se proteger!. *In:* Olhar Digital. **Olhar Digital.** *[S.l.].* 20 mar. 2019. Disponível em: https://olhardigital.com.br/2019/03/20/dicas-e-tutoriais/a-botnet-mirai-esta-de-volta-e-ameaca-a-internet-saiba-como-se-proteger/. Acesso em: 11 mai. 2021.

SEBRAE - Serviço Brasileiro De Apoio Às Micro E Pequenas Empresas. **SEBRAE.** Rio de Janeiro: SEBRAE, 2018. Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/RJ/Anexos/Industria%204_0%20-%20WEB.PDF. Acesso em: 18 mai. 2021.

SENAI - Serviço Nacional De Aprendizado Industrial. Você sabe o que é a computação na nuvem e por que ela é tão importante para a Indústria 4.0? : Este artigo foi preparado para falar justamente sobre isso. *In:* SENAI. **SENAI.** *[S.l.].* 29 mar. 2019. Disponível em: https://www.sesirs.org.br/industria-inteligente/o-papel-da-computacao-na-nuvem-na-industria-40. Acesso em: 20 set. 2021.

SHEKYAN, Sergey; HARUTYUNYAN, Artem. To Watch Or To Be Watched: turning your surveillance camera against you. Turning your surveillance camera against you. **Conference**. 2013. Disponível em: http://conference.hitb.org/hitbsecconf2013ams/materials/D2T1%20-%20Sergey%20Shekyan%20and%20Artem%20Harutyunyan%20-%20Turning%20Your%20Surveillance%20Camera%20Against%20You.pdf. Acesso em: 14 maio 2021.

SOUSA, Rafaela. Primeira Revolução Industrial. *In:* Rede Omnia. **Brasil Escola.** *[S.l.].* [20--?]. Disponível em: https://brasilescola.uol.com.br/geografia/primeira-revolucao-industrial.htm. Acesso em: 25 abr. 2021.

SOUSA, Rafaela. Segunda Revolução Industrial. *In:* Rede Omnia. **Brasil Escola.** *[S.l.].* [20--?]. Disponível em: https://brasilescola.uol.com.br/historiag/segunda-revolucao-industrial.htm. Acesso em: 25 abr. 2021.

SOUSA, Rafaela. Terceira Revolução Industrial. *In:* Rede Omnia. **Brasil Escola.** *[S.l.].* [20--?]. Disponível em: https://brasilescola.uol.com.br/geografia/terceira-revolucao-industrial.htm. Acesso em: 25 abr. 2021.

TANAKA, Shinsuke; FUJISHIMA, Kenzaburo; MIMURA, Nodoka; OHASHI, Tetsuya; TANAKA, Mayuko. IoT System Security Issues and Solution Approaches. **Hitachi**. 2016. Disponível em: https://www.hitachi.com/rev/pdf/2016/r2016_08_111.pdf. Acesso em: 11 maio 2021.

TIEMPO Development. The Future of IIoT. *In:* Tiempo Development. **Tiempo Development a 3 Pillar Global Company.** *[S.l.].* 11 mai. 2020. Disponível em: https://www.tiempodev.com/blog/the-future-of-iiot/. Acesso em: 7 nov. 2021.