FACULDADE SENAI DE TECNOLOGIA MECATRÔNICA

MITIGAR RISCOS DE ATAQUES CIBERNÉTICOS NA INDÚSTRIA 4.0

MITIGATING THE RISKS OF CYBER ATTACKS IN INDUSTRY 4.0

Renato Mattes Canoso[1], [i]
José Roberto dos Santos[2], [ii]
Thiago Tadeu Amici [3], [iii]
Paulo Sebastião Ladivez [4], [iv]
Vicente Gomes de Oliveira Junior[5] [v]

RESUMO

A Indústria 4.0 é o símbolo da quarta revolução industrial, que é influenciada por diversas tendências, como globalização, urbanização e mudanças demográficas e é caracterizado pelo aumento de informatização e automatização. No passado, as fábricas eram fechadas e a sua segurança era garantida por meio do isolamento e controle de acesso físico. Em contraste, hoje, as máquinas modernas são equipadas com uma série de dispositivos inteligentes, como sensores e atuadores, e são conectadas a outras máquinas e sistemas de processamento de dados por meio de redes sem fio ou *Ethernet* com fio. É imprescindível que a evolução tecnológica seja acompanhada pela evolução da segurança cibernética, sendo o principal objetivo deste artigo realizar uma revisão bibliográfica para elucidar quais são os ataques cibernéticos mais comuns na Indústria 4.0, bem como quais são as ações necessárias para evitá-los. Os ataques mais comuns encontrados foram os de *phishing, water holing, ransomware, scanning, spear-phishing, botnet e supply chain* e a melhor forma de mitigar os riscos desses ataques é desenvolver protocolos de prevenção ao identificar e lidar com vulnerabilidades do sistema e dos humanos envolvidos nos processos.

ABSTRACT

Industry 4.0 is the symbol of the fourth industrial revolution, which is influenced by various trends, such as globalization, urbanization and demographic change and is characterized by the increase of computerization and automation. In the past, factories were closed and their security was guaranteed through insulation and physical access control. In contrast, modern machines today are equipped with several intelligent devices, such as sensors and actuators,

[1]Pós-graduando em Indústria 4.0 na Faculdade SENAI de Tecnologia Mecatrônica. E-mail: renatocanoso@outlook.com

[2]Docente na pós-graduação de Indústria 4.0 e na graduação em Tecnologia em Mecatrônica na Faculdade SENAI de Tecnologia Mecatrônica. E-mail: joseroberto@sp.senai.br

[3]Mestre em Controle e Automação de Processos. Professor da Faculdade SENAI de Tecnologia Mecatrônica. E-mail: thiago.amici@sp.senai.br.

[4]Professor da Faculdade SENAI de Tecnologia Mecatrônica. E-mail: paulo.ladivez@sp.senai.br..

[5] Mestre em Engenharia Mecânica. Professor da Faculdade SENAI de Tecnologia Mecatrônica. E-mail: vgomes@sp.senai.br.

and are connected to other machines and data processing systems via wireless networks or wired Ethernet. It is essential that technological developments be accompanied by the evolution of cybersecurity and the main objective of this article being to conduct a bibliographic review to elucidate what are the most common cyber-attacks in Industry 4.0, as well as what are the necessary actions to avoid them. The most common attacks found were phishing, water holing, ransomware, scanning, spear-phishing, botnet and supply chain and the best way to mitigate the risks of these attacks is to develop prevention protocols by identifying and work vulnerabilities of the system and humans involved in the processes.

1 INTRODUÇÃO

A Indústria 4.0 é o símbolo da quarta revolução industrial, que é influenciada por diversas tendências, como globalização, urbanização e mudanças demográficas. Esse estágio do processo de industrialização é, assim como os três estágios anteriores, dominado por inovações tecnológicas. Enquanto a mecanização e eletrificação dos processos industriais guiaram as primeiras revoluções industriais, o terceiro estágio que é caracterizado pelo aumento de informatização e automatização, representa a principal característica da próxima revolução industrial (ALBERTIN et al., 2017). Marcada pela integração de sistemas cibernéticos e físicos na manufatura e logística de processos, bem como o uso da Internet das Coisas em processos industriais, Bartodziej (2017) afirma que a Indústria 4.0 e as suas tecnologias terão diversos impactos na criação, organização e modelos de negócios das empresas. Dentre esses impactos, encontra-se o conceito de Fábrica Inteligente, que desempenha um importante papel na forma com que se enxerga a nova Era Industrial, tendo a literatura atual mencionado que um ambiente descentralizado, auto-organizado e com produção flexível vai substituir o clássico modelo de hierarquia de produção centralizada e controlada que conhecemos.

Nesse processo de modernização, de acordo com Raposo (2018), a cibersegurança não era vista como uma preocupação há 20 anos, quando a Internet dava seus primeiros passos na indústria, no entanto, com todas as novas tecnologias que influenciam cada vez mais os processos industriais, esse segmento de inteligência é considerado elemento chave para garantir a continuidade do atual e futuro desenvolvimento da Indústria 4.0. Para Gilchrist (2016), ao passo que a inserção da tecnologia é aliada da indústria, trazendo inúmeros benefícios e avanços, também é ferramenta de ciber-criminosos, que encontram novas formas de utilizar a Internet das Coisas (IoT) para fins maliciosos. Com um ambiente onde cada vez mais dispositivos estão conectados, abrem-se novas brechas para ataques e há aumento no número de possíveis alvos frágeis para serem invadidos.

Em estudo realizado com mais de 500 empresas ao redor do mundo sobre os impactos financeiros provenientes de invasões do tipo *data breach* pela *International Business Machines Corporation* (IBM, 2019), é possível observar que a perda média anual por este tipo de ação é de US$ 3,92 milhões de dólares, cujo valor equivale a cerca de R$ 21 milhões de reais em conversão da moeda realizada pelos autores em Setembro/2020, quando US$ 1 equivalia a R$ 5,32. Ainda de acordo com o relatório, mais de 50% das invasões foram mal-intencionadas, custando um valor adicional de $ 1 milhão de dólares (R$ 5,39 milhões de reais) por invasão. Embora esse seja o tipo mais comum de ataque, os que ocorrem por falha humana e de equipamento técnico também aparecem na lista dos mais comuns, o que para a IBM é um indicativo de que se deve melhorar aspectos como

treinamento da equipe, investimento em tecnologia e testes do sistema para identificar possíveis falhas acidentais, que permitiram vazamento de dados.

É imprescindível que a evolução tecnológica seja acompanhada pela evolução da segurança cibernética, sendo o principal objetivo desse artigo realizar uma revisão bibliográfica para elucidar quais são os ataques cibernéticos mais comuns na Indústria 4.0, bem como quais são as ações necessárias para evitá-los descritos na literatura até então.

2 REFERENCIAL TEÓRICO

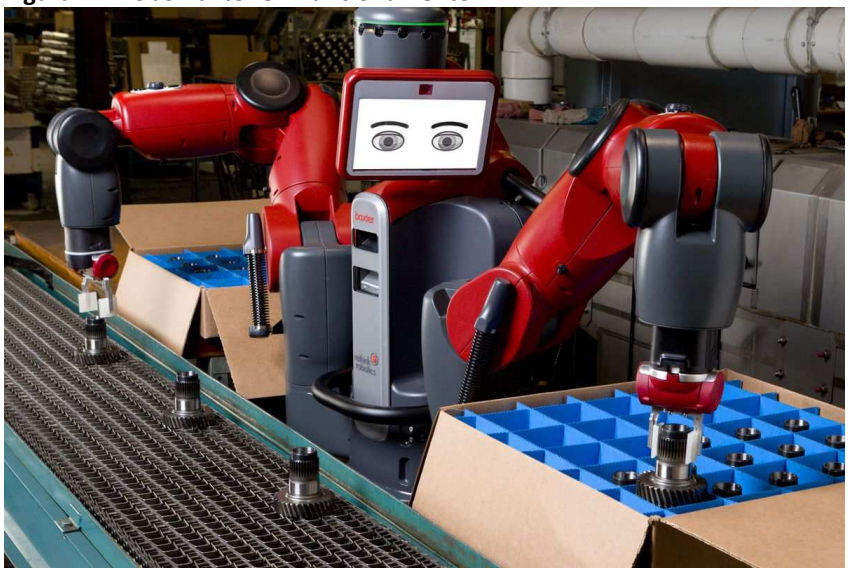
O aumento do uso das máquinas foi anunciado nos anos 1970 como o futuro das indústrias manufatureiras e a solução para erros humanos nas linhas de produção, causando grande preocupação. A dúvida era se as máquinas iriam dominar a produção, ideia que, inicialmente, pareceu se tornar uma realidade de sucesso, resultando na automação industrial. Gilchrist (2016) salienta que esse processo de automação começou a brilhar nos anos 1980, onde o desejo por eficiência na indústria fez com que muitos empregados que atuavam em processos manuais perdessem suas funções para as máquinas, considerado como o fim de humanos trabalhando em linhas de produção. É fato que, no início, o aumento do uso de máquinas e robôs substituiu muitos trabalhadores, no entanto, a quarta revolução industrial é uma transição para a transformação digital das indústrias manufatureiras, cujo objetivo é unir os mundos digital e físico, o que não significa necessariamente diminuir o trabalho humano.

O foco da Indústria 4.0 é o estabelecimento de produtos e processos de produção inteligentes, dessa forma combinando tecnologias que quebram paradigmas entre a economia, negócios, sociedade e pessoas. Segundo Erboz (2017), a Indústria 4.0 é sustentada por nove pilares, sendo eles:

***Big Data* –** termo difundido por John Mashey em 1990 cuja definição se baseia em três dimensões: volume de dados, variedade de dados e velocidade de geração de novos dados e análise. A análise dos dados previamente salvos é usada para descobrir ameaças que ocorreram em diferentes processos de produção, prever novos problemas que podem ocorrer e as possíveis soluções para impedir que continuem se repetindo (ERBOZ, 2017);

Robôs autônomos – com o tempo os robôs têm se tornado cada vez mais autônomos, flexíveis e cooperativos. Em breve interagirão entre si e trabalharão ao lado dos humanos, aprendendo com eles de maneira segura. Os robôs podem ser usados para desempenhar funções onde há interesse em maior precisão, além de poderem ser submetidos a condições de trabalho insalubres para humanos. Bahrin et al. (2016) citam os robôs autônomos utilizados atualmente em diferentes processos industriais. São eles, Kuka LBR iiwa, da empresa Kuka, descrito como um robô leve para tarefas industriais sensíveis; BioRob Arm, da empresa Bionic Robotics, desenvolvido para uso seguro em proximidade com humanos; Baxter, da empresa Rethink Robotics, que atua com empacotamento de produtos, conforme ilustra a Figura 1.

Figura 1 – Robô Baxter em funcionamento



Fonte: Rethink Robotics (2020).

Nuvem – A nuvem nada mais é do que um sistema de armazenamento de dados digital, que elimina a necessidade de armazenamento local/físico de dados. A computação em nuvem sustenta o sistema de conexão e comunicação da Indústria 4.0 e a massiva quantidade de dados compartilhados diariamente (PEREIRA e SIMONETTO, 2018).

Integração de sistemas horizontais e verticais – Hoje os sistemas ainda não são inteiramente integrados, ou seja, as indústrias não se conectam aos seus fornecedores e clientes. Ainda de acordo com Pereira e Simonetto (2018), na Indústria 4.0 é esperado que a organização toda esteja interconectada e também conectada com outras empresas. Os sistemas verticais se referem a flexibilidade e a possibilidade de reconfiguração de sistemas dentro da fábrica, tornando seus setores e equipamentos integrados. Os sistemas horizontais lidam com a integração de parceiros que estão fora da fábrica. Com essa integração a indústria tende a ficar mais automatizada.

Internet das Coisas Industrial (IIoT) – O termo "internet das coisas" diz respeito a uma rede de objetos conectados entre si. Para Borlido (2017), com sua utilização é possível que esses objetos interajam com um ambiente existente e respondam a ele caso haja mudanças, dando início ao processo de obtenção de respostas em tempo real. A principal tarefa da Internet das Coisas (IoT) é se conectar à internet coletando dados de objetos físicos. Na Indústria, a IIoT pode ser utilizada para gerenciar ativos, analisar parâmetros de manutenção. Além disso, permite a conexão direta com o fornecedor de produtos, que podem analisar sua utilização na linha de produção, bem como os dados de entrada e saída de material em tempo real. Tais ferramentas aumentam a rapidez na tomada de decisão, tendem a diminuir erros e desperdício de materiais, influenciando no ganho de tempo e criando oportunidade para novas produções e negócios.

Simulação – As simulações serão usadas para espelhar o mundo físico num mundo digital em tempo real (gêmeo digital), onde se pode reproduzir máquinas, produtos e humanos. Pode-se simular em duas ou três dimensões (2D e 3D, respectivamente) o consumo de energia e as configurações de máquina para o próximo produto antes do início da produção, por exemplo, reduzindo o tempo necessário para a configuração do equipamento em espaço físico, uma vez que esses parâmetros já podem ser definidos por meio da simulação (ERBOZ, 2017).

Realidade aumentada – De acordo com Pereira e Simonetto (2018), os sistemas baseados em realidade aumentada podem fornecer informações em tempo real para os trabalhadores, auxiliando a tomada de decisão. Essa tecnologia aumenta a interação humano-máquina, ao permitir controle remoto de tarefas de manutenção e inspeção visual fornecidos pelo humano virtualmente.

Manufatura Aditiva – permite que produtos sejam produzidos em menor escala, customizados e descentralizados. Esse método de fabricação diminui as despesas com estocagem e transporte de uma grande quantidade de produtos. Uma aliada desse pilar é a impressão 3D, que permite a criação de objetos personalizados (LANDHERR et al., 2016).

Segurança cibernética – Com o aumento da conectividade e o uso de protocolos de comunicação que surgiram com a Indústria 4.0, é preciso proteger sistemas industriais de ataques cibernéticos, uma ameaça que tem aumentado cada vez mais. Em resposta a esse aumento, sistemas confiáveis com gerenciamento de identidade e acesso sofisticados têm sido necessários. Os ataques cibernéticos possuem impactos destrutivos às indústrias, a depender da intenção da invasão. Soluções que previnam e defendam esses ataques são necessários para diminuir seus efeitos negativos (ROSSIT et al., 2019).

3 METODOLOGIA

Trata-se de artigo de revisão bibliográfica, onde se procura por temas que já foram contextualizados e estudados por diversos grupos de pesquisadores. Ao reunir esses trabalhos, é possível ter uma visão de como o tema foi e tem sido estudado através do tempo e da evolução tecnológica que o acompanha. Devido a isso, não se delimitou um período de tempo para a seleção dos artigos, já que é interessante selecionar estudos que demonstram como o assunto era tratado no passado e como está sendo tratado agora.

4 CIBERSEGURANÇA NA INDÚSTRIA 4.0

No passado, as fábricas eram fechadas e a sua segurança era garantida por meio de isolamento e controle de acesso físico. Em contraste, hoje, as máquinas modernas são equipadas com uma série de dispositivos inteligentes, como sensores e atuadores, e são conectadas a outras máquinas e sistemas de processamento de dados por meio de redes sem fio ou Ethernet com fio. Os componentes usam protocolos específicos para se comunicar em redes industriais dedicadas, mas podem não fornecer proteção adequada contra ameaças cibernéticas. Para Wu et al. (2018), essas conexões de rede inseguras tornam os sistemas de manufatura vulneráveis a cada vez mais ataques cibernéticos, de modo que usuários não autorizados possam acessar os dados associados a esses sistemas.

Segundo Thames e Schaefer (2017), cibersegurança e segurança da informação giram em torno de três principais pilares: confidencialidade, integridade e disponibilidade. Essas três fundações podem facilmente experienciar tensões entre si. Por exemplo, é possível desenvolver camadas de proteção – tanto físicas quanto eletrônicas – para os dados e sentir-se confiante de que eles permanecerão confidenciais e inalterados, mas isso não parece promissor se os dados estiverem tão protegidos que são inacessíveis a quem precisa deles. Por outro lado, fazer com que os dados se tornem disponíveis para usuários legítimos significa que eles também estarão disponíveis para indivíduos que podem coletar

informações não autorizadas, assim violando a confidencialidade, ou podem maliciosamente mudar dados, destruindo sua integridade.

É do entendimento de Cruz (2013) que o risco de invasão, que concede acesso a informações, vem de uma série de falhas cujo impacto e consequente dano à Indústria depende das oportunidades disponíveis ao invasor, sua habilidade e sua motivação. Por exemplo, uma conta virtual com senha de acesso simples exige muito pouco esforço e capacidade para ser invadida. Com pouco conhecimento técnico, invasores podem usar ferramentas disponíveis na *Internet* para conseguir acesso e explorar seu conteúdo de modo a completar seu objetivo, seja ele motivado por ganho financeiro, vantagens comerciais ou protestos políticos.

Uma condição relacionada à segurança de rede diz respeito ao grau de conhecimento das pessoas sobre as vulnerabilidades nos sistemas de controle digital e gerenciamento de informações. Quanto menor o conhecimento sobre as vulnerabilidades do sistema, maior a possibilidade de invasões maliciosas, sendo importante destacar internamente o impacto de possíveis invasões na organização (GOES, 2019). Para evitar ataques cibernéticos no ambiente industrial, é necessário manter a proteção da comunicação adotando protocolos de acesso estrito. Rübmann et al. (2015) entende que manter um gerenciamento complexo, identificando permissões de acesso ao sistema de *hardware* e obtendo permissões de usuário torna-se cada vez mais importante.

O Centro Nacional de Cibersegurança do Reino Unido - NCSC (2016) criou uma cartilha onde descreve que os ataques mais comuns podem ser divididos em duas categorias: ataques sem alvo definido, onde se procuram máquinas e serviços vulneráveis, sem discriminação de quem são ou onde pertencem. Para isso, é possível utilizar técnicas facilmente encontradas *online*, como:

a) *Phishing* – Envio de e-mails a muitas pessoas solicitando informações como dados bancários ou as encorajando a visitar páginas falsas na *internet* conforme mostra a Figura 2;
b) *Water holing* – criação de uma página falsa na *internet* que compromete a existência da página original para extorquir os usuários que a visitam;
c) *Ransomware* – distribuição de *malware* que infecta o equipamento e exibe mensagens que exigem pagamento de uma taxa para que o sistema volte a funcionar;
d) *Scanning* – ataques aleatórios a diversas páginas na *internet* onde podem ser coletados dados como endereço IP, nomes de dispositivos, sistema operacional etc.

Figura 2 – Ataque do tipo *Phishing*

Fonte: Kratikal Tech PVT LTD (2019)

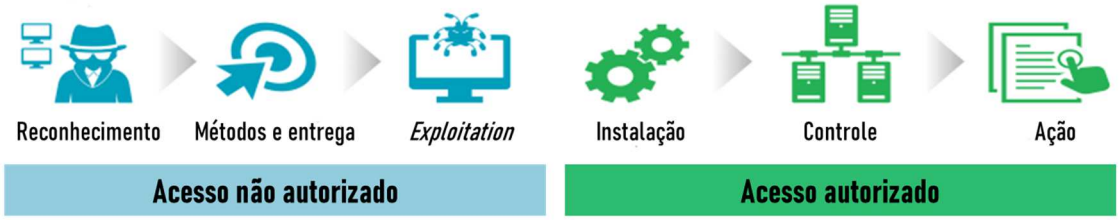
Ainda de acordo com a cartilha do NCSC (2016), outra categoria de ataques é a que envolve alvos marcados. Nestes ataques, há interesse em comprometer ou acessar os dados que a sua organização produz, seja para benefício próprio ou por encomenda. É comum que nesse processo os responsáveis pelo ataque levem meses estudando e definindo qual é a melhor via de acesso ao alvo, seja ele o usuário ou o próprio sistema. Esse ataque é comumente mais danoso do que os ataques não direcionados a um alvo específico, pois foi pensado para invadir um sistema em particular. Os ataques a alvos específicos podem incluir:

a) *Spear-phishing* – envio de e-mails para indivíduos marcados contendo *malware* em arquivos anexos que serão descarregados;
b) *Botnet* – também conhecido como Ataque de Negação de Serviço Distribuído (DDOS), que interfere no funcionamento do serviço ao sobrecarregar seu sistema com múltiplas solicitações.
c) *Supply chain* – ataque feito ao comprometer um equipamento ou *software* que vai ser entregue a organização.

As vulnerabilidades que criam oportunidades para invasores podem ocorrer por falhas no sistema, utilização de recursos extras que ao mesmo tempo em que aumentam a experiência do usuário e ajudam a diagnosticar problemas, também podem ser utilizados por invasores, e erro do usuário – ao divulgar informações úteis a invasores, como a função de funcionários e seus horários de trabalho, definir senhas fracas e instalar *malwares* (LEZZI et al., 2018).

As fases de um ataque cibernético são descritas por Palo Alto Networks (2015) e podem ser visualizadas na Figura 3, que ilustra o reconhecimento – fase em que os invasores pesquisam e identificam seus alvos; Métodos e entrega – quando definem qual vai ser o modo de ação e decidem a quem entregar; *Exploitation* – já dentro do sistema, os invasores conseguem acesso e podem tomar controle das ações; Instalação – os invasores estabelecem as operações, *root kit*, definem privilégios; Comando e Controle – estabelecimento de um canal para onde serão transferidos os dados entre dispositivos infectados e o servidor; Ação – quando invasores cumprem seus objetivos ao invadirem o sistema, de acordo com a motivação do ataque.

Figura 3 – Estágios do ataque cibernético



Fonte: Palo Alto Networks (2015)

4.1 Mitigando riscos de ataques cibernéticos

A princípio, deve-se atentar a segurança dos dispositivos periféricos criando uma linha de defesa, onde o escopo de segurança deve ser definido por meio de recursos de *firewall*, Sistema de Detecção de Intrusão (IDS) e Sistema de Prevenção de Intrusão (IPS). Dentre os métodos de proteção de rede, Goes (2019) apontou que existem vários meios usados para protegê-lo, como a configuração que permite acesso apenas por pessoal autorizado, utilizando *Network Acess Control (NAC)*. A segmentação da rede fornece uma lógica que pode distinguir entre grupos de *hardware* e gerenciar a transmissão de informações entre eles, o que poderá dificultar o acesso indevido e aumentar a probabilidade de se detectar um agente invasivo.

As soluções de criptografia permitem que você garanta a autenticação de usuários com as identidades selecionadas para acessarem o sistema. Além da criptografia, mecanismos que permitem o uso de várias chaves de acesso também podem ser usados para facilitar as garantias necessárias ao usar certificados digitais. Essas medidas confirmam a integridade e o sigilo das informações (GOES, 2019).

A avaliação da necessidade de atualização dos dispositivos de *hardware* e *software* também é muito importante, pois garante a evolução dos sistemas de defesa. Manter um sistema desatualizado facilita a invasão, já que ele pode se tornar obsoleto para identificar e lidar com invasões.

Para mitigar a fase de reconhecimento de um ataque cibernético, o treinamento dos usuários é ponto importante. Todos eles devem entender como publicar informações sobre sistemas e a forma de operação pode revelar vulnerabilidades potenciais dentro da empresa. A NCSC (2016) destaca a importância de estar atento aos riscos de se discutir tópicos de trabalho em redes sociais e conversas casuais. A fase de definição do alvo, método e entrega do ataque pode ser identificada e ter seus riscos diminuídos ao utilizar um *antimalware* atualizado para bloquear e-mails maliciosos e prevenir que conteúdos suspeitos sejam descarregados de *websites*. Utilizar ferramentas como *firewalls* e *proxy servers* podem bloquear *websites* inseguros e gerar uma lista destes.

A NCSC (2016) ainda diz que, para mitigar os riscos nesse estágio, também é recomendado que se sejam definidas senhas mais complexas com autenticação adicional para acessar conteúdos confidenciais. Para os estágios de instalação, comando e controle, recomenda-se novamente a utilização de *antimalware* que detecte códigos maliciosos no sistema. Em conjunto a isso, habilitar controles de acesso e definir configurações que removam programas desnecessários e usuários padrões do sistema pode ser aliado ao processo. Além de detectar uma ameaça é importante monitorar todas as redes que podem ser portas de entrada para este tipo de ação.

Caso os cuidados e recomendações de segurança sejam seguidos, a maioria dos ataques não terá sucesso, a não ser que o invasor seja experiente e tecnicamente capaz com motivação para acessar o seu sistema. Neste caso, é muito mais difícil detectar suas ações e eliminar a sua presença, sendo necessária utilização de estratégias para defender e eliminar as ameaças do sistema.

O NIST – Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (2018) em sua publicação intitulada "Framework for Improving Critical Infrastructure Cybersecurity", cita 5 passos para lidar com ataques cibernéticos, sendo:

a) Identificar: desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética para sistemas, pessoas, dados e recursos. Compreender o contexto de negócios, os recursos disponíveis e os riscos de segurança cibernética relacionados permitem que uma organização se concentre e priorize seus esforços de acordo com sua estratégia de gestão de riscos e necessidades de negócios. Exemplos de categorias de desta função incluem: Gerenciamento de ativos; Ambiente de negócios; Governança; Avaliação de risco; e Estratégia de Gerenciamento de Risco;
b) Proteger: desenvolver e implementar salvaguardas adequadas para garantir a entrega dos serviços. A função de proteção suporta a capacidade de limitar ou conter o impacto de um potencial evento de cibersegurança. Exemplos de categorias dentro desta função incluem: Gerenciamento de identidade e controle de acesso; Conscientização e treinamento; Segurança de dados; e Manutenção;
c) Detectar: desenvolver e implementar atividades apropriadas para identificar a ocorrência de um evento de cibersegurança. Detectar permite a descoberta efetiva de eventos de segurança cibernética. Exemplos de categorias dentro desta função incluem: Segurança e monitoramento contínuo; e Processos de detecção;
d) Responder: desenvolver e implementar atividades apropriadas para tomar medidas em relação ao incidente de segurança cibernética detectado. Responder aumenta a capacidade de conter o impacto de um potencial incidente de segurança cibernética. Exemplos de categorias dentro desta função incluem: Planejamento de Resposta; Comunicações; Análise; Mitigação; e Melhorias.
e) Recuperar: desenvolver e implementar atividades adequadas para manter planos de resiliência para restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de cibersegurança. Recuperar oferece suporte à recuperação oportuna das operações normais para reduzir o impacto de um incidente de segurança cibernética. Exemplos de dentro desta função incluem: Planejamento de recuperação; Melhorias; e Comunicações.

5 CONSIDERAÇÕES FINAIS

Foi possível identificar os ataques cibernéticos mais comuns nos ambientes da Indústria 4.0, sendo eles o *phishing*, *water holing*, *ransomware*, *scanning*, *spear-phishing*, *botnet* e *suply chain,* bem como encontrar quais são as melhores formas de lidar com estes tipos de ataque, descritos como o treinamento das pessoas com acesso ao sistema, tanto sobre questões técnicas, quanto questões éticas. Outras formas de lidar com esses taques são desenvolver protocolos de prevenção ao identificar e lidar com vulnerabilidades do sistema, utilizar programas *antimalware* e mantê-los ativos, e atualizados. Desta forma, torna-se possível mitigar os ataques cibernéticos que podem comprometer a segurança do sistema, dos dados e da segurança das pessoas que atuam em ambientes já adaptados à quarta revolução industrial.

REFERÊNCIAS

ALBERTIN, Marcos; ELIENESIO, Maria; AIRES, Aline; PONTES, Heráclito; ARAGÃO, Dmontier. Principais inovações tecnológicas da Indústria 4.0 e suas aplicações e implicações na manufatura*. In*: SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO, 24, 2017, Bauru, SP. **Anais** [...] Bauru, SP: UNESP, . 2017. Disponível em: https://simpep.feb.unesp.br/anais_simpep.php?e=12. Acesso em: 16 set. 2020.

BARTODZIEJ, Christoph. **The concept Industry 4.0**: an empirical analysis of technologies and applications in production logistics. Wiesbaden: Springer Gabler BestMasters, 2017. 150 p.

BAHRIN, M. A. K. et al. Industry 4.0: a review on industrial automation and robotic. **Jurnal Teknologi Sciences & Engineering**, p. 137–143, 2016. Disponível em: https://journals.utm.my/jurnalteknologi/article/view/9285/5537. Acesso em: 15 dez. 2020.

BORLIDO, David. **Indústria 4.0:** aplicações a sistemas de manutenção. 2017. Dissertação (Mestrado Integrado em Engenharia Mecânica) - Universidade do Porto, Porto, Portugal, 2017.

CRUZ, Samuel. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Brasília: Instituto de Pesquisas Aplicadas – IPEA, 2013.

ERBOZ, Gizem. How to define Industry 4.0: the main pillars of Industry 4.0. **Managerial trends in the development of enterprises in globalization Era**, Nitra, Slovakia, p. 761-767, Out. 2017.

GILCHRIST, Alasdair. **Industry 4.0**: the industrial internet of things. Nova Iorque: Apress, 2016. 250 p.

GOES, Nuno. Cibersegurança na Indústria Nacional: dossiê sobre cibersegurança industrial. **Robótica**, Porto, v. 1, n. 114, p.56-62. 2019.

INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM). IBM study shows data breach costs on the rise; financial impact felt for years. **News Room IBM**. July 30, 2019. Disponível em: https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years. Acesso em: 16 set. 2020.

KRATIKAL TECH PVT LTD. **The complete guide to "phishing attack" for 2019.** Disponível em: https://kratikal.medium.com/the-complete-guide-to-phishing-attack-for-2019-a90535ebd430. Acesso em: 15 dez. 2020.

LANDHERR, Martin; ULRICH, Schneider; BAUERNHANSL, Thomas. The application center Industrie 4.0: Industry-driven manufacturing, research and development. **Procedia CIRP**, v. 57, p. 26-31, 2016. Disponível em: https://www.sciencedirect.com/science/article/pii/S2212827116311593?via%3Dihub. Acesso em: 15 dez. 2020.

LEZZI, Mariana; LAZOI, Mariangela, CORALLO, Angelo. Cybersecurity for Industry 4.0 in the current literature: a reference framework. **Comput. Ind.** v. 103, 97–110, 2018.

NATIONAL CYBER SECURITY CENTRE (NCSC). Common cyber-attacks: reducing the impact. **Cyber Attacks White Paper,** January 2016. Disponível em: https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact. Acesso em: 15 dez. 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Framework for Improving Critical Infrastructure Cybersecurity.** Versão 1.1, 16 abr. 2018. Disponível em: https://doi.org/10.6028/NIST.CSWP.04162018. Acesso em: 15 dez. 2020.

PALO ALTO NETWORKS. **Breaking the cyber attack lifecycle**: the enterprise security company. 2015. Disponível em: https://gantech.com.br/wp-content/uploads/2017/01/breaking-the-cyber-attack-lifecycle.pdf. Acesso em: 15 dez. 2020.

PEREIRA, Adriano; SIMONETTO, Eugênio. Indústria 4.0: conceitos e perspectivas para o Brasil. **Revista da Universidade Vale do Rio Verde**. v.16, p. 1-9, 2018.

RAPOSO, Dandara. Indústria 4.0: Realidade, mudanças e oportunidade. Orientador: Agnaldo Reis. 2018. 38 f. Monografia (Graduação em Engenharia de Controle e Automação) - Universidade Federal de Ouro Preto, Ouro preto, Minas Gerais, 2018.
RETHINK ROBOTICS. Disponível em: https://www.rethinkrobotics.com. Acesso em: 9. Out. 2020.

ROSSIT, Daniel; TOHMÉ, Fernando; FRUTOS, Mariano. Production planning and scheduling in Cyber-Physical Production Systems: a review. **International Journal of Computer Integrated Manufacturing**, UK, p. 1-11, 2019.

RÜBMANN, Michael; LORENZ, Markus, GERBERT, Philipp; WALDNER, Manuela; ENGEL, Jan; HARNISCH, Michael. Industry 4.0: the future of productivity and growth in manufacturing industries. **Boston Consulting Group**. 2015. Disponível em: https://www.bcg.com/pt-br/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries. Acesso em: 15 dez. 2020.

THAMES, Lane; SCHAEFER, Dirk. **Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing**. Cham, Suiça: Springer, 2017.

WU, Dazhong; REN, Anqi; ZHANG, Wenhui; FAN, Feifei; LIU, Peng; FU, Xinwen; TERPENNY, Janis. Cybersecurity for digital manufacturing. **J. Manuf. Syst**. v. 48, p. 3–12, 2018.

AGRADECIMENTOS

Agradeço primeiramente a Deus por minha vida, pelas bênçãos em minha vida e carreira.

Agradeço a ajuda dos colegas e docentes deste curso pelo apoio, ensino e todo o aprendizado proporcionado.

Agradeço o apoio da minha família, que sempre esteve presente e me auxiliando não só durante o curso, mas como em todos os momentos de minha vida.

Sobre os autores:

_____

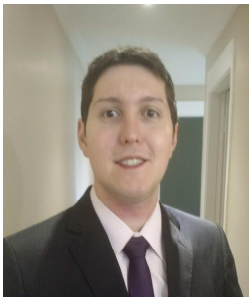
[i] RENATO MATTES CANOSO

Atualmente trabalha com projetos de automação industrial com CLPs, Drives, IHMs e sistemas supervisório na Termomecânica São Paulo SA; atuando dede 1986 na área da eletroeletrônica em manutenção e desenvolvimento de máquinas industriais; lecionou cursos de eletroeletrônica e CLP por sete anos no SENAI Almirante Tamandaré. Graduado em tecnologia eletrônica pela Faculdades Integradas Senador Flaquer (1995), cursando atualmente a Pós-Graduação em Industria 4.0 pela Faculdade SENAI de Tecnologia Mecatrônica (2020).

[ii] JOSÉ ROBERTO DOS SANTOS

Atualmente ministra aulas na pós-graduação de Indústria 4.0 e na graduação em Tecnologia em Mecatrônica na Faculdade SENAI de Tecnologia Mecatrônica, que fica no SENAI Armando de Arruda Pereira. Assessora também o Instituto SENAI de Tecnologia Metalmecânica em projetos industriais com foco na Indústria 4.0. Durante 9 anos ministrou aulas pelo SENAI-SP, nos cursos de técnico em eletroeletrônica, cursos de aprendizagem industrial eletricista de manutenção e mecânico de usinagem, além de Formação Inicial e Continuada (FIC) com cursos voltados a área de redes de computadores e programação, possui treinamento de Linux, cisco e Microsoft. Possui Pós-graduação na área de segurança da informação pela Uninove (2016), graduação em tecnologia da informação e bacharel em sistema da informação (2009), além de superior em Automação industrial. Tem experiencia na área de Segurança da informação, administração de ambientes de redes Windows e Linux, automação indústria. CV: http://lattes.cnpq.br/2495692420793433

[iii] THIAGO TADEU AMICI



Ministra aulas na pós-graduação de Indústria 4.0 e na graduação em Tecnologia em Mecatrônica Industrial no SENAI Armando de Arruda Pereira, além de assessorar o Instituto SENAI de Tecnologia Metalmecânica. Durante 7 anos ministrou aulas pelo SENAI-SP, nos cursos de técnicos de Mecatrônica, Eletrônica, Eletroeletrônica e Automação Industrial, além de Formação Inicial e Continuada (FIC) com cursos voltados ao CLP da Siemens. Possui mestrado em Automação e Controle e Processos pelo Instituto Federal de Ciências e Tecnologia de SP (IFSP - 2018), graduação em Engenharia Elétrica pela Faculdade de Engenharia São Paulo (2012), graduação em Tecnologia em Automação Industrial pelo IFSP (2009) e ensino profissionalizante em Eletrônica pela Instituição Liceu de Artes e Ofícios de São Paulo (2002). Tem experiência na área de Engenharia Elétrica, Automação Industrial, Mecatrônica, Robótica e Indústria 4.0. Experiência internacional na aprovação de linha de produção (Cavemil) em Milão na Itália e sua instalação no Brasil. Participou do desenvolvimento do projeto, programação, montagem e apresentação da Linha de Manufatura Avançada Industrial 4.0 realizada em parceria entre o SENAI-SP e a ABIMAQ, que foi exposta na FEIMEC 2018 e da linha de Confecção 4.0, em parceria entre o SENAI-SP e a ABIT. CV: http://lattes.cnpq.br/9165856219131658

[iv] **PAULO SEBASTIÃO LADIVEZ**

Possui graduação em Engenharia Elétrica pela Universidade Mogi das Cruzes (1984) com especialização em Tecnologias e Sistemas de Informação pela Universidade Federal do ABC (2013). Atualmente é professor da Faculdade SENAI de Tecnologia Mecatrônica, lecionando as disciplinas Projetos, Microcontroladores, Linguagem de Programação no curso Tecnológico em Mecatrônica Industrial e na Pós-Graduação em Automação Industrial. Tem experiência na área de Engenharia Eletrônica, com ênfase em Automação Industrial e Mecatrônica, atuando principalmente nos seguintes temas: Mecatrônica, Manufatura Digital, Redes Industriais, Automação Industrial, Microcontroladores e Controle. CV: http://lattes.cnpq.br/7235073442326291

[v] **VICENTE GOMES DE OLIVEIRA JUNIOR**

Possui graduação em Tecnologia Elétrica pela Universidade Presbiteriana Mackenzie (1982). Complemento em pedagogia na Universidade Metodista de Piracicaba (1999), Mestrado em Engenharia Mecânica pela Universidade Estadual de Campinas (2006). Atualmente é professor na área de automação industrial da Faculdade Senai de Tecnologia Mecatrônica nos cursos de graduação e pós-graduação. Tem experiência na área de Automação Industrial, atuando principalmente nos seguintes temas: pneumática, eletropneumática, hidráulica, eletrohidráulica, controlador programável, robótica básica, sistema supervisório, algumas redes industriais.