Grupo de Estudo de Sistemas de Informação e Telecomunicação para Sistemas Elétricos-GTL

6 Ds em Segurança Cibernética: Uma análise dos conceitos para aplicação em infraestruturas críticas de sistemas elétricos de potência

NILSON TINASSI PERES(1); ANDRÉ LUIZ FRANCESCHETT(2); FÁBIO LEANDRO PEREIRA DE BARROS(2); USP(1);Siemens (2);

RESUMO

A motivação deste artigo são os ataques cibernéticos sofridos pelo setor elétrico. Esse trabalho explica o motivo pelo qual a abordagem dos 6 D's em segurança cibernética é apropriada. Finalmente, disserta-se sobre cada um dos conceitos: *Deter* (dissuadir), *Detect* (detectar), *Defend* (defender), *Deflect* (desviar), *Document*, (documentar) e *Delay* (atrasar). Além de definir os conceitos, destaca-se também o quão eficientes as ferramentas e/ou ações nestes baseadas podem ser. Para cada conceito uma tabela apresenta sua associação com os sistemas elétricos de potência, exemplificando a aplicação dessas ações/ferramentas. O texto é concluído com uma discussão acerca da eficiência dessa abordagem.

PALAVRAS-CHAVE

Segurança cibernética, Subestação, Sistemas elétricos, Plano de ação, Infraestrutura crítica.

1.0 - INTRODUÇÃO

Esse estudo inicia-se por definir brevemente a motivação dos esforços e recursos investidos em segurança cibernética em tempos recentes. Através de casos conhecidos na literatura, realiza-se uma jornada através de suas causas e consequências e como elas contribuíram para o progresso do estado da arte. Esses casos também atestam que a frequência, a proporção e o escopo dos ataques cibernéticos têm aumentado, fato que resulta em uma preocupação cada vez maior com a segurança dos sistemas de infraestrutura crítica, como o Sistema Elétrico de Potência (SEP).

O objetivo deste documento é analisar como podem ser aplicados 6 conceitos de segurança cibernética e projetar os resultados esperados para tais medidas de segurança. Essa discussão é de suma importância por permitir aplicar todos os conceitos abordados pelos 6 D's da segurança cibernética na criação de um plano estratégico de segurança cibernética através de uma abordagem holística que garanta mitigar drasticamente os riscos em infraestruturas críticas de sistemas elétricos [1].

Como resultado da aplicação desses conceitos no planejamento de um sistema de segurança cibernética, espera-se obter uma infraestrutura e arquitetura que desestimule ataques, detecte comportamentos suspeitos, defenda o sistema dos ataques, desvie os ataques das funções críticas de operação ou das informações confidenciais, documente todos os incidentes relevantes e que atrase o máximo todo e qualquer ataque que tente ser realizado ao sistema.

Cada um dos conceitos citados acima terá um capítulo único para discussão, tendo suas principais medidas e ferramentas brevemente explicados de maneira a contribuírem com um estado mínimo de segurança ao sistema. Pontos tais quais a relevância dessas medidas no setor elétrico, exemplos de aplicação e uma breve introdução da teoria por trás de cada conceito são abordados.

(*) Av. Dr. Renato de Toledo Porto, n° 83 – apto 12 – CEP 13.564-190 São Carlos, SP – Brasil
Tel: (+55 16) 99141-3544 – Email: nilson.peres@usp.br

A combinação dessas medidas aplicadas na infraestrutura crítica garante que os riscos sejam mitigados e permite concluir que a abordagem dos 6 D's em segurança cibernética é válida e aplicável no Sistema Elétrico de Potência, base deste estudo.

2.0 - CENÁRIO HISTÓRICO DOS RISCOS CIBERNÉTICOS NO SETOR DE INFRAESTRUTURA CRÍTICA

Esta seção se propõe a recapitular brevemente alguns ataques cibernéticos que aconteceram nos útimos anos, esses ataques introduzem e reforçam a necessidade de investimentos (tempo, recursos e mão de obra qualificada) em segurança cibernética voltada para sistemas de infraestrutura crítica, como o Sistema Interligado Nacional (SIN).

2.1 BlackEnergy, Ucrânia, 2015: Um ataque bem-conhecido

O BlackEnergy foi um ataque que utilizou um malware primeiramente identificado em meados de 2007 com objetivo de executar ataques DDOS (Distributed Denial of Service), porém alguns anos foram suficientes para que esse malware evoluísse e se tornasse uma ferramenta poderosa e perigosa [2].

Às vésperas do Natal de 2015, no dia 23 de dezembro, o BlackEnergy foi responsável por um apagão de 6 horas afetando cerca de 230 mil pessoas na Ucrânia após comprometer importantes centros de distribuição de energia.

Esse ataque cibernético se tornou um marco na história da segurança cibernética voltada para sistemas elétricos de potência, sendo o principal responsável por atrair as atenções das empresas, organizações e instituições parte do setor. Finalmente, o setor elétrico começou a investir tempo e recursos em análises, estudos, técnicas, ferramentas e infraestrutura de segurança.

2.2 Industroyer, Ucrânia, 2016: Perigo Reincidente

O ataque anterior não foi um incidente isolado. Após o apagão de 2015, quase um ano depois, em dezembro de 2016 um ataque similar ocorreu, novamente na Ucrânia. Premeditado e com altos níveis de privilégio, o ataque foi orquestrado por um grupo de criminosos com bastante conhecimento sobre infraestrutura de sistemas elétricos de potência. [3]

Esse ataque mostrou-se ainda mais preocupante para todos os órgãos e empresas envolvidas por se tratar de um ataque calculado e direcionado. Sendo executado através de um malware desenvolvido com características únicas do sistema elétrico, tais como a capacidade de fazer uso de protocolos de comunicação especifícos do setor (IEC 101, IEC 104, IEC 61850 e OPC DA). [4]

O setor elétrico, caracterizado por uma engenharia única e especializada e com protocolos exclusivos não estava blindado dos ataques cibernéticos. Pelo contrário, a reincidência através de um malware tão sofisticado e único reforçou que os sistemas elétricos de potência seriam a cada dia um alvo mais atraente para os criminosos, um alvo tão importante que esforços e recursos não seriam medidos para comprometer a operação desse setor de infraestrutura crítica.

2.3 GreyEnergy, Ucrânia e Polônia, 2016-2018: Discretamente Malicioso

Os ataques acima citados atraíram a atenção de inúmeros profissionais e empresas de segurança cibernética. Uma de suas principais descobertas se deu com o malware GreyEnergy. Esse software malicioso foi desenvolvido para operar sem causar danos ao sistema, projetado para ser executado discretamente e passar despercebido por todas as camadas de proteção. Nesse caso, os criminosos investiram seus esforços com outros objetivos e motivações: fazer reconhecimento, mapeamento e espionagem dentro do sistema, adquirindo informações de funcionamento e operação. Essas ações não causam danos nem falhas no setor elétrico e poderiam nunca ter sido descobertas, porém o aumento dos investimentos em segurança e infraestrutura revelou uma série de companhias de energia já infectadas pelo GreyEnergy por toda Ucrânia e Polônia.

Através de informações críticas de funcionamento e comportamento do sistema elétrico, os desenvolvedores do GreyEnergy seriam capazes de realizar um ataque ainda maior e mais prejudicial, afetando direta ou indiretamente todos os setores de infraestrutura crítica no país e dezenas de milhões de pessoas.

Esse malware é mais uma evidência de que os criminosos continuam à procura de vulnerabilidades e, ainda mais, continuam arquitetando seus ataques visando aumentar os danos e consequências por eles causados, reafirmando as preocupações concernentes a segurança cibernética em sistemas de infraestrutura crítica [5].

A figura 1 traz um resumo dos 3 ataques abordados para uma análise e comparação entre eles.

BlackEnergy	Industroyer	GreyEnergy
Local		
Ucrânia	Ucrânia	Ucrânia Polônia
Consequências		
- Tipo: Apagão - Alcance: 230 mil pessoas - Duração: 6 horas	- Tipo: Apagão - Alcance: ~2,5 millhões de pessoas - Duração: 1 hora	- Tipo: Espionagem - Alcance: Não se aplica - Duração: Não se aplica
Características		
- Spearphishing (email) usado para infecção, arquivos de Excel infectavam computadores através das macros - Roubo de senhas, screenshots, roubo de privilégios de acesso - Controle remoto e destruição de discos de armazenamento.	- Desenvolvido para afetar redes de energia, infiltrado na rede através da exploração de um relé de proteção - Usado como backdoor para expor o sistema a ataques - Foco em DJ e relés, com comunicação IEC 104, IEC 61850 e OPC DA (protocolos especificos)	- Spearphishing para infecção; Web Servers contaminados para disseminar na rede local - Uso de técnicas de espionagem - Uso de técnicas de camuflagem - Roubo de senhas, informações, screenshots, entre outros

FIGURA 1 - Comparação entre ataques BlackEnergy, Industroyer e GreyEnergy

2.4 Planos Estruturados de Ataque requerem Planos Estruturados de Segurança

Os casos destacados são ataques modernos e bem planejados que aplicaram um método militar chamado *Cyber Kill Chain* (Sequência de Destruição Cibernética), as partes desse plano estruturado de ataque podem ser observadas na figura 2.

Conhecidos os riscos envolvidos e casos históricos, determinar um plano similarmente bem estruturado com o objetivo de proteger contra essas ameaças através da intervenção por etapas constitui-se uma ótima abordagem para aplicação em sistemas de infraestrutura crítica tais como os sistemas elétricos de potência.

3.0 - CONCEITOS DE SEGURANÇA CIBERNÉTICA APLICADOS SOB DIFERENTES ABORDAGENS E PERSPECTIVAS

Conceitos são definidos filosoficamente como: “representações mentais que se mostram como instrumento fundamental do pensamento nas tarefas de identificar, descrever e classificar diferentes elementos e aspectos da realidade”.

O objeto, elemento ou aspecto da realidade em questão é a segurança cibernética. Dessa forma, podem existir inúmeras representações mentais que auxiliem a identificar, descrever e classificar as ideias aplicadas em segurança cibernética. Cada uma dessas representações mentais possui suas particularidades, vantagens e desvantagens.

Artigos da literatura [6] desenvolveram a proposta de subdivisão dos métodos, técnicas e ferramentas usados em aplicações de segurança cibernética em 6 grandes conceitos, sendo eles (conforme figura 3): Deter, Detectar, Defender, Defletir, Documentar e Atrasar (*delay*).

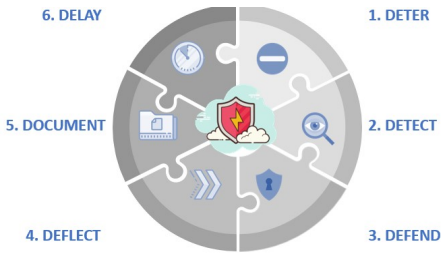

FIGURA 2 – 6 conceitos usados para definir um plano de segurança cibernética

A principal vantagem em agrupar métodos, técnicas e ferramentas em 6 grandes grupos (representados por cada conceito acima) se dá por fornecer uma abordagem sucinta que compreende as áreas da segurança cibernética através de uma descrição fácil de assimilar, resultando assim em uma abordagem didática para implementação, porém, ao mesmo tempo, completa.

A desvantagem existente diz respeito à possível perda de propriedade técnica no processo de subdivisão de uma área tão multidisciplinar (segurança cibernética) em apenas 6 grandes conceitos. Ainda assim, a abordagem dos 6 conceitos já foi estudada sob diferentes perspectivas pertecentes ao escopo de tecnologia da informação e mostrou-se eficiente.

Apesar de bem sucedida sob o escopo de tecnologia da informação, não existe nenhuma abordagem na literatura que utilize esses 6 conceitos para identificar, descrever e classificar os métodos, técnicas e ferramentas sob o escopo de tecnologia de operação e de informação para sistemas elétricos de potência. Assim, em vista dessa oportunidade, esse trabalho mostra sua característica inovativa por discutir e propor um plano de segurança cibernética voltado à subestações de energia sob a abordagem desses 6 conceitos.

4.0 - MEDIDAS PREVENTIVAS PARA DESESTIMULAR ATAQUES E PROTEGER SISTEMAS

"Impedir um sujeito de executar uma ação ou reduzir seu entusiasmo em atingir o objetivo por dificultar a execução da ação ou por ameaçar através de más consequências resultantes", [7] assim se define, em uma tradução livre do Cambridge Dictionary, a base do primeiro dos seis conceitos que serão abordados nesse artigo: *DETER* [*inglês*].

O sinônimo mais apropriado para *deter* é *dissuade*, que pode ser entendido como dissuadir. Um artigo de Denis Onuoha (*Chief Information Security Officer* na Arqiva) descreve a dissuasão como uma das formas de defesa mais eficientes do mundo cibernético [8] e ela é a primeira barreira contra o início de um ataque.

O início de todo ataque se dá quando o atacante (attacker), seja uma organização, grupo ou pessoa, define um alvo (target) e um objetivo (goal) (veja figura 4). O alvo do ataque pode ser uma pessoa ou organização e ter inúmeros objetivos tais como: roubo de informações, manipulação de dados, danos à infraestrutura de TI ou TO, vantagens financeiras, entre outros. Assumindo que o atacante têm seu alvo e objetivos conhecidos, têm-se então bem definidos os 3 parâmetros do processo de ataque.

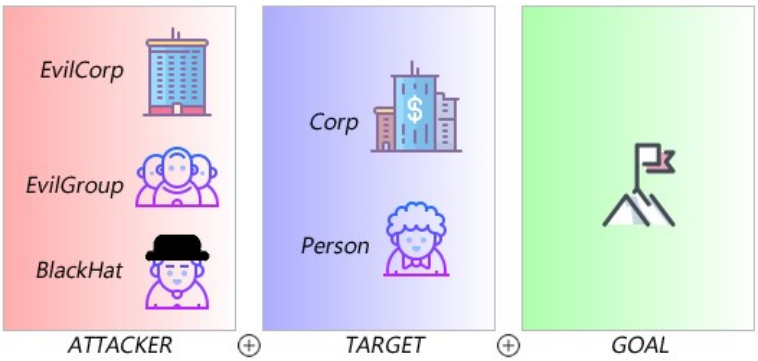

FIGURA 3 – As três variáveis iniciais que originam um ataque

A dissuasão (*deter*) consiste em utilizar tudo que for possível para desistimular o atacante, uma pesquisa do Instituto Ponemom apoiada pelo Palo Alto Networks constatou que cerca de 72% dos atacantes desistem quando a primeira barreira de defesa é bastante resistente e que fazer com que o atacante precise investir mais de 40 horas no ataque reduz em 60% as chances dele continuar em busca de seu objetivo [9]. De fato, a dissuasão é extremamente eficiente na prevenção de ataques, por isso, na sequência apresenta-se um exemplo de como dificultar um ataque.

Uma das tarefas iniciais de um ataque é o reconhecimento do alvo (*reconnaissance*), etapa na qual todas as informações podem ser relevantes e, quanto mais específicas, mais preciosas. Consiste em uma tentativa sistemática de localizar, agrupar, identificar, salvar e analisar todas as informações disponíveis sobre o alvo. Estudos estimam que a taxa de sucesso do ataque está diretamente ligada à quantidade de informações sobre o alvo às mãos do atacante.

Nenhum ataque será concretizado se o atacante não possuir informações críticas sobre seu alvo, visto que frações preciosas de informação são a base para o início de um ataque. Quando as técnicas de dissuasão são aplicadas, aumenta-se consideralvemente a dificuldade e complexidade do processo de reconhecimento a ser executado pelo atacante, atuando como um forte desistimulante frente motivação do ataque.

A tabela 1 a seguir sugere alguns métodos para desestimular ataques no setor elétrico.

TABELA 1 – Técnicas de Dissuasão em Sistemas Elétricos de Potência

Ação	Efeito	Exemplo SEP
1. Gestão de Senhas, Contas e Permissões	Controlar o acesso dos usuários e dos papéis e privilégios de cada um no sistema	Alterar as senhas *default* de todos os equipamentos do sistema (switches, roteadores, computadores, IEDs, servidores NTP), criando usuários de acordo com os papéis no sistema (operador, administrador, etc) e configurando seus privilégios.
2. Autenticação Multifator	Garantir o acesso apenas aos usuários permitidos	Exigir, quando permitido pelo software, a autenticação através de 2 fatores tais como cartão de identidade (*token*) e senha.
3. Criação de Políticas de Segurança	Assegurar que todos conheçam e apliquem medidas preventivas de	Alertar todos os colaboradores parte do processo quanto às medidas de segurança que devem ser seguidas tais como: usar senhas difíceis de serem quebradas por força-bruta, bloquear os

	segurança, reduzindo vulnerabilidades	computadores após uso, carregar junto de si o token de identificação, não expor informações confidenciais na internet, não acessar sites inseguros, entre outras.
4. Atualização Constante dos Softwares	Assegurar que nenhuma vulnerabilidade já corrigida torne o sistema exposto	Criar rotinas de atualização de todos os softwares e do sistema operacional, bem como dos firmwares de IEDs, roteadores e switches.
5. Utilizar Whitelisting (lista de softwares confiáveis)	Permissão de execução concedida apenas à uma lista de aplicações confiáveis configurada	Executar o mapeamento de softwares confiáveis nos computadores de natureza estática (sem constantes atualizações, como IHM's) após setup completo e "congelar" o sistema para não receber novos softwares.

5.0 - FERRAMENTAS E TÉCNICAS PARA ANÁLISE, DESCOBERTA E MONITORAMENTO DE AMEAÇAS

As ações de dissuasão citadas no capítulo anterior são importantes visto que contribuem para o desistimulo do atacante e também aumentam as chances de detecção do ataque, escopo dessa seção.

Detectar o ataque consiste em usar ferramentas de observação e monitoramento de sistemas e processos para verificar comportamentos não usuais (anomalias) que possam indicar tentativas de ataque ou presença de malwares, sendo parte essencial de um plano de ação que vise a segurança e a redução de danos de um sistema de infraestrutura crítica [8].

Quando um ataque está sendo executado cada fração de tempo possui sua importância particular, assim detectar tentativas de ataques com rapidez e precisão (baixa quantidade de falsos-positivos/alarmes-falsos) faz-se parte crucial do processo de redução de danos e proteção do sistema.

Se for detectada uma tentativa de ataque, quando o atacante está a procura de vulnerabilidades, o sistema entrará em estado de alerta e em modo de segurança crítica, elevando as permissões requisitadas e notificando os responsáveis pela segurança para estudo e análise de técnicas para garantia da segurança geral.

Se for detectado um ataque, quando o atacante já ultrapassou algumas barreiras de proteção por meio de vulnerabilidades, o sistema também entrará em modo de segurança crítica e estado de alerta notificando os responsáveis, porém agora as ações serão direcionadas para eliminar o acesso do atacante, encontrar as vulnerabilidades e corrigi-las, bem como proteger o sistema e/ou reduzir os danos sobre o mesmo.

Para aplicar os conceitos de detecção de ameaças e ataques faz-se necessário conhecer bem as ferramentas de análise, descoberta e monitoramento de ameaças. Algumas opções interessantes estão dispostas na tabela 2.

TABELA 2 – Ferramentas de Detecção em Sistemas Elétricos de Potência

Ação	Efeito	Exemplo SEP
6. Utilizar Blacklisting (lista de softwares não confiáveis).	Proteção contra ameaças e malwares conhecidos	Instalar softwares (antivírus) em todos os computadores parte do sistema e manter atualizadas as listas de ameaças.
7. Utilizar NGFW	Identificação de ameaças	Instalar e configurar o Next Generation Firewall para análise do tráfego de informações e protocolos em uso.
8. Monitoração com SIEM	Identificação de ameaças	Analisar tentativas falhas de acesso aos softwares do sistema elétrico, identificar possíveis ameaças através do comportamento de um usuário (tentativa de execução de uma tarefa fora de seu escopo de permissões).

6.0 - INSTRUÇÕES DE DEFESA CONTRA AMEAÇAS DENTRO DO SISTEMA

O ataque foi parcialmente bem sucedido, o atacante conseguiu acessar os sistemas através da exploração das vulnerabilidades. Porém, nem tudo está perdido, ainda há tempo para atuar e proteger o sistema.

Apesar de não terem identificado as tentativas de ataque, os softwares de detecção podem detectar o atacante dentro do sistema através da análise de anomalias e operações. Uma vez confirmado o ataque, é o momento de defender o sistema para impedir que os objetivos do atacante sejam atingidos.

Institutos de várias nações desenvolveram guias de instruções responsivas à ataques, sendo um dos mais respeitados deles o norteamericano National Institute of Standards and Technology (NIST) que publicou um guia de instruções para incidentes de segurança com cerca de 79 páginas nomeado Computer Security Incident Handler Guide [10]. Este guia é a recomendação deste paper como base para atuação da defesa na minimização dos anos e na recuperação do sistema.

Para exemplificar sua aplicação, na tabela 3 a seguir são sugeridas ações sobre o sistema elétrico de potência que podem ser úteis no procedimento de defesa.

TABELA 3 – Defesa em Sistemas Elétricos de Potência

Ação	Efeito	Exemplo SEP
9. Isolamento da ameaça	Impedir que se espalhe	Desconectar da rede o equipamento infectado (quando não prejudicar a operação) até que a ameaça seja neutralizada.
10. Restauração do sistema	Retomar as operações	Utilizar backups (recentes), para eliminar a ameaça do sistema e recuperar suas funcionalidades sem perdas.

7.0 - ESTRATÉGIAS E ARTIFÍCIOS USADOS PARA DESVIO DE ATAQUES E MINIMIZAÇÃO DE SEUS EFEITOS

Conforme discutido na seção 4 desse artigo, desistimular o atacante é ótimo, porém uma medida similar pode ser usada para impedir o sucesso de um ataque.

A deflexão (*deflect*) consiste em alterar ou desviar a trajetória natural de alguém ou de alguma coisa, assim esse princípio visa desviar o atacante de seus objetivos, impedir que ele alcance os danos desejados, atuando assim como medida eficiente de segurança do sistema e de minimização de danos.

Um artifício muito difundido é o uso de *honeypots* (potes de mel) [11] como *decoys* (armadilhas) [12] para manter os atacantes afastados de seções críticas do sistema atraindo-os para falsas seções deste e para conteúdos irrelevantes/incoerentes mascarados como informações críticas.

Através das medidas de proteção são criados 2 caminhos… O primeiro desses caminhos é menos seguro, a intenção é que se o atacante conseguir invadir o sistema, ele consiga atravessar as barreiras de proteção pelo caminho cuja proteção é menos robusta. O atacante não está ciente da existência de 2 caminhos, assim quando ele conseguir atravessar as barreiras através do caminho menos seguro ele pensará estar mais próximo seu objetivo. De fato, a cada barreira de proteção que o mesmo atravessar esse deve ser o sentimento. Finalmente, quando ele atravessar a última barreira de proteção, lá estará conforme suas expectativas o seu pote de mel (aquilo que ele procurava). Porém, o atacante acreditando que teve sucesso, na verdade teve acesso apenas ao que a segurança permitiu, nenhum dano foi causado, nenhuma informação relevante foi roubada ou perdida. O ataque fracassou.

Outros artifícios para desvio de ataques podem ser observados na tabela 4.

TABELA 4 – Deflecção de Ataques em Sistemas Elétricos de Potência

Ação	Efeito	Exemplo SEP
11. Pesquisa de Vulnerabilidade	Verificar se o sistema é um alvo de interesse para ataques	Verificar se buscadores de vulnerabilidades encontram equipamentos do sistema desprotegidos; Realizar varreduras de vulnerabilidades;
12. Honeypots	Identificar ataques, vulnerabilidades e desviar atenção das funções críticas	Utilizar propositalmente equipamentos desprotegidos (que não executem papel crítico na operação do sistema) para identificar atacantes e quantificar seu interesse em atacar o sistema (honeypots).

8.0 - PROCEDIMENTOS DE COLETA E ARMAZENAMENTO HISTÓRICO DE REGISTROS DE CONSEQUÊNCIAS E AÇÕES EM FUNÇÃO DE VULNERABILIDADES, AMEAÇAS E ATAQUES

Um dos procedimentos mais esquecidos e ignorados é o de documentação (*document*). Esse procedimento é, muitas vezes, tratado como repetitivo e desnecessário, porém deve ser visto como um dos pilares mais importantes na arquitetura de segurança cibernética implementada.

É através da documentação que são elaborados os planos de ação e de resposta a incidentes em casos de ataque, esses planos devem ser bem estruturados, organizados e didáticos, de forma a permitir fácil acesso e uso mediante situações de emergência [13].

A documentação também contém informações históricas e detalhadas sobre todas as tentativas de ataque, ameaças e ataques bem-sucedidos contra o sistema, junto com essas informações são descritos quais as ações e decisões que levaram à solução dos problemas e reestabelecimento da operação do sistema.

Ter essas informações em mãos permite uma rápida reação mediante incidentes e principalmente em casos reincidentes já tratados anteriormente. Também contribui para que os envolvidos tenham uma sequência clara de ações a serem executadas em situações emergenciais críticas, evitando decisões confusas ou guiadas por qualquer fator que não seja lógico e racional.

A tabela 5 a seguir lista algumas das informações que podem ser documentadas em caso de incidentes no sistema elétrico de potência.

TABELA 5 – Documentação para Segurança Cibernética em Sistemas Elétricos de Potência

Ação	Efeito	Exemplo SEP
13. Mapeamento dos ativos de software e hardware	Garantir segurança física e utilização de softwares atualizados	Criar planilhas que detalhem todos os softwares e firmwares identificados por suas versões e pela data da última atualização; Criar planilhas que detalhem a infraestrutura física e virtual, onde os equipamentos estão localizados, quais suas configurações de rede (endereço IP, gateway, etc), quais equipamentos comunicam entre si e quais protocolos são utilizados.
14. Logging	Registrar todas as informações geradas pelos sistemas	Configurar cada software (antivírus, ferramentas de engenharia, sistemas operacionais) e hardware (roteadores, switches e IEDs) para salvar seus registros (tentativas de acesso, atualizações, erros, alertas, ações, entre outros). Essas informações podem ser agrupadas e analisadas através de softwares como o SiEM (já apresentado).
15. Mapeamento de incidentes e ações	Permitir rápida reação em reincidências	Criar relatórios que descrevam todas os ataques detectados, quais vulnerabilidades eles exploraram, como essas vulnerabilidades foram corrigidas, como o ataque foi neutralizado, quais foram seus impactos no sistema, qual foi o comportamento do atacante, qual a duração do ataque, entre outras características que possam ser úteis para prevenção de futuros incidentes e para rápida reação.

9.0 - DEFESA EM PROFUNDIDADE, UMA ESTRATÉGIA PARA RETARDAR ATAQUES

Conforme mencionado anteriormente, o tempo necessário para que o atacante atinja o objetivo é determinante se ele continuará com a tentativa de ataque e também se o ataque será bem sucedido em passar furtivamente por todas as camadas de defesa. Cada instante de tempo a mais que o atacante leva para passar pelas camadas de proteção do sistema o deixa mais próximo de seu fracasso.

Assim, uma das técnicas mais comumente aplicadas para atrasar (*delay*) um atacante é a defesa em profundidade [14]. Essa consiste em uma abordagem que aplica vários mecanismos de defesa em série através de camadas para proteger o acesso a uma funcionalidade ou à informações críticas.

Um artigo [15] defende a aplicação da defesa em profundidade em sistemas elétricos de potência, na tabela 6 são comentados 3 exemplos:

TABELA 6 – Estratégias para retardo de ataques em Sistemas Elétricos de Potência

Ação	Efeito	Exemplo SEP
16. Criptografar protocolos de controle remoto	Segurança da comunicação entre as partes do sistema	Protocolos DNP 3.0 e IEC-104 podem ser criptografados para estabelecer comunicação segura entre partes como Centro de Controle Remoto e Operador Nacional do Sistema.
17. Segmentação de Rede	Garantir comunicação protegida entre os equipamentos da rede	Segmentar a rede através de zonas, utilizando uma zona DMZ (desmilitarizada) para a comunicação externa, impendido que a rede local possa ser acessada diretamente. Configurar corretamente o firewall para comunicação segura.
18. Redução da Superfície de Ataques (Hardening)	Redução das vulnerabilidades que podem ser exploradas	Desativar todas as portas/protocolos não utilizados e eliminar/desativar todos os sistemas e softwares que não são parte do processo, reduzindo as opções de exploração de equipamentos como IEDs e IHMs ou de qualquer outro equipamento parte da rede.

10.0 - CONCLUSÃO

A abordagem dos 6 D's em segurança cibernética permite uma ampla visão do escopo de atuação da segurança cibernética através do agrupamento de métodos, ações e ferramentas em 6 grandes grupos associados à conceitos de fácil memorização. Essa abordagem provê de forma simples e completa uma estratégia de implementação de um sistema de segurança eficiente e robusto.

A aplicação dos conceitos através de 18 ações no setor elétrico mostra-se possível e extremamente viável, sendo suficiente para mitigar drasticamente os riscos de ataque e os possíveis danos ao sistema elétrico de potência. O plano de ação sugerido é, em certo sentido, escalável e replicável. Ou seja, pode ser distribuído através do sistema

elétrico para seus inúmeros componentes com a mesma qualidade e eficiência, permitindo o estabelecimento de um padrão de proteção contra ataques cibernéticos.

Para validação, as alternativas apresentadas foram configuradas em uma bancada de testes de pequena escala na Siemens dotada de 1 computador de serviço para acesso remoto, 1 estação de trabalho (computador com ferramentas de engenharia e softwares de configuração de relés), 1 interface homem-máquina, 2 IEDs (relés de proteção), 1 switch, 1 roteador, 1 remota concentradora de dados e 1 servidor NTP, conforme figura 5. Através desses equipamentos a bancada simulava um subsistema de subestação de energia.

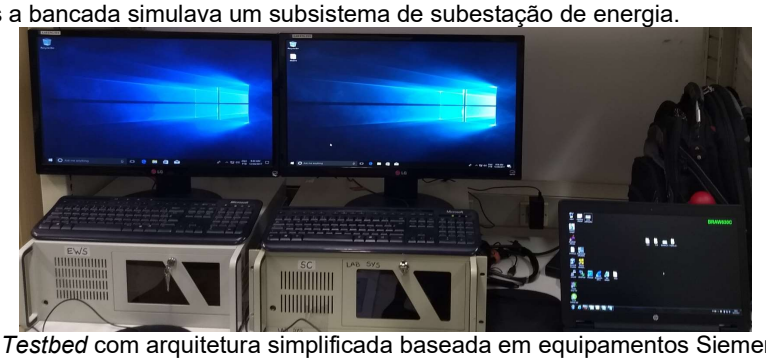

FIGURA 4 – *Testbed* com arquitetura simplificada baseada em equipamentos Siemens e terceiros

Por colocar em prática as 18 sugestões descritas nesse documento tais como segmentação de rede, uso de antivírus para blacklisting e aplicações de whitelisting, configuração correta de rotas, configuração de firewall, aplicação de conceitos de defesa em profundidade, configuração para monitoramento e registro, entre outras, foi possível obter uma arquitetura de subestação apropriadamente segura contra ataques cibernéticos. Assim, concluiu-se que os métodos estudados e aqui apresentados são eficientes e podem ser reproduzidos no ambiente de operação de sistemas elétricos de potência.

11.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) CUSIMANO, Joey. The 6 D's of Cyber Security (2015). InfoSec Institute. <resources.infosecinstitute.com/the-6-ds-of-cyber-security>. Acesso em: 09/10/2018.

(2) Ataques de APT BlackEnergy na Ucrânia. Kaspersky. <www.kaspersky.com.br/resource-center/threats/blackenergy>. Acesso em: 09/10/2018.

(3) Polityuk, Pavel. Ukraine's power outage was a cyberattack: Ukrenergo. <www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA>. Acesso em 12/10/2018.

(4) Osborne, Charlie. Industroyer: Behind Ukraine's power grid blackout. <www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout>. Acesso em: 12/10/2018.

(5) Cherepanov, Anton; GreyEnergy: Arsenal of one of the most dangerous threat actors. <www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/>. Acesso em: 18/10/2018.

(6) Ramirez, Vanessa. The 6 Ds of Tech Disruption. <singularityhub.com/2016/11/22/the-6-ds-of-tech-disruption-a-guide-to-the-digital-economy/>. Acesso em: 21/10/2018.

(7) Deter. Cambridge Dictionary. <dictionary.cambridge.org/dictionary/english/deter>. Acesso em: 25/10/2018.

(8) Onuoha, Denis. CYBER DEFENCE 2017: DETER, DETECT & DEFEND (2017).

(9) How to Deflect 70% of Cyber Attacks? (2016). Minerva Labs. <blog.minerva-labs.com/how-to-deflect-70-of-cyber-attacks>. Acesso em: 15/11/2018.

(10) Cichonski, Paul; Millar, Tom. Computer Security Incident Handling Guide (2012) Revision 2. NIST.

(11) Hoepers, Cristine; Steding-Jessen, Klaus. Honeypots e Honeynets: Definições e Aplicações (2007). CERT BR. <www.cert.br/docs/whitepapers/honeypots-honeynets/>. Acesso em: 15/11/2018.

(12) Kolton, Doron. Popular Decoys and Breadcrumbs for Deception Defense. Fidelis Cybersecurity. <www.fidelissecurity.com/threatgeek/deception/popular-decoys-and-breadcrumbs>. Acesso em: 15/11/2018.

(13) Example Cybersecurity & Privacy Documentation. Compliance Forge. <www.complianceforge.com/example-cybersecurity-documentation>. Acesso em 15/11/2018.

(14) What is Defense in Depth?. Forcepoint. <www.forcepoint.com/pt-br/cyber-edu/defense-depth>. Acesso em: 21/11/2018.

(15) Snyder, Joel. Six Strategies for Defense-in-Depth. OPUS.

12.0 - DADOS BIOGRÁFICOS

Nilson Tinassi Peres
Universidade de São Paulo [USP] – Engenharia Elétrica com ênfase em sistemas de energia e automação – 2019
Desenvolvedor Python (Ciência de Dados e Inteligência Artificial) [3P Tecnologia] – 2019
Estágio em Segurança Cibernética para Subestações de Energia [SIEMENS] – 2018

André Luis Franceschett
Universidade Estadual Paulista [UNESP] – Engenharia Elétrica – 2006
Pós-graduação em Redes de Computadores [UNICAMP] – 2009
Engenheiro Desenvolvimento de Sistemas Senior [SIEMENS] – 2010 ~ atualmente

Fábio Leandro Pereira de Barros
Faculdade Impacta Tecnologia – Tecnólogo em Redes de Computadores – 2019
Especialista de Engenharia [SIEMENS] – 2017 ~ atualmente