INSTITUTO FEDERAL DO PARANÁ

PEDRO EDSON DE SOUZA

SEGURANÇA CIBERNÉTICA EM TECNOLOGIA DE AUTOMAÇÃO E OPERACIONAL

COLOMBO

2021

INSTITUTO FEDERAL DO PARANÁ

PEDRO EDSON DE SOUZA

SEGURANÇA CIBERNÉTICA EM TECNOLOGIA DE AUTOMAÇÃO E OPERACIONAL

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal do Paraná, Campus Colombo, como requisito parcial para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Prof. Dr. Eduardo Liquio Takao

COLOMBO

2021

TERMO DE APROVAÇÃO

PEDRO EDSON DE SOUZA

SEGURANÇA CIBERNÉTICA EM TECNOLOGIA DE AUTOMAÇÃO E OPERACIONAL

Trabalho de Conclusão de Curso aprovado como requisito parcial para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, pelo Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, do Instituto Federal do Paraná, Campus Colombo, pela seguinte banca examinadora:

Prof. Dr. Eduardo Liquio Takao

Orientador

Prof. Me. Marcos Dinís Lavarda

Prof. Me. Ademir Luiz do Prado

Colombo, 22 de outubro de 2021.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela saúde e paz para concluir este trabalho de conclusão de curso num momento difícil de pandemia SAR-COVID 19.

Agradeço a todos os professores e professoras do curso de graduação pelo conhecimento que adquiri no decorrer do curso.

Agradeço a minha família pelo apoio e compreensão em todo o período de estudo.

RESUMO

O presente trabalho de conclusão de curso em Análise e Desenvolvimento de Sistemas teve como objetivo de abordar as vulnerabilidades no ambiente de segurança cibernética, bem como conhecer as vulnerabilidades existentes a fim de compreender e analisar as práticas de segurança cibernética em tecnologia de automação e industrial e, dessa forma, verificar a aderência da segurança cibernética baseado nas melhores práticas em segurança cibernética para tecnologia de automação e operacional no Brasil. Para chegar ao objetivo proposto realizamos uma pesquisa bibliográfica, bem como um levantamento sobre o tema a partir de sites de pesquisa na internet, visando conhecer as vulnerabilidades do ambiente cibernético. Assim, identificamos algumas vulnerabilidades voltadas as redes de comunicação industrial, sistemas de controle e automação industrial, as pessoas, o ambiente interno, redes corporativas, Virtual Private Network (VPN) entre outras. Ainda, na segurança cibernética em tecnologia operacional e automação foi possível entender que os riscos são diferentes no domínio de Tecnologia de Informação (TI) e Tecnologia de Operação (TO), e que as ameaças de ataques podem ser as mesmas, especialmente nos sistemas industriais modernos. Também foi possível saber que há ferramentas de segurança cibernética como o Sistema de Controle de Supervisão e Aquisição de Dados (SCADA), Sistema de Controle Industrial (ICS), Controlador Lógico Programável (PLC) e Sistema Instrumentado de Segurança (SIS) que contribuem para uma política de proteção de dados bem como apresentar algumas das melhores práticas em segurança cibernética. Assim, conclui-se que deve haver ações de prevenção e proteção, programação e implementação de controles à fim de impedir previamente a ocorrência de ataques cibernéticos.

Palavras-chave: Segurança cibernética, automação, ataque cibernético.

ABSTRACT

This course completion work in Systems Analysis and Development aimed to address vulnerabilities in the cybersecurity environment, as well as to know the existing vulnerabilities in order to understand and analyze cybersecurity practices in automation and industrial technology and, in this way, verify the adherence of cybersecurity based on the best practices in cybersecurity for automation and operational technology in Brazil. In order to reach the proposed objective, we carried out a bibliographical research, as well as a survey on the subject from internet research sites, in order to know the vulnerabilities of the cybernetic environment. Thus, we identified some vulnerabilities related to industrial communication networks, industrial control and automation systems, people, the internal environment, corporate networks, Virtual Private Network (VPN) among others. Still, in cyber security in operational technology and automation it was possible to understand that the risks are different in the domain of Information Technology (IT) and Operation Technology (OT), and that the threats of attacks can be the same, especially in industrial systems modern. It was also possible to know that there are cyber security tools such as the Supervision Control and Data Acquisition System (SCADA), Industrial Control System (ICS), Programmable Logic Controller (PLC) and Security Instrumented System (SIS) that contribute to a data protection policy as well as presenting some of the best practices in cyber security. Thus, it is concluded that there must be prevention and protection actions, programming and implementation of controls in order to previously prevent the occurrence of cyber attacks.

Keywords: Cyber security, automation, cyber attack.

LISTA DE SIGLAS E ABREVIATURAS

CIS	- Sistema de Controle Industrial
CISA	- Agência de Segurança Cibernética e de Infraestrutura
CSA	- Avaliação Completa da Cibe segurança
DCS	- Sistema de Controle Distribuído
IACS	- Sistema de Automação e Controle Industrial
ICS	- Sistema de Controle Industrial
IDPSs	- Sistema de Detecção e Prevenção de Intrusão
IDSs	- Intrusão Sistemas de Detecção
IEC	- Comissão Eletrotécnica Internacional
IoT	- Internet das Coisas
ISA	- Sociedade Internacional de Automação
PLC	- Controlador Lógico Programável
PNSIC	- Plano Nacional de Segurança de Infraestruturas Críticas
SCADA	- Sistema de Controle de Supervisão e Aquisição de Dados
SIS	- Sistema Instrumentado de Segurança
TI	- Tecnologia de Informação
TIC	- Tecnologia da Informação e Comunicação da Informação
TO	- Tecnologia de Operação

SUMÁRIO

1. INTRODUÇÃO

Com a velocidade de transformação do mundo tecnológico, e o alto nível de conectividade, aumentou a quantidade de ataques cibernéticos com roubo de dados sensíveis, segredos industriais, pesquisas, acesso e controle de linhas de produção automatizadas, ataques a empresas de energia elétrica, empresas de água e saneamento, entre outras.

Diante disso, é possível perceber que há um aumento de ataques cibernéticos aos diversos segmentos industriais, operacionais, prestação de serviços, investimentos e outros. Nesse sentido, as empresas tem cada vez mais buscado desenvolver suas políticas de segurança cibernética que englobe todos os processos automatizados ou acessados de forma remota ou por pessoa *in loco* para mitigar o risco de ataque cibernético.

Assim, as fraquezas de segurança cibernética para as indústrias demandam em um grande esforço das empresas para a criação de uma política de segurança cibernética corporativa, com diretrizes, responsabilidades e conceitos, que envolvam todos os usuários que tenha acesso na organização.

Portanto, a segurança cibernética em automação e operacional deve ser feita com a utilização de todas as ferramentas de segurança cibernética disponíveis no mercado com a finalidade de evitar um ataque cibernético com consequências desastrosas para as empresas. Contudo, deve haver treinamentos e conscientização das pessoas quanto a sua importância na proteção dos dados da empresa pois a segurança cibernética é essencial para todos os envolvidos.

Dessa forma, pretende-se conhecer as vulnerabilidades encontradas no ambiente de segurança cibernética, compreender o ambiente de segurança cibernética, analisar as boas práticas de segurança cibernética e abordar as vulnerabilidades de segurança cibernética em tecnologia de automação e operacional.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Este trabalho tem como objetivo geral abordar as vulnerabilidades no ambiente de segurança cibernética em tecnologia de automação e industrial.

2.2 OBJETIVOS ESPECÍFICOS

a) Conhecer as vulnerabilidades existentes em segurança cibernética de automação e industrial.
b) Compreender o ambiente de segurança cibernética em tecnologia de automação e industrial.
c) Analisar as práticas de segurança cibernética em tecnologia de automação e industrial.

3 REVISÃO DA LITERATURA

Este capítulo se propõe a descrever a Metodologia e o Referencial Teórico pesquisado para a escrita deste trabalho.

3.1 METODOLOGIA

No presente trabalho foi utilizado o método de pesquisas bibliográficas e levantamento de conhecimento existente na internet para conhecer e entender a metodologia da segurança cibernética. Nesse sentido para Ruiz (1986, pg. 67):

> "não é necessário ler tudo que um autor escreveu, ou tudo que muitos escreveram sobre o assunto, mas é preciso ler com critério, com discernimento, com a atenção necessária para distinguir o fundamental do secundário, o relevante do irrelevante para o tema que se tem em mãos".

No entanto, Marconi (2002, pg. 35) diz que "na interpretação dos dados da pesquisa é importante que eles sejam colocados de forma sintética e de maneira clara e acessível", sendo estas pesquisas adaptadas conforme o andamento do trabalho de conclusão do curso.

Também, para auxiliar na interpretação dos dados, foi utilizado alguns quadros para facilitar o leitor na interpretação e compreensão dos dados apresentados. (MARCONI, 2002). Nesse sentido, "o assunto de uma pesquisa é qualquer tema que necessita melhores definições, melhor precisão e clareza do que já existe sobre o mesmo", (CERVO, 1983, pg. 74) e também o presente trabalho foi dividido em partes que se complementam para o entendimento do assunto abordado (CERVO, 1983).

Do mesmo modo, é importante ressaltar que a pesquisa na internet foi necessária para aprofundar o conhecimento sobre o assunto proposto, pois "a Internet pode propiciar ao pesquisador a recuperação de grande diversidade de materiais úteis, muitas vezes não encontrados em bibliotecas". (CRUZ, 2010, pg. 126). Assim, a internet "possibilita a realização de pesquisas em uma rede de computadores interligados no mundo inteiro, por meio da qual o pesquisador pode ter acesso a uma grande quantidade de informações, que poderão servir como referência ao estudo" (CRUZ, 2010, pg. 127) e com o acesso à Internet, essa "forma de pesquisa tornou o acesso muito mais amplo e praticamente sem fronteiras físicas". (ANDRADE, 2003, pg. 44).

Dessa maneira, o trabalho foi desenvolvido visando abordar as vulnerabilidades no ambiente de segurança cibernética em tecnologia de automação e industrial, bem como conhecer essas vulnerabilidades e compreender e analisar o ambiente e as melhores práticas de segurança cibernética.

3.2 REFERENCIAL TEÓRICO

3.2.1 Fundamentos da Segurança Cibernética

No mundo interligado pela internet, é fundamental políticas de segurança com “instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações” (MITNICK, 2003 pg. 208). Nesse sentido, “uma empresa precisa coordenar seus esforços em todo o seu sistema de informações e tecnologia” (RS, 2022) para proteger informações da organização.

Diante disso, a fim de proteger e promover o gerenciamento e a “segurança dos dados digitais e sistemas de armazenamento eletrônico” (STW, 2022), temos os três pilares da segurança da informação, a integridade, a disponibilidade e a confidencialidade.

De acordo com (IMO, 2022), integridade é: “a garantia de que a informação é utilizada sem apresentar erros”, e, para (SENHA, 2022), integridade é “responsável por manter as características originais dos dados, assim como foram configurados em sua criação”.

Também, de acordo com (IMO, 2022), a disponibilidade é: “a garantia de que a informação está disponível para o usuário e para o sistema de informação”, e, dessa perspectiva (SENHA, 2022), diz que a disponibilidade “ideal num sistema de informação é que os dados estejam disponíveis para o que for necessário, garantindo o acesso dos usuários no tempo integral”.

A confidencialidade, ainda de acordo com (IMO, 2022), é: “a garantia de que a informação é acessada somente por usuários com o devido direito”, e, segundo (SENHA, 2022), a base da confidencialidade “é controlar o acesso por autenticação de senha, podendo ser também por verificação biométrica, e criptografia”.

Assim sendo, os pilares da segurança da informação são importantes ferramentas que trazem benefícios a organização e “muitas soluções já são usadas

por diversas empresas, buscando eliminar os riscos aos sistemas de segurança, consolidando os pilares da segurança da informação em sua organização” (SENHA, 2022).

3.2.2 Caracterização de Ataques Cibernéticos

Os ataques cibernéticos são cada vez mais frequentes neste ambiente que vivemos atualmente e “as empresas precisam considerar o risco e o custo dos ciberataques, investindo em métodos para proteger os ativos digitais da organização” (CLARANET, 2021), bem como para proteger segredos industriais, danos à imagem da empresa, entre outros. Além disso, (IEC, 2021)

> “ativos cibernéticos apresentam sérios desafios e as empresas devem determinar como lidar com a realidade dos ataques cibernéticos deliberados, bem como permanecer resilientes diante de ameaças cibernéticas inadvertidas decorrentes de erros pessoais, a complexidade dos sistemas, falha de equipamento e natural desastre”.

Nesse sentido, a evolução das tecnologias e a facilidade de acesso a rede de computadores deixou mais complexa o ambiente cibernético “e a infraestrutura de TI sofrem riscos diários de intrusão visando o “roubo” de dados e a disseminação de códigos maliciosos e vírus, o que pode afetar, sobremaneira, a operação da empresa” (FERNANDES, 2012 p. 9).

O número de acidentes cibernéticos é muito grande e não é possível saber a quantidade exata de ataques, “a grande maioria dos ataques ainda não chega ao sistema de controle, ou não são detectados pela falta de sistemas de detecção em plantas industriais” (RC&I, 2021). Além do mais, “as ferramentas usadas pelos invasores utilizam a automação para localizar e explorar vulnerabilidades nos sistemas de uma organização, e os ataques também tornaram mais sofisticados e demorados para prevenir” (THESEUS, 2021)

“Os ataques à Segurança Cibernética Industrial são definidos com a invasão dos sistemas de controle por qualquer via de comunicação, de forma a manipular os processos controlados com a intenção de causar dano ou de interromper suas operações” (AQUARIUS, 2021)

As ameaças cibernéticas tornam-se cada vez maior na indústria, que utiliza “sistemas cyber-físicos que são capazes de fazer máquinas e humanos se comunicarem entre si por meio da Internet das Coisas (IoT) e da Internet”. (A VOZ, 2021). Do mesmo modo, “as instalações industriais de hoje dependem amplamente de software para controle da planta, em vez de dispositivos eletromecânicos tradicionais”. (MIT, 2021). Além disso, no ambiente da indústria os “dispositivos interagem com o sistema de “supervisão” de nível superior que permite aos operadores controlar os sistemas locais e a operação geral da planta, seja no local ou remotamente.” (MIT, 2021).

Nesse sentido, ressalta-se que “os ataques contra organizações industriais sempre têm o potencial de ser especialmente devastadores, tanto em termos de interrupção da produção quanto prejuízos financeiros”. (CISO, 2021).

É importante ressaltar que PAREKH, 2021, pg. 311

> “o valor dos dados residentes no IACS para a empresa aumentou significativamente a interconectividade do IACS, tanto internos quanto externos à organização. A combinação dessas tendências tornou o IACS mais vulnerável a ataques cibernéticos”.

No Quadro 1, podemos visualizar vários ataques cibernéticos com impacto no Sistema de Automação e Controle Industrial (IACS):

Quadro 1. Alguns ataques cibernéticos notáveis com impacto no IACS

Data	Alvo	Método
2000	Australian Sewage Plant	Insider
2010	Iran Uranium Enrichment	Stuxnet
2013	ICS Supply Chain attack	Havex
2014	German Steel Mill	Spear-phishing and social engineering
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2016	Ukraine Substation	CrashOverride
2017	Global shipping company	NotPetya
2017	IoT DDos attack	BrickerBot
2017	Health care, Automotive, many others	WannaCry
2017	Saudi Arabia Petrochemical	TRITON/TRISIS
2019	Norwegian Aluminum Company	LockerGoga

Fonte: ISA GLOBAL CIBERSECURITY ALLIANCE (2021)
Guia de início rápido: uma visão geral das normas ISA / IEC 62443

Os dados ilustrados acima, mostram diversos tipos de ataque cibernético com impacto no sistema IACS ocorrido em algumas empresas existentes no mundo a partir do ano 2000 até 2019, os quais ocorreram em momentos diferentes de acordo com a linha histórica dos ataques cibernéticos apresentados. Assim, para contribuir com o tema, segue algumas definições dos métodos de ataque e prejuízos causados para as empresas e a população.

Diante do quadro apresentado, (GARCIA, pg. 17, 2022) destaca que “o insider é alguém que recebeu privilégios que autorizam o acesso e a utilização de sistemas ou instalações na respectiva organização”. Este método de ataque realizado na empresa Maroochy Shire Council de Australian Sewage Plant (RISIDATA, 2022)

> “acessou computadores que controlavam o sistema de esgoto do Maroochy Shire Council, alterando dados eletrônicos em relação a estações de bombeamento de esgoto específicas e causando mau funcionamento em suas operações (...) uma estação de bombeamento transbordou fazendo com que o esgoto bruto escapasse (...) a vida marinha morreu, a água do riacho ficou preta e o fedor era insuportável para os moradores”.

O método de ataque Stuxnet (WIKIPEDIA, 2022)

> “é um worm malicioso de computador (...) O Stuxnet visa especificamente os controladores lógicos programáveis (CLPs), que permitem a automação de processos eletromecânicos, como aqueles usados para controlar máquinas e processos eletromecânicos, como aqueles usados para controlar máquinas e processos industriais, incluindo centrífugas de gás para separação de material nuclear”.

Segundo (VERNE, 2022), “O worm Stuxnet supostamente infectou mais de 200.000 máquinas em 14 instalações iranianas e pode ter arruinado até 10% das 9.000 centrífugas em Natanz”, e também (LARGE, 2022) descreve que “embora o Irã não tenha divulgado detalhes específicos sobre os efeitos do ataque, atualmente estima-se que o worm Stuxnet destruiu 984 centrífugas de enriquecimento de urânio”.

O método de ataque do malware Havex (TREND, 2022)

> “coleta informações e carrega os dados roubados para os servidores de comando e controle (C&C). O malware coleta a versão do sistema operacional da máquina infectada, o nome do computador, o usuário conectado, lista de arquivos e diretórios.
> Este Trojan pode baixar e executar arquivos de componentes. Esses arquivos de componentes são capazes de enumerar todos os recursos de rede conectados, como computadores ou recursos compartilhados”,

neste malware, (SECURITY, 2022) “os ataques watering hole envolvem software trojanizado plantado em sites comprometidos pertencentes a pelo menos três fornecedores de ICS/SCADA”.

Igualmente no método spear-phishing and social engineering (TREND, 2022) descreve que “o indivíduo ou grupo responsável pelo ataque conseguiu se infiltrar no sistema usando técnicas de spear phishing e engenharia social”, e os problemas causados pelo (TREND, 2022) “ataque, que parecia atingir especificamente operadores de plantas industriais, fez com que componentes dos controles da planta falhassem, resultando em um forno não regulamentado, o que causou danos físicos à planta siderúrgica”.

Acrescente-se ainda que, o método BlackEnergy, KillDisk (Cyberlaw, 2022) informa que “o código malicioso foi enviado através de e-mails com anexos maliciosos, visando indivíduos específicos dentro das diferentes empresas de energia, a fim de recuperar credenciais de administrador e obter acesso às redes das subestações de energia”, e como se não bastasse, houve uma segunda parte do ataque cibernético em que (Cyberlaw, 2022) “os atores ativaram um malware destrutivo KillDisk, que conseguiu limpar partes dos discos rígidos dos computadores e impedir a reinicialização dos sistemas, levando a quedas de energia”.

Além disso, (E-ISAC, 2022) “os incidentes ucranianos afetaram até 225.000 clientes em três territórios de serviço de distribuição diferentes”, com várias interrupções de energia.

Para o método de ataque cibernético CrashOverride que (DRAGOS, 2022) “interrompeu o fluxo de eletricidade manipulando ICS equipamentos e atrasou as operações de recuperação para prolongar o impacto”. Esse ataque de hackers “causaram uma queda de energia na Ucrânia em uma tentativa deliberada de deixar as residências sem eletricidade durante o que normalmente é um dos meses mais frio do ano”.

Por outro lado, o método de ataque NotPetya (PLATTE, 2022) “foi o ataque cibernético mais prejudicial que o mundo já viu, causando cerca de US$ 10 bilhões em todo mundo”.

De acordo com (INDUSTRIAL)

> “o NotPetya era composto por dois elementos principais: uma ferramenta de penetração chamada EternalBlue (...), e Mimikatz, um aplicativo de software que tinha a capacidade de extrair senhas de usuários da RAM e reutilizá-las para comprometer as máquinas alvo”,

bem como para este método de ataque (INDUSTRIAL, 2022) “o código era indiscriminado em quem atacava; ele foi projetado para causar a maior quantidade de dano o mais rápido possível e com a maior área de destruição”.

O método de ataque BrickerBot (TREND, 2022) “bloqueia o dispositivo que infecta, tornando o dispositivo permanentemente inoperável”, além disso o BrickerBot “ao explorar falhas de segurança ou configurações incorretas, esse tipo de ataque cibernético pode destruir o firmware e/ou funções básicas do sistema” (RADWARE, 2022) bem como o BrickerBot “é uma instância do mundo real de phlash – ou negação de serviço permanente (PDoS) – em que falhas de segurança no hardware do dispositivo são exploradas e seu firmware modificado” (TREND, 2022).

O WannaCry (RC&I, 2021) “acessou os sistemas de automação industrial a partir de redes corporativas locais e VPN, e a internet é a principal fonte de infecção dos computadores que fazem parte da infraestrutura industrial”.

No Brasil, após o ataque do WannaCry, (AUTOMAÇÃO, 2021)

> “pesquisa mostra que empresas de telecomunicações, transportes, energia, abastecimento de água e gás, as chamadas indústria de infraestrutura crítica, não estão adequadas a recomendações internacionais de segurança cibernética.”

Igualmente o método de ataque Triton/Trisis, pode (MIT, 2022) “desativar sistemas de segurança projetados para evitar acidentes industriais catastróficos”, bem como “o malware foi projetado para se infiltrar nos sistemas instrumentados de segurança que permitem o desligamento seguro de plantas industriais.” (CYBERSCOOP, 2022). Além disso, (MIT, 2022) “o código desonesto poderia ter levado à liberação de gás tóxico de sulfeto de hidrogênio ou causado explosões, colocando vidas em risco na instalação quanto na área circundante”.

De acordo com (SECURITY, 2022) os ataques LockerGoga “são especialmente sérios para fabricantes de metais ou produtos químicos devido ao risco de incidentes graves de segurança e ambientais e ao impacto final da deterioração de materiais em

processo e custos de limpeza”. Do mesmo modo, o ataque hacker na empresa (RECORDED, 2022) “segundo a Reuters, o ataque foi grave o suficiente para interromper partes da produção da Norsk Hydro”. Acrescentando-se que, “o ransomware bloqueia arquivos e exige um pagamento de resgate por uma chave de descriptografia” (TECHCRUNCH, 2022).

Além disso, “ataques em empresas de utilidade pública podem afetar sinais de celular, provocar apagão, explosões e inundações, por exemplo, causando impacto social, econômico, político e ameaçando até a segurança nacional.” (AUTOMAÇÃO, 2021). Nesse sentido, (CNU, 2021) “companhias elétricas acabam se tornando alvos preferidos dos criminosos, pois por serem serviços sociais imprescindíveis, podem forçar pagamentos, normalmente cobrados em criptomoedas.” Assim sendo, salienta-se que (KASPERSKY, 2021) “um único ataque cibernético à indústria tem grande potencial destrutivo e implica perigo real de danos aos processos industriais, ameaçando até a continuidade dos negócios.”

Disso discorre que, (MZ, 2021) “ao longo de 2020 até fevereiro de 2021, foram identificadas 11 Companhias que arquivaram documentos relacionados a Incidentes Cibernéticos”, e essas empresas aparecem no relatório descrito no Quadro 2:

Quadro 2 - Relação dos ataques cibernéticos ocorridos no Brasil de janeiro de 2020 a fevereiro de 2021 conforme a MZ:

SETOR	EMPRESA	DATA	ASSUNTO	INFORMAÇÕES / CONTEÚDO
Máquinas, Equipamentos, Veículos e Peças	MENDES JUNIOR ENGENHARIA S.A	14/12/2020	Ataque cibernético de hackers	Arquivos criptografados e acesso perdido
Máquinas, Equipamentos, Veículos e Peças	EMBRAER S.A.	09/12/2020	Ataque cibernético	Divulgação de dados supostamente atribuídos à Companhia
Energia Elétrica	CIA PARANAENSE DE ENERGIA - COPEL	01/02/2021	Comunicado sobre ataque cibernético	Incidente cibernético na área de TI
Energia Elétrica	CIA PARANAENSE DE ENERGIA - COPEL	10/02/2021	Recebeu informações sobre o ciberataque nos sistemas da Copel e o Plano de Contingência implementado;	Plano de Contingência
Energia Elétrica	CIA PARANAENSE DE ENERGIA - COPEL	19/02/2021	Informações sobre o Ciberataque nos sistemas da Copel e Plano de Contingência; Atualização do cenário financeiro da Companhia e execução orçamentária	Atualização do Plano de Contingência
Petróleo, Gás e Derivados	BRASKEM S.A.	19/10/2020	Braskem comunica atualizações sobre invasão em seu ambiente de Tecnologia da Informação	Possivel extração de informações e dados pessoais
Petróleo, Gás e Derivados	BRASKEM S.A.	07/10/2020	0 Braskem comunica sobre invasão em seu ambiente de Tecnologia da Informação	Possivel extração de informações e dados pessoais
Saúde	HAPVIDA PARTICIPACOES E INVESTIMENTOS SA	06/07/2020	Incidente	Possivel extração de informações e dados pessoais
Transportes	RUMO S.A.	11/03/2020	Incidente TI	Incidente cibernético na área de TI
Transportes	RUMO S.A.	15/03/2020	Incidente de TI	Atualização de informações sobre incidente cibernético
Varejo	NATURA &CO HOLDING S.A	26/06/2020	Reinício dos sistemas afetados da Avon após incidente cibernético	Atualização de informações sobre incidente cibernético
Varejo	NATURA &CO HOLDING S.A	09/06/2020	Incidente cibernético	Incidente cibernético na área de TI
Varejo	NATURA &CO HOLDING S.A	12/06/2020	Atualização sobre incidente cibernético	Atualização de informações sobre incidente cibernético
Exploração de Imóveis	ALIANSCE SONAE SHOPPING CENTERS S.A.	03/07/2020	Incidente Cibernético	Ataque cibernético por vírus
Aluguel de Veículos	CIA LOCAÇÃO DAS AMÉRICAS	23/11/2020	Indisponibilidade do Sistema de Informação	Incidente cibernético na área de TI
Aluguel de Veículos	CIA LOCAÇÃO DAS AMÉRICAS	25/11/2020	Atualização sobre o incidente de segurança	Atualização de informações sobre incidente cibernético
Energia Elétrica	ELETROPAULO METROP. ELET. SAO PAULO S.A	08/12/2020	(iv) Incidente de segurança com dados pessoais – Osasco	Incidente de segurança envolvendo alguns clientes da Companhia, em Osasco
Petróleo, Gás e Derivados	ULTRAPAR PARTICIPACOES S.A.	25/01/2021	Atualização sobre incidente cibernético	Atualização de informações sobre incidente cibernético
Petróleo, Gás e Derivados	ULTRAPAR PARTICIPACOES S.A.	12/02/2021	Incidente cibernético	Incidente cibernético na área de TI
Petróleo, Gás e Derivados	ULTRAPAR PARTICIPACOES S.A.	12/01/2021	Incidente cibernético	Incidente cibernético na área de TI

Fonte: MZ (2021), organizado pelo autor.

Disso, extrai-se do quadro acima que embora os incidentes cibernéticos relatados sejam na área de TI, estas são ligadas a TO, ou seja, estes ataques poderiam causar maiores danos a população e ao meio ambiente por meio de blecaute, abertura de barragens e interrupção na produção industrial (RAJAMÄKI, 2021). Além disso, o quadro expõe o roubo de dados sensíveis ligados diretamente a Lei 13.709 – Lei Geral de Proteção de Dados (LGPD). (Lei nº 13.709)

3.2.3 Conscientização em Segurança Cibernética

A segurança cibernética deve ter um conjunto especial de políticas que englobe a proteção de dados, governança em TI, e que forneça informações e orientações aos empregados, bem como, (RAJAMÄKI, 2021, pg. 16) “combinar os programas e as pessoas (operadores) que controlam e supervisionam o sistema, a produção e o processo”, e deve conter ações de identificação e avaliação do risco, ações de prevenção e proteção dos riscos, monitoramento e testes dos riscos e reciclagem e revisão dos riscos. Segundo RAJAMÄKI, 2021, pg. 16 “a rede OT em fábricas de manufatura ou de processo e os conceitos de ICS podem ser resumidos como um sistema complexo grande ou enorme de automação – e redes, dispositivos, sensores, válvulas e motores em cima de um grande campo ou área.”

Deste modo, torna-se cada vez mais importante o uso de ferramentas de segurança cibernética como o SCADA, ICS ou DCS, políticas de segurança, melhores práticas, treinamentos aos funcionários com procedimentos e instruções claras em todos os ambientes para o aumento da segurança cibernética nas empresas (MITNICK, 2003), bem como “os componentes ou funcionalidades do ICS e a terminologia comum em alto nível pode ser divididos e descritos” (RAJAMÄKI, 2021, pg. 16) conforme o Quadro 3:

Quadro 3. Ferramentas de segurança cibernética, componentes e funcionalidades.

Ferramentas	Componentes e funcionalidades:
SCADA	Pode ser espalhado para áreas geográficas maiores de diferentes automações ou subestações de rede de energia de onde são operadas e controladas por exemplo.
DCS	É um sistema de automação em nível de planta para controlar diferentes processos de produção.
PLC	Pode ser uma parte menor do DCS para controlar processo em tempo real por meio de conexões de barramento de campo de E / S múltiplas.
SIS	Está detectando situações de insegurança no processo produtivo e de segurança de pessoal e meio ambiente. Integrações de sistemas de controle industrial ao Centro de Operação e Segurança de Tecnologia da Informação.

Fonte: RAJAMÄKI, 2021, pg. 16, organizado pelo autor.

Neste contexto, (AUTOMAÇÃO, 2021)

> "podemos listar algumas ações básicas que devem ser consideradas de imediato:
>
> - Autenticação de usuários e equipamentos
> - Controle de acesso - físico e lógico
> - Detecção de intrusão - física e lógica
> - Criptografia de dados
> - Assinatura digital
> - Isolamento e/ou segregação de ativos
> - Varredura de vírus
> - Monitoramento de atividade do sistema/rede
> - Segurança perimetral da planta,

também, define-se autenticação como (TECMUNDO, 2022) "o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira".

O controle de acesso físico (MAGIKEY, 2022) "é usado para gerenciar o fluxo de pessoas com o auxílio de funcionários, fechaduras, catracas e chaves" e também o controle de acesso físico (BLOG GESTÃO, 2022)

> "são medidas de segurança adotadas explorando se os meios físicos, organizacionais e tecnológicos, e utilizando-os como barreiras físicas de proteção a um perímetro de segurança previamente delimitado, a fim de controlar a administrar o acesso ao referido perímetro";

o controle de acesso lógico "usa a tecnologia para permitir acesso a locais ou sistemas" (MAGUKEY, 2022) e também este controle de acesso lógico (BLOG

GESTÃO, 2022) “é um conjunto de recursos executados para proteger o sistema, dados e programas contra tentativas de acessos de pessoas ou programas desconhecidos”.

O sistema de detecção de intrusão tem o objetivo de (FIBRE, PG. 57, 2022) “monitorar a rede ou o host e identificar comportamentos maliciosos – tipicamente ataques”.

A criptografia de dados (AVAST, 2022) “é o ato de codificar dados sigilosos e informações pessoais para protege-los contra o acesso de pessoas não autorizadas, como cibercriminosos”.

A assinatura digital (QUALI, 2022) “é uma tecnologia que utiliza a criptografia e vincula o certificado digital ao documento eletrônico que está sendo assinado”.

Na segregação de ativos (ADVISERA, 2022) “A ISO 27001 considera a segregação de funções um dos potenciais controles a serem aplicados para controlar a implementação e operação da segurança da informação dentro da organização”, sendo que “uma organização pode identificar os elementos mais vulneráveis e críticos a missão do negócio para os quais a segregação de funções representará valor agregado real ao negócio e a outras partes interessadas” (ADVISERA, 2022).

Do mesmo modo, a varredura de vírus é feita quando (GETTI, 2022) “o vírus tenha acesso ao sistema, o papel de um antivírus começa por meio de uma varredura que o detecta e evita que ele se espalhe ainda mais, excluindo-o ou isolando o arquivo que o contém”.

O monitoramento de atividade de rede é um software que (CISCO, 2022) “os administradores podem identificar deficiências de forma proativa, otimizar a eficiência e muito mais”, bem como esses sistemas de monitoramento de atividade de rede (CISCO, 2022)

> “incluem ferramentas de software e hardware que podem rastrear vários aspectos de uma rede e sua operação, como tráfego, utilização de largura de banda e período de atividade. Esses sistemas podem detectar dispositivos e outros elementos que compõem ou entram em contato com a rede, bem como fornecer atualizações de status”.

Por último, a segurança perimetral da planta (IRON, 2022) “é um método de proteção que utiliza barreiras perimetrais em torno do local de interesse” para evitar ataques hackers, sendo que (IRON, 2022) “a proteção perimetral é fundamentalmente importante para manter todo o local monitorado e bem estruturado contra invasões, roubos e inclusive desvios materiais”.

Essas considerações são reforçadas por (RAJAMÄKI, 2021, pg.19), no sentido de mostrar que, “os ambientes ICS dos processos da indústria é construído para digitalizar os status do processo e os valores são usados para monitorar e controlar o processo.”

Saliente-se ainda que, a deficiência em segurança cibernética poderá facilitar um ataque cibernético na empresa como a abertura de uma barragem, um blecaute elétrico, parar uma linha de produção, sistemas bancários e governamentais, enfim causar prejuízos para as empresas e para a sociedade. Além do mais, (RAJAMÄKI, 2021, pg.19) “o ativo protegido do ambiente OT são os controles de processo ICS e os altos riscos que estão relacionados às perdas de vida humana ou aos riscos ambientais por causa de fábrica da indústria danificada”.

Do mesmo modo, os negócios das empresas (IEC, 2021) “que tradicionalmente tratavam apenas do processo de engenharia de sistema agora devem incluir serviços e tecnologias de segurança cibernética”, e para mitigar os riscos pode-se utilizar os processos de gestão de identidade, gestão de acesso, gestão de ativos, gestão de patches, gestão de vulnerabilidades e gestão de segurança da informação, dados não estruturados, infraestrutura de redes e Telecom, infraestrutura física, firewall, acesso remoto, banco de dados, pentest e credenciais de acordo com as melhores práticas. Dessa forma, para (RAJAMÄKI, 2021, pg.19) “mesmo os riscos são diferentes no domínio de TI e OT, as ameaças de ataques podem ser as mesmas, especialmente com os sistemas industriais modernos, onde existem várias conexões entre o ICS e o ICT”.

Consequentemente, pode-se afirmar, conforme cita SMITH, 2016, que as “oito melhores práticas para projetar, construir e proteger sistemas de controle” descritas no Quadro 4, ajudam a mitigar os riscos cibernéticos em OT.

Quadro 4. Melhores práticas de segurança cibernética

1.	Conheça, limite e monitore o acesso ao sistema de controle.
2.	Implemente a segurança apropriada para cada nível do sistema de controle.
3.	Monitore continuamente o sistema de controle em todos os níveis.
4.	Tenha um plano de contingência.
5.	Corrigir, atualizar e manter.
6.	Não se esqueça da segurança física.
7.	Aprenda com os eventos.
8.	Esteja ciente de suas informações públicas.

Fonte: SMITH (2016), organizado pelo autor.

Uma das ferramentas que corrobora com a melhoria de infraestruturas de segurança cibernética é o CFS Framework Cybersecutity (NIST), esta pode “usar a estrutura para determinar o seu atual nível de segurança cibernética, definir metas que estão em sincronia com o seu ambiente de negócios e estabelecer um plano para melhorar ou manter a segurança”. (LIMA, 2018). Assim, (SOLARPLEX, 2022) “a estrutura do NIST CFS é uma orientação voluntária, baseada em padrões, diretrizes e práticas existentes para que as organizações gerenciem e reduzam melhor o risco de segurança cibernética”.

Além disso, (SOLARPLEX, 2022)

> “a estrutura combina uma série de abordagens para lidar com ameaças à segurança cibernética. Isso inclui:
> ▪ configuração de procedimentos
> ▪ treinamento
> ▪ definindo papéis
> ▪ auditoria
> ▪ monitoramento”.

Também, por meio da autenticação e autorização de usuários do sistema, (ARMIS, 2022) “a gestão de identidade e acessos reforça a segurança da informação da organização, ao evitar tentativas de fraude, comprometimento de identidade dos utilizadores e perda de dados confidenciais pertencentes a organização”.

As normas IEC 62443 “tem o objetivo de servir de ajuda para a operação segura de sistemas de automação industriais” (PHOENIX, 2021). Além disso, a norma “IEC 62443 series foi desenvolvido para proteger as redes de comunicação industrial

e os Sistemas de Controle e Automação Industrial (IACS) usando uma abordagem sistemática.” (WISEPLANT, 2021). Também, (IEC, 2021) “o Sistema IEC para Esquemas de Avaliação de Conformidade para equipamentos e Componentes Eletrotécnicos – testa e certifica a segurança cibernética no setor de automação industrial”.

Assim, a segurança cibernética em tecnologia de automação e tecnologia operacional devem ser mapeadas, planejadas e trabalhadas por meio de um plano de segurança cibernético com camadas de segurança, monitoramento e tratamento de invasões do espaço cibernético da empresa. No entanto, segundo MITNICK, 2003 pg. 207

> “à medida que os aperfeiçoamentos são feitos nas armas tecnológicas contra as quebras de segurança, a abordagem da engenharia social de usar as pessoas para acessar as informações da empresa ou penetrar na rede corporativa quase certamente serão mais frequentes e atraentes para os ladrões de informações”.

Além disso, as pessoas representam um enorme risco de vulnerabilidade para a organização porque elas podem ser manipuladas pelo engenheiro social e causar danos irreparáveis para a empresa. Também, recomenda-se (ANBIMA, 2021)

> “ações de prevenção e proteção – estabelecer um conjunto de medidas cujo objeto é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles”.

Conforme cita (GARTNER), “em 2025, os ciberataques terão ambientes de tecnologia operacional (OT) como arma para causar danos ou matar humanos com sucesso”. Dessa perspectiva, “em ambientes operacionais, os líderes de gerenciamento de segurança e risco devem se preocupar mais com os perigos do mundo real para os humanos e o meio ambiente, em vez do roubo de informações” (GARTNER, 2021).

Assim sendo, (Decreto nº 10.222)

> “a segurança cibernética é de extrema importância para o poder público e para as instituições privadas, entende-se como relevante a criação de um mecanismo de compartilhamento de informações sobre riscos cibernéticos, com o fim de contribuir para a identificação, o gerenciamento e a mitigação de riscos”.

Saliente-se ainda que, a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) descreve em seus princípios que “é possível avaliar como as ameaças podem explorar as vulnerabilidades e, com isso, determinar o nível de risco, sua probabilidade ou frequência de ocorrência e os possíveis impactos ou consequências”. (Decreto 10.566). Além disso, às medidas de avaliação das vulnerabilidades bem como a implementação de planos de segurança cibernética devem ser realizados e atualizados continuamente para ter uma efetividade nas infraestruturas. (Decreto 10.566).

4. CONCLUSÃO

No trabalho apresentado sobre a segurança cibernética em tecnologia de automação e operacional foi descrita algumas vulnerabilidades de segurança cibernética bem como algumas ações de prevenção e proteção para mitigar os riscos em segurança cibernética.

Nesse sentido, foi demonstrado que os ataques cibernéticos são definidos com a invasão a sistemas de controles, sistemas de automação, sistemas cyber-físicos e foram citados alguns ataques cibernéticos ocorridos no período de 2000 a 2019 com impactos no sistema IACS. Dentre esses ataques, destacamos o WannaCry que acessou os sistemas de automação industrial a partir de redes locais e VPN. Além disso, foi demonstrado também os ataques cibernéticos ocorridos no Brasil de janeiro de 2020 a fevereiro de 2021, o qual relaciona empresas do setor de energia elétrica, petróleo, gás e derivados, transportes e outras, ou seja, empresas essenciais para a o desenvolvimento do país.

Nesse contexto, foi exposto que a segurança cibernética deve combinar os programas e as pessoas (operadores), usar componentes e funcionalidades do ICS bem como utilizar os componentes e funcionalidades das ferramentas SCADA, DCS, PLC e SIS. Também foi listado algumas ações básicas que contribui para a mitigação do risco cibernético como detecção de intrusão – física e lógica, segurança perimetral da planta e outros.

Por meio da metodologia utilizada foi possível abordar diversas vulnerabilidades de segurança cibernética bem como abordar as boas práticas de segurança cibernética em automação e operacional e entender que algumas vulnerabilidades e algumas práticas de segurança em TI são as mesmas de TO.

Assim, foi demonstrado várias caracterizações de ataques cibernéticos e descritos que as empresas devem investir em métodos para proteger os ativos cibernéticos e permanecer resiliente diante de ameaças cibernéticas pois um ataque contra a organização industrial sempre tem o potencial de ser devastador, tanto em termos de interrupção da produção quanto prejuízos financeiros. Além disso, ataques em empresas de utilidade pública podem afetar sinais de celular, provocar apagão, explosões e inundações, causando impacto social, econômico, político, danos aos

processos industriais, danos a população e danos ao meio ambiente, ameaçando até a continuidade dos negócios e a segurança nacional.

Do mesmo modo, foi exposto a conscientização em segurança cibernética a qual aborda que a segurança cibernética deve conter ações de prevenção e proteção dos riscos, monitoramento e testes de riscos, reciclagem e revisão dos riscos, bem como fazer uso de ferramentas e ações básicas de segurança cibernética que contribuem para a mitigação dos riscos cibernéticos.

Levando-se em conta o que foi observado, entende-se que deve haver atitude preventiva, reativa, consultiva diante de ameaças cibernéticas, bem como desenvolver programas de treinamento em segurança cibernética para os trabalhadores e constante atualizações de treinamentos em face a sofisticação das ameaças cibernéticas e desenvolver uma cultura de segurança cibernética.

Por todos esses aspectos, a segurança cibernética em tecnologia de automação e operacional é de vital importância para as empresas, o meio ambiente, as pessoas, o governo e todos os envolvidos direta ou indiretamente que podem sofrer danos ou prejuízos em caso de um ataque cibernético bem sucedido.

REFERÊNCIAS

_Decreto Nº 10.222, de 05 de fevereiro de 2020 – Estratégia Nacional de Segurança Cibernética – E-Ciber. Disponível em: <_https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419> Acesso em: 14 out. 2021.

_Decreto Nº 10.569, de 09 de dezembro de 2020 - Estratégia Nacional de Segurança de Infraestruturas Críticas. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm> Acesso em: 14 out. 2021.

_**Lei Nº 13.709,** de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 23 mai. 2021.

ADVISERA. **Blog ISO 27001 e ISO 22301.** Disponível em: <https://advisera.com/27001academy/pt-br/blog/2016/11/23/segregacao-de-funcoes-em-seu-sgsi-de-acordo-com-a-iso-27001-a-6-1-2/> Acesso em: 11 fev. 2022.

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico:** elaboração de trabalhos na graduação / Maria Margarida de Andrade. 6. ed. - São Paulo: Atlas, 2003.

AQUARIUS/Software & Automação Industrial. **Introdução a Segurança Cibernética industrial.** Disponível em: <https://www.aquarius.com.br/blog/artigos/introducao-a-seguranca-cibernetica-industrial/> Acesso em: 02 ago. 2021.

A VOZ DA INDÚSTRIA. **Ameaças virtuais comuns em sistemas cyber-físicos da indústria digital.** Disponível em: <https://avozdaindustria.com.br/inovao/ataques-cibernticos-como-sua-indstria-pode-se-proteger> Acesso em: 03 ago. 2021.

ANBIMA. **Guia de Cibersegurança ANBIMA.** Edição :3 | 2021. Disponível em: <https://www.anbima.com.br/data/files/34/B3/04/8F/D96F971013C70F976B2BA2A8/Guia%20de%20Ciberseguranca%20ANBIMA.pdf> Acesso em: 03 ago. 2021.

ARMIS. **Descubra o poder da Gestão de Identidades e Acessos e a sua importância para a proteção de dispositivos, informação e a identidade dos colaboradores.** Disponível: <https://www.armisgroup.com/br/blogs/gestao-de-identidades-e-acessos/> Acesso em: 26 fev. 2022.

ARS TECHNICA. **Encontrado: malware "Crash Override" que desencadeou a queda de energia na Ucrânia.** Disponível em: <https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/> Acesso: 03 fev. 2022.

AUTOMAÇÃO Industrial: **A segurança de dados na Indústria 4.0**. Disponível em: <https://www.automacaoindustrial.info/seguranca-de-dados-na-industria-4-0> Acesso em: 23 mai. 2021.

AUTOMAÇÃO Industrial: **Pesquisa sugere que sistemas industriais no Brasil estão vulneráveis a ataques cibernéticos**. Disponível em: <https://www.automacaoindustrial.info/pesquisa-sugere-que-sistemas-industriais-no-brasil-estao-vulneraveis-a-ataques-ciberneticos/> Acesso em: 11 out. 2021.

AVAST. **Criptografia de dados: O que é?** Disponível em: <https://www.avast.com/pt-br/c-encryption#gref> Acesso em: 04 fev. 2022.

BLOG GESTÃO. **Segurança Física e Lógica da Informação: Diferença e Convergência.** Disponível em: <https://gestaodesegurancaprivada.com.br/seguranca-fisica-e-logica-nas-organizacoes/> Acesso em: 04 fev. 2022.

BRASIL Escola. **Engenharia Social: Compreendendo Ataques e a Importância da Conscientização.** Disponível em: <https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social-compreendendo-ataques-importancia-conscientizacao.htm> Acesso em: 26 mai. 2021.

CERVO, Amado Luiz. **Metodologia científica:** para uso dos estudantes universitários [por] Amado Luiz Cervo [e] Pedro Alcino Bervian. 3. ed. São Paulo: McGraw-Hill do Brasil, 1983.

CISCO. **O que é monitoramento de rede?** Disponível em: <https://www.cisco.com/c/pt_br/solutions/automation/what-is-network-monitoring.html#~perguntas-e-respostas> Acesso em: 11 fev. 2022.

CISO Advisor. **Ataques ao setor de petróleo e gás aumentam 38% no primeiro semestre.** Porcentagem de ameaças bloqueadas no setor de automação predial também avançou, de 38% para 39,9% no mesmo período. Disponível em: <https://www.cisoadvisor.com.br/ataques-ao-setor-de-petroleo-e-gas-aumentam-38-no-primeiro-semestre/> Acesso em: 11 out. 2021.

CLARANET. **O que é Cibersegurança?** Disponível em: <https://br.claranet.com/blog/tudo-sobre-ciberseguranca> Acesso em: 13 out. 2021.

CNU – Central de Notícias Uninter. **Brasil teve mais de 1,6 bilhão de ataques cibernéticos em três meses.** Disponível em: <https://www.uninter.com/noticias/brasil-teve-mais-de-16-bilhao-de-ataques-ciberneticos-em-tres-meses> Acesso em: 12 out. 2021.

CRUZ, Vilma Aparecida Gimenes da. **Metodologia da pesquisa científica:** sistemas V / Vilma Aparecida Gimenes da Cruz. São Paulo: Pearson Prentice Hall, 2010.

CYBERLAW. **Ataque cibernético à rede elétrica na Ucrânia (**2015**).** Disponível em: <https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)#cite_note-6> Acesso em: 03 fev. 2022.

CYBERSCOOP. **Investigador da Trisis diz que interrupção da planta saudita poderia ter sido evitada.** Disponível em: <https://www.cyberscoop.com/trisis-investigator-saudi-aramco-schneider-electric-s4x19/> Acesso em: 04 fev. 2022.

DRAGOS. **CRASHOVERRIDE: Reavaliando a Ucrânia de 2016 Evento de energia elétrica como um ataque focado em proteção.** Disponível em: <https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf> Acesso em: 03 fev. 2022.

E-ISAC. **Analise do Cyber Ataque a Rede Elétrica Ucraniana.** Disponível em: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf> Acesso em: 03 fev. 2022.

FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços / Aguinaldo Aragon Fernandes, Vladimir Ferraz de Abreu. – 3. Ed. – Rio de Janeiro: Brasport, 2012.

FIBRE. **Sistema de Prevenção de Intrusão baseado em SDN/OpenFlow.** Disponível em: <http://insert.ufba.br/wp-content/uploads/2018/07/2o_FIBRE_OpenCall_SDN-IPS-ItaloAdrianaLeobino.pdf> Acesso em: 04 fev. 2022.

GARCIA, Plinio Silva de. **A influência do ambiente organizacional na motivação para a prática de crimes cibernéticos**. Disponível em: <http://tede2.pucrs.br/tede2/bitstream/tede/6946/2/DIS_PLINIO_SILVA_DE_GARCIA_COMPLETO.pdf> Acesso em: 02 fev. 2022.

GARTNER. **O Gartner prevê que até 2025 os invasores cibernéticos terão ambientes de tecnologia operacional como armas para prejudicar ou matar humanos com sucesso**. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we> Acesso em: 01/10/2021.

GETTI. **Antivírus e firewall: entenda seus papéis na política de segurança.** Disponível em: <https://getti.net.br/2018/03/27/antivirus-e-firewall-entenda-seus-papeis-na-politica-de-seguranca/> Acesso em: 11 fev. 2022.

IEC – International Eletrotechnical Commission. **Segurança cibernética para automação industrial e sistemas de controle**. 24/06/20 – Equipe editorial. Disponível em: <https://www.iec.ch/blog/cyber-security-industrial-automation-and-control-systems> Acesso em: 10 set. 2021.

IEC – Loja Virtual. **Relatório de Tecnologia IEC Segurança Cibernética: 2019**. Diretrizes de segurança cibernética e resiliência para o ambiente operacional de energia inteligente. Disponível em: <https://webstore.iec.ch/publication/65943> Acesso em: 03 out. 2021.

INDUSTRIAL CYBERSECURITY PULSE. **Ataque retro: como o NotPetya acidentalmente derrubou a gigante global de remessas Maersk.** Disponível em: <https://www.industrialcybersecuritypulse.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/> Acesso em: 04 fev. 2022.

ISA GLOBAL CIBERSECURITY ALLIANCE. **Guia de início rápido: uma visão geral das normas ISA / IEC 62443.** Segurança da Automação Industrial e sistemas de controle. Disponível em: <https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf?utm_campaign=ISAGCA%20Communications&utm_medium=email&_hsmi=85876950&_hsenc=p2ANqtz-8NCaovJ-77_DowdQ7qY8b-nxPnzu5QgAQfGuVaNkd5QjzPc_5e_tJ28J9xmBuVbGFiqzQcO39nYRyHY9GAk4Fk8LHg&utm_content=85876950&utm_source=hs_automation> Acesso em: 10 out. 2021.

KASPERSKY daily. **Kaspersky agora protege uma das melhores cervejas do mundo**. Empresa fechou acordo com a Pilsner Urquell para proteger linhas de produção da maior cervejaria tcheca. Disponível em: <https://www.kaspersky.com.br/blog/kaspersky-b2b-ics-pilsner/10419/> Acesso em: 11 out. 2021.

LARGE. **Stuxnet Worm Ataque às instalações nucleares iranianas.** Disponível em: <http://large.stanford.edu/courses/2015/ph241/holloway1/> Acesso em: 02 fev. 2022.

LIMA, Cícero Augusto Fonseca de; Kuvada, Daniel Kendy; Martini, Eduardo Henrique; Melo, João Carlos Barbosa de; Paula, Weslei Leandro de. **Segurança Cibernética**. Pesquisa e Projeto (Curso de MBA em Auditoria Governamental da FAE Business School, Curitiba, 2018.

MAGIKEY. **Controle de acesso físico x controle de acesso lógico: diferença e aplicação.** <https://magikey.com.br/2017/02/controle-de-acesso-fisico-x-controle-de-acesso-logico-diferenca-e-aplicacao/> Acesso em: 04 fev. 2022.

MARCONI, Marina de Andrade. **Técnicas de pesquisa:** planejamento e execução de pesquisa, amostragem e técnicas de pesquisas, elaboração, análise e interpretação de dados / Marina de Andrade Marconi, Eva Lakatos. – 5. ed. – São Paulo: Atlas, 2002.

MITNICK, Kevin D., (1963). **A arte de enganar**/Kevin D. Mitnick; William L. Simon; tradução Kátia Aparecida Roque; revisão técnica Olavo José Anchieschi Gomes. São Paulo: Pearson Makron Books, 2003.

MIT – Massachusetts Institute of Tecnology – MIT News – **Protegendo nossa infraestrutura de energia contra ataques cibernéticos.** Os pesquisadores usam uma metodologia nova e holística para abordar as vulnerabilidades cibernéticas nos sistemas de energia atuais. Disponível em: <https://news.mit.edu/2019/protecting-our-energy-infrastructure-from-cyberattack-0604> Acesso em: 07 set. 2021.

MIT TECHNOLOGY REVIEW. **Triton é o malware mais assassino do mundo e está se espalhando.** Disponível em: <https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/> Acesso em: 04 fev. 2022.

MZ. Monitoramento de Mercado. **Ataques cibernéticos.** Janeiro de 2020 a Fevereiro de 2021. Disponível em: <https://api.mziq.com/mzfilemanager/v2/d/8136baea-90cc-46fc-9bc0-4a1f25f52a53/f7acc4b2-5ea0-cdc7-92f7-34c027c57808?origin=1> Acesso em: 12 out. 2021.

PAREKH, M., Waedt, K. & Tellabi, A., (2021). **Alinhando-se com a estrutura de segurança cibernética por meio da modelagem de segurança OT**. In: Reussner, R. H., Koziolek, A. & Heinrich, R. (Hrsg.), INFORMATIK 2020. Gesellschaft für Informatik, Bonn. (S. 311-319). Disponível em: <https://dl.gi.de/handle/20.500.12116/34736> Acesso em: 11 out. 2021.

PHOENIX CONTAT. **IEC 62443 – a norma para cibersegurança industrial** Disponível em: <https://www.phoenixcontact.com/online/portal/br?1dmy&urile=wcm:path:/brpt/web/main/solutions/subcategory_pages/Cyber_security_IEC62443/6e7d0141-b528-4ed1-be88-af7dc52fa62e> Acesso em: 18 set. 2021.

PLATTE RIVER NETWORKS. **Ser infectado por NotPetya: o que a Maersk aprendeu.** Disponível em: <https://platteriver.com/blog/being-infected-by-notpetya-what-maersk-learned/> Acesso em: 04 fev. 2022.

QUALI SIGN. **O que é assinatura digital?** Disponível em: < https://www.documentoeletronico.com.br/assinatura-digital> Acesso em: 04 fev. 2022.

RC&I - Revista Controle & Instrumentação. **Cibersegurança: crescente desafio na indústria.** Revista Controle & Instrumentação – Edição nº 239 – 2018. Disponível em: <http://www.controleinstrumentacao.com.br/arquivo/ed_239/cp_239.html> Acesso em: 11 out. 2021.

RADWARE. **“BrickertBot” resulta em negação de serviço permanente.** Disponível em: <https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/> Acesso em: 04 fev. 2022.

RAJAMÃKI, Ari. **Integrações de sistemas de controle industrial ao Centro de Operação de Operação de Tecnologia de Operação e Segurança de Tecnologia da Informação.** Disponível em: <https://www.theseus.fi/bitstream/handle/10024/502581/Thesis_Rajamaki_Ari.pdf?sequence=2> Acesso em: 12 out. 2021.

RECORDED FUTURE. **LockerGoga Ransomware interrompe as operações da Norwegian Aluminum Company.** Disponível em: <https://www.recordedfuture.com/lockergoga-ransomware-insight/> Acesso em: 04 fev. 2022.

RISIDATA. **Derramamento de esgoto de Maroochy Shire**. Disponível em: <https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill#:~:text=Description%3A,of%20Maroochydore%20in%20Queensland%2C%20Australia.> Acesso em: 02 fev. 2022.

RS DATA SECURITY. **Melhores Práticas de Segurança Cibernética.** Disponível em: <https://www.rsdatasecurity.com.br/post/melhores-pr%C3%A1ticas-de-seguran%C3%A7a-cibern%C3%A9tica> Acesso em: 24 jan. 2022.

RUIZ, João Álvaro, (1928). **Metodologia científica: guia para eficiência nos estudos.** São Paulo: Atlas, 1986.

SECURITYBRIEF. **Fabricante norueguês de alumínio é duramente atingido por ataque de ransomware LockerGoga.** Disponível em: <https://securitybrief.asia/story/norwegian-aluminium-manufacturer-hit-hard-by-lockergoga-ransomware-attack> Acesso em: 04 fev. 2022.

SECURITYWEEK. **Atacantes usando o Havex RAT contra sistemas de controle industrial**. Disponível em: <https://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems> Acesso em: 03 fev. 2022.

SENHASEGURA. **Os pilares da Segurança da Informação.** Disponível em: <https://senhasegura.com/pt-br/os-pilares-da-seguranca-da-informacao/> Acesso em: 31 jan. 2022.

SMITH, J., Pereyda, J. and Gammel, D. **Melhores práticas de segurança cibernética para criação de sistemas de controle resilientes.** Schweitzer Engineering Laboratories, Inc. Pullmann, WA USA. Disponível em: <https://cms-cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6700_CybersecurityBest_JS_20160401_Web3.pdf?v=20181015-211630> Acesso em: 12 out. 2021.

SOLARPLEX. **Estrutura de Segurança Cibernética do NIST.** Disponível em: <https://www.solarplex.com.br/noticias-e-cases/item/142-estrutura-de-seguranca-cibernetica-do-nist> Acesso em: 26 fev. 2022.

STWBRASIL. **Tudo o que você precisa saber sobre a iso 27000.** Disponível em: <https://www.stwbrasil.com/blog/tudo-sobre-a-iso-27000/> Acesso em: 31 jan. 2022.

TECHCRUNCH. **Gigante de fabricação de alumínio Norsk Hydro encerrada por ransomware.** Disponível em: <https://techcrunch.com/2019/03/19/norsk-hydro-ransomware/> Acesso em: 04 fev. 2022.

TECMUNDO. **O que é autenticação?** Disponível em: <https://www.tecmundo.com.br/seguranca/1971-o-que-e-autenticacao-.htm> Acesso em: 04 fev. 2022.

THESEUS. **Automação em segurança cibernética.** Disponível em: <https://www.theseus.fi/handle/10024/503899> Acesso em: 12 out. 2021.

TREND MICRO. **O HAVEX tem como alvo os Sistemas de Controle Industrial**. Disponível em: <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/139/havex-targets-industrial-control-systems> Acesso em: 03 fev. 2022.

TREND MICRO. **Malware BrickerBot emerge, bloqueia permanentemente dispositivos IoT.** Disponível em:

<https://www.trendmicro.com/vinfo/es/security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices> Acesso em: 04 fev. 2022.

VERVE. **O que é Stuxnet?** The game-changing malware that shocked the ICS/OT world is back in the news and still has lessons to share. Disponível em: <https://verveindustrial.com/resources/blog/what-is-stuxnet/#:~:text=Its%20objective%20was%20to%20stealthily,the%209%2C000%20centrifuges%20in%20Natanz.> Acesso em 02 fev. 2022.

WIKIPEDIA. **Stuxnet**. Disponível em: <https://en.wikipedia.org/wiki/Stuxnet> Acesso em: 02 fev. 2022.

WISEPLANT. **PADRÕES ISA/IEC-62443: A pedra angular da cibersegurança industrial** – Garantir sistemas de controle e automação industrial abrangentes. Disponível em: <https://wiseplant.com/pt/iec-62443-standards-a-cornerstone-of-industrial-cyber-security/> Acesso em: 18 set. 2021.