Apontamentos sobre Segurança Cibernética no Setor Elétrico

Davi Sehnem Castro
Lab. de Análise e Proteção de Sist. Elétricos (LAPES)
Universidade Federal de Santa Maria (UFSM)
Santa Maria, RS, Brasil
davi.sehnem@acad.ufsm.br

Luiz Fernando Freitas-Gutierres
Dpt. de Eletromecânica e Sist. de Potência (DESP)
Lab. de Análise e Proteção de Sist. Elétricos (LAPES)
Universidade Federal de Santa Maria (UFSM)
Santa Maria, RS, Brasil
luiz.gutierres@ufsm.br

***Resumo*—Sistemas elétricos de potência estão cada vez mais interligados e dependentes de dispositivos de monitoramento e proteção, interconectados por redes de comunicação e informação. Contudo, ao possibilitar novas formas de interação com o sistema, repercutem-se em novos riscos e desafios relacionados à segurança cibernética do setor elétrico. As consequências do aproveitamento de vulnerabilidades por atores mal-intencionados podem ser estimadas a partir da investigação de casos reais de ataques cibernéticos. Os incidentes abrangem desde roubos de informações até o colapso de uma rede de distribuição de energia elétrica na Ucrânia em 2015, deixando cerca de 220.000 consumidores sem abastecimento energético por horas. Dessa forma, este trabalho objetiva contextualizar o cenário atual de cibersegurança no setor elétrico. Métodos de ataque cibernético são discutidos, relacionando-os com ocorrências em sistemas elétricos ou com potenciais riscos. Por fim, metodologias que podem ser implementadas para evitar ou mitigar os efeitos desses ataques são apresentadas.**

***Index Terms*—Cibersegurança, segurança da informação, rede de comunicação, setor elétrico.**

I. Introdução

O Sistema Elétrico de Potência (SEP) é um elemento de infraestrutura essencial para o desenvolvimento de uma nação, abrangendo processos de geração, transmissão e distribuição de energia elétrica. Com a crescente demanda energética por parte das comunidades e a busca por maior confiabilidade em redes elétricas, SEPs transformaram-se de isolados para interligados, conectando países e, até mesmo, continentes. Além disso, a conexão de recursos energéticos distribuídos em SEPs é crescente, elevando complexidade, volatilidade e imprevisibilidade da rede elétrica [1]. Para lidar com isso, requer-se modernizar os equipamentos de monitoramento e proteção de forma a permitir um controle adequado do SEP, garantindo qualidade e confiabilidade no fornecimento de energia. Dentre outras formas, isso pode ser obtido por meio da digitalização de equipamentos, tornando-os cada vez mais interconectados e interdependentes, assim como permitindo a rápida troca de informações e tomada de decisão entre operadores. Em contrapartida, isso possibilitou formas de se interagir com a rede de dados e, por extensão, com os equipamentos conectados a esse sistema de informação, repercutindo em novos riscos e desafios relacionados à segurança cibernética de SEPs.

Este trabalho foi realizado com apoio do Fundo de Incentivo à Pesquisa (FIPE) da Universidade Federal de Santa Maria (UFSM): Edital UFSM-PRPGP 003/2022 (bolsa de iniciação científica e auxílio financeiro).

As dificuldades para evitar ciberataques em subestações é evidenciada ao analisar o padrão IEC 61850 [2], [3], no qual definem-se protocolos de comunicação para sistemas de automação em subestações. Em [4], definem-se, de maneira complementar, modelos de informação e serviços de comunicação utilizados por dispositivos eletrônicos inteligentes (do inglês, *Intelligent Electronic Devices* — IEDs). Nesse sentido, o *Generic Object Oriented Substation Event* (GOOSE) é um serviço de comunicação via mensagens que possibilita a rápida transmissão de sinais de estado e controle, assim como dados lógicos e analógicos por meio do protocolo *Ethernet* em redes de área local [4], [5]. Contudo, não há previsão de criptografia na troca de mensagens, já que atrasos afetarão a confiabilidade do sistema [6]. Mesmo com a publicação do padrão IEC 62351 em 2007 [7], estabelecendo requerimentos de segurança para protocolos de comunicação (como o GOOSE), um agente malicioso pode tomar vantagem de lacunas de segurança e alterar o fluxo de informações. A título de exemplo, um ataque cibernético pode resultar nas aberturas de disjuntores ou de chaves seccionadoras em subestações [8].

Como agravante do exposto anteriormente, existem eventos nos últimos anos nos quais sistemas elétricos foram comprometidos. Em 2015, ciberataques foram realizados contra dezenas de subestações no oeste da Ucrânia, deixando mais de 220.000 consumidores sem fornecimento de energia elétrica [9]. Em 2021, a *Delta-Montrose Electric Association* (DMEA), uma cooperativa distribuidora de energia elétrica do Estado norte-americano do Colorado, foi vítima de um ataque de *ransomware* [10] que eliminou de 20 a 25 anos de dados armazenados, afetou a plataforma de faturamento e obrigou a empresa a desligar 90% de sua rede interna de computadores [11]. Em 2022, mais um ataque foi direcionado ao sistema elétrico ucraniano. Nessa ocasião, foi impedido, mas teria o potencial de afetar mais de dois milhões de consumidores se obtivesse êxito [12].

Outra situação preocupante foi anunciada pela *Cybersecurity & Infrastructure Security Agency* (CISA) que, em 13 de abril de 2022, publicou um alerta sobre a possibilidade de que agentes capazes de ameaças persistentes avançadas

teriam condições de invadir múltiplos Sistemas de Controle Industriais (ICSs) e Sistemas de Supervisão e Aquisição de Dados (SCADA) [13]. Alinhado a isso, um relatório [14] encomendado pela Barracuda, uma companhia de segurança em nuvem, mostrou que, dentre aqueles que tomaram parte no estudo, 94% afirmam terem sido alvos de ataques com alvo em seus sistemas industriais de 2021 a 2022. Um registro temporal de incidentes cibernéticos significantes é mantido em [15].

Dessa forma, é imperativo desenvolver estratégias de segurança cibernética para dispositivos eletrônicos inteligentes constituintes do setor elétrico, sem prejudicar o tempo de resposta e a confiabilidade dos equipamentos, assegurando o fornecimento de energia elétrica. Este trabalho objetiva destacar apontamentos sobre segurança cibernética em SEPs. Para tanto, o trabalho está organizado da seguinte maneira: na Seção II, são apresentados alguns tipos de ataques cibernéticos que podem ser usados para debilitar sistemas elétricos, além de um incidente na rede de distribuição ucraniana ser detalhado. A Seção III retrata abordagens que podem ser implantadas para evitar e combater ataques cibernéticos. Por fim, há as seções de Conclusão e Referências Bibliográficas.

II. Métodos de Ataque Cibernético e Ocorrências em Sistemas Elétricos

A. Incidente na Rede de Distribuição Ucraniana

Um dos principais exemplos de ataques cibernéticos no setor elétrico ocorreu na rede de distribuição ucraniana em 2015, atingindo três distribuidoras de forma síncrona e desconectando cerca de trinta subestações [9]. Como ilustrado na Fig. 1, as etapas de um ataque com essa magnitude podem ser discriminadas conforme instrui relatório técnico do instituto americano *Escal Institute of Advanced Technologias* (SANS) [16]:

a) Inicialmente, há ações de reconhecimento e tentativas de infiltração. Em geral, busca-se identificar trabalhadores (administradores, técnicos, engenheiros ou profissionais de tecnologia da informação) com privilégios sob os controles das subestações e, em seguida, eles são expostos a ataques do tipo *spear phishing* [17], [18]. Baseada em Engenharia Social [17], [19], essa técnica consiste em entrar em contato com indivíduos ou instituições específicos por meio de e-mails, tomando vantagem das informações coletadas para aparentar ser um contato confiável. As mensagens eletrônicas almejam persuadir os alvos e disponibilizam arquivos anexados ou URLs nos quais *malwares* [17], [20] poderão infectar os computadores dos usuários.
b) Aproveitando vulnerabilidades de programas ou do sistema operacional, o *malware* permite o reconhecimento das redes de computadores ou, inclusive, de ICSs, a depender das possibilidades de acesso das máquinas infectadas. Além disso, informações importantes podem ser capturadas pelos cibercriminosos, viabilizando roubos de identidade ou fraudes contra os alvos.
c) Os cibercriminosos podem se apoderar de credenciais de acesso a sistemas, obtendo nomes de usuários e senhas. Nessa etapa, os pontos de acesso iniciais podem ser abandonados e outras estações de trabalho são invadidas, escalando privilégios [21] e elevando o potencial de dano.
d) Com privilégios de acesso, os invasores conseguem investigar a operação e, inclusive, interagir com dispositivos via ICSs ou SCADA.
e) Finalmente, os cibercriminosos podem executar comandos e alterar o funcionamento de dispositivos, bem como modificar configurações e *firmwares*.

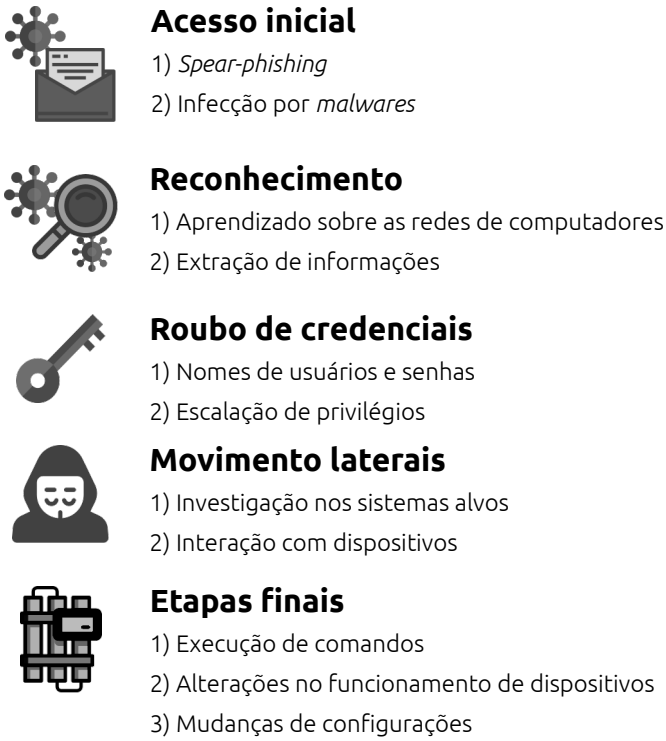

Figura 1. Etapas de um ataque cibernético em redes SCADA ou ICS.

No incidente na Ucrânia, e-mails contendo anexos com o *malware* intitulado *BlackEnergy3* [22] foram enviados para profissionais da tecnologia da informação e administradores de sistemas que trabalhavam para múltiplas empresas responsáveis pela distribuição de energia elétrica. O *malware* estabelecia um *backdoor* [23] nas máquinas quando a funcionalidade de macro de um editor de texto era habilitada pelos usuários para abrir os documentos anexados e infectados. Isso viabilizou acesso a redes corporativas das empresas. Mas, não havia acesso aos sistemas supervisórios, como o SCADA, pois estavam abrangidos por redes segregadas das redes corporativas por *firewalls*.

Houve um processo de reconhecimento das redes corporativas e, após meses, os atacantes obtiveram acesso a controladores de domínio. Com isso, obtiveram credenciais de trabalhadores e, com destaque, conseguiram dados para acesso remoto a redes privadas virtuais (do inglês, *Virtual Private Network* — VPN) utilizadas para autenticar a entrada nas redes SCADA. Com esses privilégios, os cibercriminosos substituíram *firmwares* de conversores industriais de série para

Ethernet de várias subestações com o intuito de evitar que operadores enviassem comandos remotos para fechamento de disjuntores. Mais do que isso, eles reconfiguraram fontes de alimentação ininterrupta (do inglês, *Uninterruptible Power Supply* — UPS) que garantiriam autonomia energética a centros de comando.

Após concretizar os procedimentos elencados acima, os atacantes executaram comandos para desabilitar as UPSs e para abrir disjuntores das subestações. Ademais, lançaram ataques de *Telephony Denial of Service* (TDoS) [24] contra centrais de atendimento que impossibilitaram relatos de falta de energia por parte dos consumidores. Por fim, utilizaram o *malware* chamado de *KillDisk* para excluir arquivos críticos dos centros de comando, tornando-os inoperáveis [9], [25].

No total, seis horas foram requeridas, aproximadamente, para reestabelecer o fornecimento de energia elétrica em todos os locais afetados. Entretanto, isso só foi possível ao se operar os equipamentos manualmente, por causa das substituições de *firmware* realizadas.

Durante a escalada do conflito entre Rússia e Ucrânia em 2022, várias reportagens e relatórios técnicos indicam novas ocorrências de tentativas e de ataques cibernéticos efetivos à rede de distribuição ucraniana. Alguns relatos sobre a "batalha digital" entre essas nações estão disponíveis em [26], [27].

B. Ataques de Negação de Serviço

Um ataque de negação de serviço (do inglês, *Denial of Service* — DoS) possui o objetivo de impedir que usuários, operadores e sistemas legítimos de um serviço obtenham acesso ao mesmo [17], [28]. Isso é conquistado por meio do envio excessivo de solicitações ou mensagens ao serviço que, por sua vez, acaba sobrecarregado e impedido de funcionar corretamente. Dessa forma, o serviço é negado a usuários legítimos.

Em [29], ataques são demonstrados via Telnet e protocolo de transferência de arquivos (do inglês, *File Transfer Protocol* — FTP). Como IEDs possuem, em geral, capacidades computacionais de processamento limitadas e permitem um número reduzido de conexões paralelas a um determinado serviço, um atacante pode abrir sessões e mantê-las ociosas. Outros tipos de ataques são explorados em [30], como o SYN-*flood* e o *buffer-overflow*. O primeiro, conhecido também como ataque de fragmentação, consiste em enviar uma série de requisições SYN (*synchronize*) a um sistema alvo na tentativa de consumir recursos computacionais suficientes de servidores. O servidor envia um SYN-ACK (*acknowledge*) e permanece no aguardo da resposta para confirmar a conexão. Mas, a resposta não é validada pelo usuário falso e o grande volume de solicitações provoca a indisponibilidade do serviço. O segundo, chamado de transbordamento de dados, ocorre quando um programa tenta gravar dados além do que o *buffer* de memória possibilita e isso sobrecarrega o sistema operacional. Cibercriminosos utilizam essa técnica de ataque ao executar códigos maliciosos em computadores com o intuito de controlá-los.

Uma outra técnica é o ataque de negação de serviço distribuído (do inglês, *Distributed Denial of Service* — DDoS). Ela diferencia-se de um DoS por utilizar múltiplas fontes (ou *botnet* [17] que corresponde a um conjunto de computadores ou sistemas infectados) para realizar as solicitações. Isso potencializa a capacidade do ataque, assim como dificulta a defesa [31].

C. Manipulação de Medidas por Injeção de Dados Falsos

Como estabelecido na Introdução, SEPs modernos são compostos por uma grande quantidade de unidades de monitoramento, as quais estão, constantemente, coletando dados, como tensões nos barramentos, correntes de linha, temperaturas, entre outros. Essas informações são enviadas para sistemas de controle que, a partir delas, podem estimar o estado do SEP, considerando ainda o processamento de erros. Todavia, é possível interferir na transmissão das medições e injetar dados falsos [32] que podem passar desapercebidos nas etapas de detecção de erros. Isso faz com que os sistemas de controle atuem com base em uma projeção incorreta do SEP. Esse tipo de ataque pode ser usado para danificar dispositivos e instalações conectadas a SEPs. Além disso, a manipulação de medidas é investigada com ênfase em ganhos financeiros em operações de tempo real no mercado de energia, como discutido em [33].

Como contraponto, salienta-se que executar os procedimentos demonstrados em [32] é, consideravelmente, complexo, exigindo conhecimento acerca das configurações e da topologia do SEP. Mais do que isso, requer-se, possivelmente, o acesso físico aos centros de controle e/ou aos medidores utilizados para a estimação de estado. Nota-se, porém, que investigações relatam a viabilidade de realizar esse tipo de ataque cibernético com uma quantidade cada vez mais limitada de recursos [34]. O leitor interessado nessa temática é referenciado para [35] em que se elaborou um compilado sobre as consequências potenciais da injeção de dados falsos no mercado de energia.

Ataques por injeção de dados falsos foram analisados também contra sistemas de transmissão em corrente contínua em alta tensão (do inglês, *High Voltage Direct-Current* — HVDC). Segundo [36], essa técnica de ataque cibernético pode ser empregada para corromper o controle de amortecimento de oscilações em SEPs com linhas de HVDC, existindo risco de perda de estabilidade. Nesse contexto, as manipulações provocam a verificação enganosa de diferença nas frequências mensuradas entre as unidades de retificação e inversão.

D. Riscos de Ataques Cibernéticos em Recursos Energéticos Descentralizados

A integração de recursos energéticos descentralizados em sistemas elétricos de distribuição demanda uso de inversores com funções e protocolos de comunicação cada vez mais avançados [37]. Entretanto, as eventuais vulnerabilidades constantes na rede de transmissão de dados de controle e monitoramento de unidades de Geração Distribuída (GD) são uma oportunidade para cibercriminosos corromperem esses sistemas. Como exposto em [38], o limite de despacho de potência ativa de uma GD é, geralmente, determinado pelo

operador por meio de um valor-alvo. Assim, há o risco de um cibercriminoso obter acesso ao sistema de controle para alterar essa configuração, criando problemas que podem impactar tanto a GD quanto o SEP ao qual ela está conectada.

Cabe destacar que o impacto ao SEP de ataques cibernéticos a GDs é proporcional à quantidade desses recursos energéticos descentralizados que estão sob o domínio dos atacantes. Contudo, conseguir acesso a diversas dessas unidades geradoras não é algo fora do imaginável. Como relatado em [39], uma empresa de energia solar promoveu uma atualização remota em mais de 800 mil inversores fotovoltaicos a partir de seus servidores. Isso impõe uma vulnerabilidade visto que atacantes podem tentar obter acesso a esse tipo de funcionalidade e atribuir configurações aos inversores fotovoltaicos de modo a provocar flutuações de tensão e problemas de estabilidade na rede de distribuição, podendo resultar, até mesmo, em blecautes.

E. Manipulação de Demanda por Controle de Equipamentos Inteligentes

Outra ameaça de cibersegurança está associada ao aumento do uso de eletrodomésticos e acessórios inteligentes conectados à rede. Esses equipamentos fazem parte da chamada Internet das Coisas (do inglês, *Internet of Things* — IoT) [40], a qual se caracteriza por dispositivos interconectados via Internet, com viabilidade de controle remoto por meio de aplicativos de celular, por exemplo. Contudo, esses aplicativos podem demonstrar vulnerabilidades que, por sua vez, podem ser aproveitadas por terceiros mal-intencionados para controlar os equipamentos.

Ares-condicionados, fornos elétricos e chuveiros elétricos, entre outros, caracterizam-se por demandar elevado consumo energético durante suas operações. Uma residência com um conjunto desses eletrodomésticos pode somar um consumo de alguns kilowatts de potência. Nesse sentido, o risco cibernético existe quando um agente malicioso possui controle de uma quantidade suficiente desses equipamentos (*botnets* [17]) em um aglomerado de unidades residenciais. Como demonstra a Fig. 2, a demanda exigida de alimentadores de redes de distribuição pode ser manipulada, substancialmente, ao ligar ou desligar um número adequado de equipamentos infectados.

Com base em análises de [41] sobre o sistema elétrico polonês em referência ao ano de 2008, um aumento de 1% na demanda que seria alcançado a partir do controle de 210.000 ares-condicionados, correspondente a uma invasão de 1,5% das residências polonesas, causaria um efeito cascata com uma estimativa de 263 falhas. Ainda que a probabilidade de ataques dessa natureza seja baixa na atual conjuntura, é preciso considerar que a tendência crescente de adoção de equipamentos de IoT pode atingir um ponto crítico que torne sistemas elétricos de distribuição suscetíveis.

Figura 2. Exemplo de um ataque cibernético por controle de equipamentos inteligentes e manipulação de demanda.

III. Métodos de Mitigação de Ataques Cibernéticos

Considerando as discussões anteriores, evidencia-se a importância de desenvolver e implementar protocolos e metodologias de segurança para evitar ou mitigar danos e prejuízos a sistemas elétricos. Entretanto, qualquer ação tomada com fim em aumentar a segurança da rede, não deve interferir na disponibilidade energética do SEP [1]. Além disso, todo procedimento de segurança cibernética efetuado deve ser projetado com base em estudo das características e vulnerabilidades do sistema, prezando pela distribuição homogênea de estratégias defensivas entre os diversos componentes que compõe a rede, já que o sistema será tão seguro a depender de suas parcelas mais vulneráveis.

Uma recomendação para implementar os métodos de mitigação de ataques cibernéticos é seguir o conceito de camadas de segurança (do inglês, *defense-in-depth*) [21], [42]. Como estabelece a Fig. 3, as camadas de segurança envolvem: segurança de dispositivos e aplicativos; segurança da rede; segurança física; e procedimentos e políticas de segurança.

Em [42], detalham-se ações que podem ser tomadas em cada camada de segurança. Na sequência, seguem observações sobre cada uma delas:

i. Procedimentos e políticas de segurança: É a camada mais externa da Fig. 3 e é composta por procedimentos e boas práticas que devem ser seguidas por funcionários e operadores. Elas envolvem, por exemplo, limitar o uso de aparelhos pessoais conectados à rede corporativa, bem

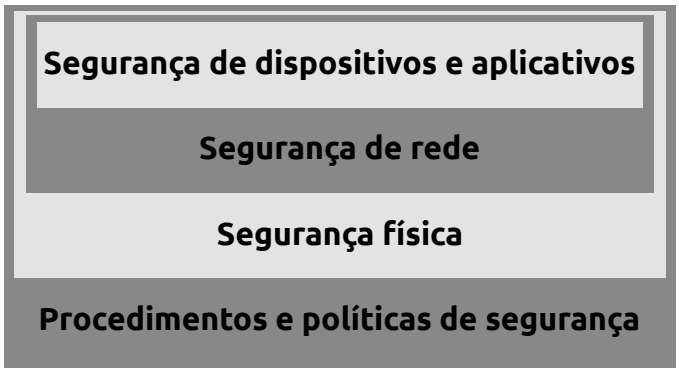

Figura 3. Camadas de segurança cibernética.

como alertar sobre formas de *spear phising* comumente utilizadas. Além disso, procedimentos de resposta para casos de detecção de incidentes devem ser delineados, reduzindo o tempo de reação e acelerando o reestabelecimento de sistemas em caso de desligamentos ou paradas forçadas.

ii. Segurança física: Os elementos físicos de segurança existem para evitar um acesso direto a locais, regiões ou dispositivos. Correspondem a cercas, bloqueios, travas, alarmes, câmeras de segurança, sensores de movimentos, entre outros. É uma das camadas de segurança com maior facilidade de ser implementada, sobretudo em locais com alta concentração de equipamentos críticos, como subestações.

iii. Segurança da rede: Uma das ferramentas mais eficazes para a proteção da rede é o seu seccionamento em diversas zonas [17], [21], definidas por funções ou áreas de interesse, e interconectadas através de *firewalls*. A segmentação da rede dificulta a movimentação lateral de um atacante, caso ele consiga se infiltrar em uma das redes isoladas, além de impedir que ele possa adquirir conhecimento sobre o sistema como um todo. Dentre as estratégias possíveis, a segmentação pode ser realizada a partir de *demilitarized zones* ou *software-defined networking*.

iv. Segurança de dispositivos e aplicativos: Dada a grande extensão de redes de energia elétrica, pode-se utilizar equipamentos que possuam *hardwares* e/ou *softwares* diversificados, impossibilitando que sejam comprometidos por um único tipo de ataque. Ademais, deve-se utilizar ferramentas de análise de *firmwares* antes que esses sejam atualizados, bem como garantir que todos os equipamentos sejam capazes de reverter as atualizações, caso falhas sejam, posteriormente, detectadas.

Outro importante conceito para a segurança cibernética de sistemas é o princípio do menor privilégio [17], [21]. Ele dita que nenhum usuário ou processo deve ter permissão para realizar ou acessar algo que vá além ao mínimo necessário para cumprir a sua função. Seguir esse conceito reduz o risco de acidentes, a difusão de *malwares* e limita as consequências do roubo de credenciais, já que elas permitem acesso limitado de acordo com hierarquia predefinida. Além disso, deve-se garantir que todos os pontos de acesso ao sistema requeiram *login* para serem utilizados, de preferência com autenticação de dois fatores e senhas seguras. Os sistemas devem ainda estar configurados para executar *logout* automático decorrido um determinado tempo.

IV. Conclusão

Este trabalho contextualizou o cenário atual de cibersegurança no setor elétrico. Para tanto, métodos de ataque cibernético foram discutidos, abrangendo ataques de negação de serviço, manipulação de medidas por injeção de dados falsos, riscos de ataques cibernéticos em recursos energéticos descentralizados e manipulação de demanda por ocntrole de equipamentos inteligentes. Além disso, o incidente na rede de distribuição ucraniana em 2015 foi discutido e as etapas desse ataque foram detalhadas. Por fim, alguns métodos de mitigação de ataques cibernéticos foram apresentados. Espera-se que os apontamentos elencados neste trabalho sirvam como apoio para a compreensão de fundamentos de cibersegurança aplicados ao setor elétrico, bem como para o desenvolvimento de uma visão geral sobre os riscos de ataques cibernéticos.

Referências

[1] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: challenges and opportunities," *Sensors*, vol. 21, no. 18, pp. 6225, Sep. 2021.

[2] R. E. Mackiewicz,"Overview of IEC 61850 and benefits," in *Proc. IEEE PES Power Systems Conference and Exposition*, Atlanta, GA, USA, 2006, pp. 623-630.

[3] H. Falk, *IEC 61850 demystified*. Boston, USA: Artech House, 2019.

[4] M. S. Thomas, and J. D. McDonald, *Power system SCADA and smart grids*. Boca Raton, USA: CRC Press, 2015.

[5] E. Padilla, *Substation automation systems: design and implementation*. Chichester, UK: John Wiley & Sons, 2016.

[6] V. S. Rajkumar, M. Tealane, A. Ştefanov, and P. Palensky, "Cyber attacks on protective relays in digital substations and impact analysis," in *Proc. 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, Sydney, Australia, 2020, pp. 1-6.

[7] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643-5654, Sept. 2020.

[8] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: a practical attack on cyber-infrastructure," in *Proc. IEEE Globecom Workshops*, Anaheim, CA, USA, 2012, pp. 1508-1513.

[9] Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Cyber-attack against ukrainian critical infrastructure," Feb. 25, 2016. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3psT1Sx.

[10] Cyber Security Coalition, *Cyber security incident management guide*. Brussels, Belgium: Cyber Security Coalition/Centre for Cyber Security Belgium, 2016.

[11] CISO Advisor, "Ataque a distribuidora de energia destrói 25 anos de dados," Dec. 6, 2021. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3T1c83v.

[12] IronNet Threat Research Team, and M. Demboski, "Industroyer2 malware targeting ukrainian energy company," Apr. 18, 2022. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3QEesfi.

[13] Cybersecurity and Infrastructure Security Agency (CISA), "APT cyber tools targeting ICS/SCADA devices," Apr. 13, 2022. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3wjiWzE.

[14] S. Sharma, "Barracuda report: almost everyone faced an industrial attack in the last year," July 12, 2022. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3bMJ8vx.

[15] Center for Strategic & International Studies (CSIS), "Significant cyber incidents," July 2022. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3A9Ua6r.

[16] M. J. Assante, and R. M. Lee, "The industriall control system cyber kill chain," Escal Institute of Advanced Technologies (SANS), Oct. 5, 2015. Acessed: Aug. 9, 2022. [Online]. Available: https://www.sans.org/white-papers/36297/.

[17] C. J. Brooks, C. Grow, P. Craig, and D. Short, *Cybersecurity essentials*. Indianapolis, USA: John Wiley & Sons-Sybex, 2018.

[18] M. S. Baig, F. Ahmed, and A. M. Memon, "Spear-phishing campaigns: link vulnerability leads to phishing attacks, spear-phishing electronic/UAV communication-scam targeted," in *Proc. 4th International Conference on Computing & Information Sciences (ICCIS)*, Karachi, Pakistan, 2021, pp. 1-6.

[19] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094-85115, 2020.

[20] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, "The world of malware: an overview,"in *Proc. IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain, 2018, pp. 420-427.

[21] J.-M. Flaus, *Cybersecurity of industrial systems*. Hoboken, USA: John Wiley & Sons-ISTE, 2019.

[22] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of Black Energy 3, Crashoverride, and Trisis, three malware approaches targeting operational technology systems," in *Proc. 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vienna, Austria, 2020, pp. 1537-1543.

[23] K. Thakur, and Al-S. K. Pathan, *Cybersecurity fundamentals: a real-world perspective*. Boca Raton, USA: CRC Press, 2020.

[24] Cybersecurity and Infrastructure Security Agency (CISA), "Cyber risks to 911: telephony denial of service,". Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3T37eTC.

[25] Wired, "Inside the cunning, unprecedented hack of Ukraine's power grid," Mar. 3, 2016. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3QG252m.

[26] Wired, "The race to rescue Ukraine's power grid from Russia," Mar. 18, 2022. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3wmE8Vx.

[27] Wired, "Ukraine's digital battle with Russia isn't going as expected,"Apr. 23, 2022. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3A9y43J.

[28] M. T. A. Rashid, S. Yussof, Y. Yussof, and R. Ismail, "A review of security attacks on IEC 61850 substation automation system network," in *Proc. 6th International Conference on Information Technology and Multimedia*, Putrajaya, Malaysia, 2014, pp. 5-10.

[29] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. Tan, "An intrusion detection system for IEC 61850 automated substations," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2376-2383, Oct. 2010.

[30] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM Based DoS attacks using data mining in smart grid," *Energies*, vol. 5, no. 10, pp. 4091–4109, Oct. 2012.

[31] S. Asri, B. Pranggono, "Impact of distributed denial-of-service attack on advanced metering infrastructure," *Wireless Pers Commun*, vol. 83, pp. 2211-2223, Aug. 2015.

[32] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1-33, May 2011.

[33] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659-666, Dec. 2011.

[34] D. Khezrimotlagh, J. Khazaei, and A. Asrari, "MILP modeling of targeted false load data injection cyberattacks to overflow transmission lines in smart grids," in *Proc. North American Power Symposium (NAPS)*, Wichita, KS, USA, 2019, pp. 1-7.

[35] M. A. Rahman, and G. K. Venayagamoorthy, "A survey on the effects of false data injection attack on energy market," in *Proc. Clemson University Power Systems Conference (PSC)*, Charleston, SC, USA, 2018, pp. 1-6.

[36] R. Fan, J. Lian, K. Kalsi, and M. Elizondo, "Impact of cyber attacks on high voltage DC transmission damping control," *Energies*, vol. 11, no. 5, pp. 1046, Apr. 2018.

[37] Y. Xue, M. Starke, J. Dong, M. Olama, T. Kuruganti, J. Taft, and M. Shankar, "On a future for smart inverters with integrated system functions," *Proc. 9th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Charlotte, NC, USA, 2018, pp. 1-8.

[38] R. S. de Carvalho, and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *Proc. Resilience Week (RWS)*, San Antonio, TX, USA, 2019, pp. 226-231.

[39] U.S. Government Accountability Office (GAO), "Electricity grid cybersecurity: DOE needs to ensure its plans fully address risks to distribution systems," Mar. 2021. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3dLe8Nh.

[40] I. Butun, Ed. *Industrial IoT: challenges, design principles, applications, and security*. Cham, Switzerland: Springer, 2020.

[41] S. Soltan, P. Mittal, H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Security Symposium*, Baltimore, MD, USA, 2018, pp. 15-32.

[42] S. Kunsman, and M. Braendle, "Cyber security for substation automation, protection and control systems," ABB. Acessed: Aug. 8, 2022. [Online]. Available: https://bit.ly/3QxqtDb.