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

Avaliação da Segurança Cibernética em Instalações da Rede Básica da COPEL GET

PEDRO GUSTAVO SCHIER (*)
Copel GET

EDGAR LUCIANO IUBEL
Copel GET

ALEX SANDRO IVANKIO
Copel GET

RESUMO

A segurança cibernética em instalações de infraestrutura crítica não é um assunto novo, porém o nível de exigência dos órgãos reguladores e a maturidade das organizações brasileiras sobre o tema necessitam de evolução. A cada dia os dados referentes a ataques cibernéticos em infraestruturas críticas, fornecidos por organismos especializados em todo o mundo, só aumentam. Isso seria justificado pelo aumento da exposição, da interconexão e das possibilidades que a tecnologia atual permite, além da necessidade emergente de processos com maior integração e que, por consequência, requerem maior inteligência embarcada e automatismo. A proposta deste trabalho é utilizar ferramentas de avaliação de segurança Cibernética que estão alinhadas as melhores práticas e normas, para confirmação da real condição de exposição de subestações de energia da Rede Básica (RB-SE).

Atualmente os Estados Unidos seguem o padrão NERC-CIP (North American Reliability Corporation – Critical Infrastructure Protection), o qual recomenda a adequação das instalações do setor elétrico. De forma complementar, existem recomendações do NIST (National Institute of Standards and Technology) sobre políticas e procedimentos para segurança de aplicações computacionais utilizadas em meio industrial.

Com o objetivo de avaliar o nível de segurança cibernética implantada em uma instalação da rede básica da Copel Geração e Transmissão (Copel GET), optou-se em escolher a subestação Curitiba Norte que está localizada no município de Almirante Tamandaré - PR que possui ativos com tecnologias e topologias de rede mais avançadas dentre outras subestações. Utilizando as ferramentas CSET (*Cyber Security Evaluation Tool*) e C2M2 (*Cybersecurity Capability Maturity Model*) espera-se avaliar a capacidade da segurança cibernética atual e o nível de maturidade da organização com relação ao tema. Além do aprendizado na utilização destas ferramentas, pretende-se identificar as lacunas nos resultados fornecidos, propondo melhorias.

Serão realizadas intervenções na instalação visando desenvolver um trabalho de *Hardening* nos níveis de IED e Subestação, que consiste em mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, apresentando os resultados obtidos. Outras atividades previstas de serem executadas são: Camada IED (Intelligent Electronic Device) - Alteração de senhas default, níveis hierárquicos de acesso, desabilitação de funções não utilizadas; Camada Subestação - Controle de acesso na subestação, controle de acesso à rede Ethernet da subestação, implantação de firewalls através de migração para VPN, desabilitação de portas não utilizadas nos switches e terminais servers, configuração de MAC estático por porta, alteração de senhas default dos equipamentos, identificação visual de pontos da rede a serem segregados em caso de ataque.

Após a implantação das melhorias em campo será realizada uma nova avaliação através do CSET para verificar qual foi o percentual de evolução, considerando o SAL (*Security Assurance Level)* e CIA Levels (*Confidentialy, Integrity e Availability*), também será verificado através do C2M2 a evolução do MIL (*Maturity Indicator Level*), que deverá indicar um nível de maturidade para a segurança da instalação.

Com a aplicação das ferramentas e análise dos resultados, pretende-se definir um padrão mínimo de segurança

(*) Rua João Sigismundo Wysocki, s/n Orleans– CEP 82310-435 Curitiba, PR, – Brasil
Tel: (+55 41) 3331-2052 – Fax: (+55 41) 3331-3575 – Email: pedro.schier@copel.com

cibernética que deve ser implantado nas subestações, utilizando-se de base o piloto realizado na subestação Curitiba Norte. Serão elaborados procedimentos e políticas que preencham as lacunas identificadas, bem como espera-se fortalecer as melhores práticas já adotadas, contribuindo para a disponibilidade, integridade e confiabilidade das instalações da rede básica da Copel GET.

PALAVRAS-CHAVE

Segurança Cibernética, Tecnologia da Operação

1.0 - INTRODUÇÃO

A premissa do atual modelo do setor elétrico brasileiro, no qual ocorre o compartilhamento de instalações entre diversos agentes e um considerável fluxo de dados entre redes diversas, além da percepção de uma ausência de normas e procedimentos regulatórios que proporcionem a padronização de requisitos relacionados à Segurança Cibernética de instalações críticas, tornando estas tão vulneráveis, a ponto de comprometer a disponibilidade do Sistema Interligado Nacional.
Nesse cenário existem várias ferramentas, processos, padrões e diretrizes de gerenciamento de riscos em segurança cibernética já amplamente usados pelas organizações do setor de energia internacional que podem se alinhar com as necessidades nacionais.
A aplicação de uma avaliação utilizando o software CSET, permitirá conhecer o nível de maturidade com relação a segurança cibernética aplicado em instalações da rede básica da Copel, bem como propor ações para preencher possíveis lacunas com relação ao tema.

2.0 DESENVOLVIMENTO

2.1 Melhores Práticas

Após avaliar as recomendações dos principais fabricantes presentes nas subestações da Copel GET observa-se convergência nos seguintes pontos:

- Definir políticas, procedimentos e práticas de segurança;
- Proteger fisicamente todos os equipamentos, ou seja, garantir o acesso físico a computadores, equipamentos de rede, controladores, limitando o acesso apenas a pessoas autorizadas;
- Proteger os sistemas removendo ou desabilitando todas as conexões de rede e serviços, além de arquivos desnecessários, garantindo que todas as funções restantes tenham configurações de segurança apropriadas;
- Permitir que apenas usuários autorizados façam logon no sistema, impondo senhas fortes que sejam alteradas regularmente. Alterar as senhas “default” dos dispositivos para reduzir a possibilidade de acessos indevidos aos mesmos.
- Segregar a rede operativa da rede corporativa;
- Não permitir a instalação de nenhum software não autorizado no sistema;
- Utilizar antivírus configurado de acordo com as recomendações do fornecedor do sistema de automação;
- Restringir a conexão temporária de computadores portáteis, cartões de memória USB e outros portadores de dados.
- Se os computadores portáteis precisarem estar conectados, por exemplo, para fins de manutenção ou serviço, eles devem ser verificados quanto a vírus antes da conexão.
- Todos os dispositivos de dados removíveis, devem ser verificados quanto a existência de vírus, antes de serem introduzidos na zona confiável;
- Monitorar continuamente o sistema em busca de tentativas de invasão;
- Manter o sistema atualizado incluindo o sistema operacional, software do sistema de automação, aplicativos e programas;
- Definir e manter planos para resposta a incidentes, incluindo como recuperar-se de ocorrências;
- Segmentação de rede via DMZ (Demilitarized Zone);
- Uso de Firewalls Industriais para proteger as zonas de segurança da rede de automação;
- Criptografia de protocolos de controle remoto: o objetivo é realizar a criptografia de protocolos de comunicação utilizados para controle remoto da instalação crítica (subestação, unidade de geração de energia, etc.) de maneira a estabelecer uma comunicação segura com um Centro de Controle remoto do Operador Nacional do Sistema (O.N.S.).

- Aplicação do conceito de *Hardening* que consiste em aumentar a segurança de um sistema reduzindo as vulnerabilidades existentes, desabilitando serviços, alterando padrões de acesso e configurações de fábrica. Esse conceito se aplica a qualquer equipamento e/ou dispositivo conectado na rede da infraestrutura crítica;

Após avaliar as recomendações dos fabricantes podemos estabelecer o conceito de defesa em profundidade (*Defense In-Depth*) que se baseia na aplicação de diversas camadas de controles de segurança em um sistema. O conceito, amplamente utilizado em sistemas de Tecnologia da Informação, é totalmente adaptado a arquiteturas de rede de instalações críticas em sistemas de automação de energia. A defesa em camadas garante redundância de proteção caso ocorra falha em uma das camadas ou apresente alguma vulnerabilidade, que possa ser eventualmente explorada por ataques maliciosos para realizar acessos não autorizados a sistemas de automação de energia. Considerando uma defesa em camadas como mostra a figura 01, no caso de uma invasão direcionada para os equipamentos no pátio da subestação a segurança física é o único método de defesa, em linhas gerais podemos abordar as seguintes recomendações para as demais camadas:

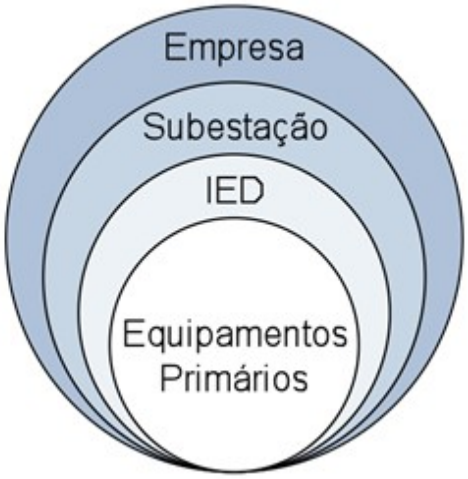


Figura 01 – Camadas

- Camada IED (*Intelligent Electronic Device*): Utilização de senhas, níveis hierárquicos de acesso, desativação de funções não utilizadas, monitoramento da rede;

- Camada Subestação: Controle de acesso interno e externo à rede Ethernet da subestação por firewalls, roteadores, desativação de portas não utilizadas nos switches, etc.;

- Camada Empresa: Políticas de segurança corporativas baseadas em firewalls, antivírus, controle de acesso centralizado.

2.2 Ferramenta de Avaliação

A ferramenta utilizada para avaliação do nível de segurança cibernético na instalação, foi o CSET (*Cyber Security Evaluation Tool*) versão 8.1, este software foi desenvolvido pelo Departamento de Segurança Interna dos Estados Unidos (*Homeland Security)* - departamento cuja responsabilidade é proteger o território dos EUA, contra ataques terroristas e agir em caso de desastres naturais.- e o Centro Nacional de Integração da Cibersegurança e Comunicações (NCCIC) que faz parte do Escritório de Segurança Cibernética.

A ferramenta utiliza informações fornecidas pelo usuário como:

- Setor de Atividade;

- Valores dos ativos a serem protegidos;
- Expectativa de tempo de preenchimento;

Após as informações iniciais preenchidas é possível elaborar o desenho da arquitetura de rede conforme a figura 02:

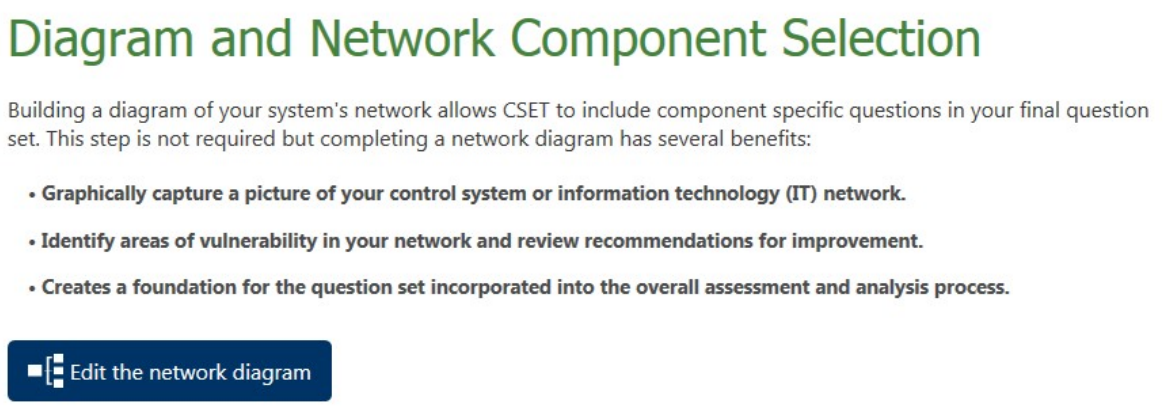


Figura 02 – Diagrama da arquitetura de rede

Os modos de seleção variam do básico (*key Questions*), cerca de 200 questões até o modo avançado que gera aproximadamente 4300 questões.

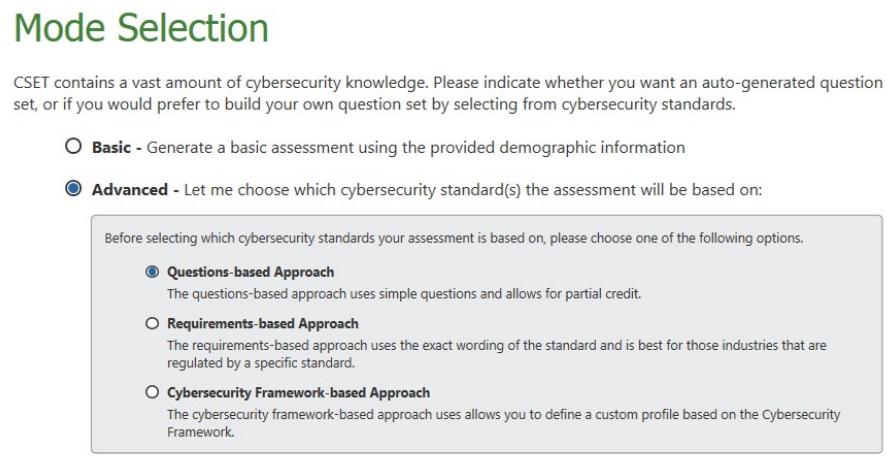


Figura 03 – Modos de Seleção

No modo avançado é possível estabelecer níveis de maturidade para o sistema a ser avaliado denominado de SAL (*Security Assurance Level*) que variam entre os níveis *Low, Moderate, High e Very High.* Para determinar o SAL é possível utilizar o CIA *Levels* (*Confindetiality, Integrity, Availability*), ou guias (*General SAL Guidance e FIPS 199 SAL Guidance*) com valores pré-estabelecidos definidos pelo tipo de atividade ou do impacto de sua indisponibilidade. Baseado nas atividades do processo o sistema sugere algumas normas e boas práticas a serem consideradas na avaliação conforme figura 04. Após a avaliação é possível gerar um relatório indicando as principais lacunas e oportunidades de melhoria.

Figura 04 – Normas e Publicações

2.2.1 Modelo de maturidade de capacidade de segurança cibernética

O Departamento de Energia dos EUA (DOE), como a agência específica do setor de energia, em parceria com os conselhos coordenadores dos subsetores de eletricidade e de petróleo e gás natural, juntamente com outras agências específicas do setor, desenvolveram um guia de Implantação de um framework especifico para proprietários e operadores do setor de energia. Ele é adaptado ao ambiente de riscos do setor de energia e às ferramentas e processos existentes para gerenciamento de segurança cibernética e de riscos que as organizações podem usar para implantação o framework. Este guia de implantação do framework é projetado para auxiliar as organizações do setor de energia a:

- Identificar seu nível de segurança cibernética atual e objetivo;
- Identificar lacunas existentes nos seus programas de gerenciamento de risco em segurança cibernética, usando o Framework para orientar e identificar áreas onde as práticas atuais podem exceder o Framework;
- Reconhecer que as ferramentas, padrões e diretrizes existentes do setor podem apoiar a implantação do Framework;

A ferramenta específica para auxiliar na implantação de um Framework é o Cybersecurity Capability Maturity Model – C2M2 (Modelo de Capacidades e Maturidade para Defesa Cibernética em tradução livre) desenvolvido pelo DOE e pela indústria. Cada domínio do C2M2 inclui quatro níveis de indicador de maturidade (MILs): MIL0 (Não Realizado), MIL1 (Iniciado), MIL2 (Realizado) e MIL3 (Gerenciado). As organizações avançam progressivamente no nível de maturidade, melhorando: a integridade, a perfeição ou o nível de desenvolvimento das práticas em um dado domínio. As organizações obtêm uma MIL quando realizam os objetivos e práticas de segurança cibernética específicos do domínio e as atividades de gerenciamento dessa MIL. As organizações podem estabelecer uma meta de MIL para cada domínio para orientar sua melhoria na segurança cibernética

2.3 Aplicação da Avaliação

Com o objetivo de avaliar o nível de segurança cibernética implantada em uma instalação da rede básica da Copel Geração e Transmissão (Copel GET), optou-se em escolher a subestação Curitiba Norte (SE CTN) que está localizada no município de Almirante Tamandaré-PR e que possui ativos com tecnologias e topologias de rede mais avançadas dentre outras subestações.

Para essa avaliação foram definidos 4 cenários:

- Cenário 01: Avaliação no modo básico para verificar a situação atual do nível de segurança cibernético da Subestação (SE);
- Cenário 02: Avaliação no modo básico após intervenção na SE aplicando as principais recomendações dos fabricantes;
- Cenário 03: Avaliação no modo básico após a implementação teórica do plano de ação do GT Cyber;
- Cenário 04: Avaliação no modo avançado considerando como referência o C2M2 (*Cybersecurity Capability Maturity Model*) no nível de maturidade MIL 1

2.3.1 Cenário 01

Para realizar a avaliação do nível de segurança cibernética, foram preenchidas as informações relativas ao Setor, valor de ativos a serem protegidos e o tempo estimado de preenchimento do relatório.

Após a etapa inicial foi desenhada a arquitetura de rede resumida da SE, indicando os principais equipamentos utilizados e conexões realizadas e foi selecionado o modo básico de preenchimento que gerou cerca de 200 questões alinhadas as melhores práticas e normas internacionais, por

As questões no modo básico de preenchimento abordam os seguintes requisitos:

Controle de Acesso, gerenciamento de contas, auditoria e responsabilização, proteção de comunicação, gerenciamento de configurações, continuidade dos processos, resposta a Incidentes, proteção de Informações, monitoramento e malware, organizacional, pessoal, segurança física, planos, políticas e procedimentos gerais, portátil, móvel, sem fio, controle de acesso remoto, gestão e avaliação de riscos, aquisição de sistemas e serviços, integridade do sistema, proteção do sistema e treinamento.

2.3.2 Cenário 02

O segundo cenário avaliado considerou a implantação de algumas das melhores práticas apresentadas no item 2.1.
No período de 10/09/2018 a 21/09/218 foi executada a programação na SE CTN com perda de supervisão para os níveis superiores COS-D, COGT e ONS.

Nessa programação foram realizadas as seguintes atividades:

- Migração da rede de automação da VPN42 (Rede de Automação da Transmissão e Distribuição) para a VPN409 (Rede de Automação dedicada Transmissão). Para essa migração foi contratado através da engenharia de proteção e automação o serviço de firewall (camada 4) da Telecom;
- Habilitação e configuração nos switches gerenciáveis do Agente SNMP (*Simple Network Management Protocol*) visando realizar o monitoramento da rede através destes ativos;
- Desabilitação de portas que não estão sendo usadas nos switches;
- Aplicação de *Whitelist* de MAC address na configuração dos switches;
- Alteração de senhas default dos switches;
- Reconfiguração do GPS, visando disponibilizar o sinal NTP na nova rede operativa denominada VPN409;
- Reconfiguração das máquinas virtuais adequando-as a nova rede operativa;
- Elaboração do rascunho para o novo procedimento de inclusão e manutenção de ativos na rede operativa de automação;

2.3.3 Cenário 03

Para a realização do cenário 03 considerou-se o cumprimento do plano de ação elaborado pelo grupo de cibersegurança da Copel GET que foi instituído em 22/11/2016 pelo documento corporativo “Aviso GET 033/2016” e tem o objetivo de criar, implantar e verificar a adequação dos procedimentos associados à Segurança da Informação das redes operativas, no âmbito da COPEL GeT. Este plano de ação foi baseado na norma NBR ISO/IEC 27002 que apresenta um conjunto completo de práticas e controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.

O plano de ação do grupo aborda questões relativas a:

- Reuniões Semanais, projetos de P&D, levantamento de necessidades de Notebook dedicados, criação de políticas de segurança, gestão de ativos de TO, antivírus aplicado na rede de automação, procedimentos de backup, plano de recuperação, recursos de TO, uso de portas USB, uso de pastas da rede operativa, gerencia de senhas, desenvolver e adquirir software, ambientes virtualizados, redes, responsabilidade, contato com entidades externas, gestão de recursos humanos, treinamentos, integração de terceiros, gerência de acesso físico, rastreabilidade, banco de dados, firewall, isolamento de estação contaminada, operação de infraestrutura, aquisição de equipamentos, acessos Remotos, autenticação/autorização, gerenciamento de rede, ambientes virtualizados, sistemas da automação, sistemas operacionais, desenvolver e adquirir software, gerência de software, aquisição de equipamentos, gerência de senhas.

2.3.4 Cenário 04

Avaliação no modo avançado considerando como referência o C2M2 (*Cybersecurity Capability Maturity Model*)

O C2M2 (*Cybersecurity Capability Maturity Model*) está sendo considerado na avaliação pois a ABRATE (Associação Brasileira das Transmissoras de Energia) está realizando uma força tarefa desenvolvendo um framework para auxiliar os agentes na verificação da capacidade da segurança cibernética de uma organização, priorizando suas ações e investimentos para melhorar sua segurança cibernética baseado no C2M2.

2.4 Avaliação de Resultados

Após a aplicação da avaliação nos 04 cenários determinados verificou-se os seguintes resultados:

2.4.1 Cenário 01: Avaliação no modo básico para verificar a situação atual do nível de segurança cibernético da Subestação (SE).
A média de atendimento aos requisitos básicos estabelecidos pelas questões padrões, foi de 44%. Como não existe um padrão mínimo, pode-se afirmar apenas que 65% das questões relacionadas a padrões e 45% das questões relacionadas a equipamentos não foram atendidas. Sendo que a categoria referente ao gerenciamento de contas demonstrou um desempenho inferior as demais.

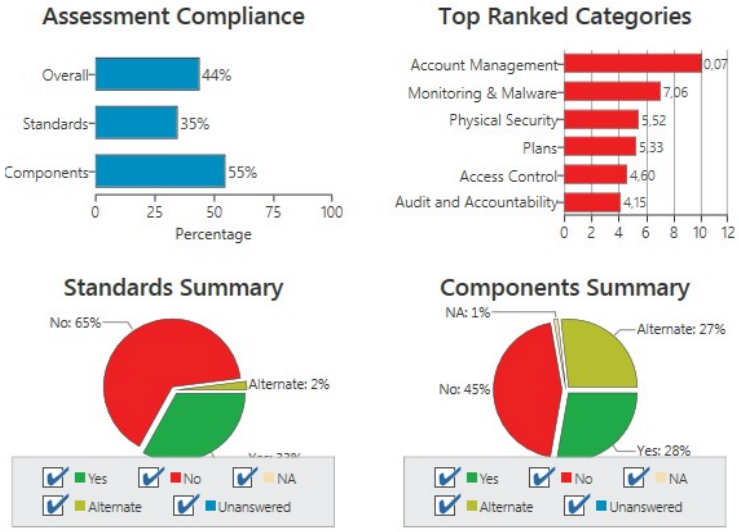


Figura 05 –Avaliação Cenário 01

2.4.2 Cenário 02: Avaliação no modo básico após intervenção na SE, aplicação das principais recomendações dos fabricantes
A média de atendimento aos requisitos básicos, estabelecidos pelas questões padrões, foi de 51%. Sendo que 59% das questões relacionadas a padrões e 32% das questões relacionadas a equipamentos não foram atendidas, porém comparando ao resultado do cenário 01, percebe-se uma evolução devido as ações executadas citadas no item 6.3.2.

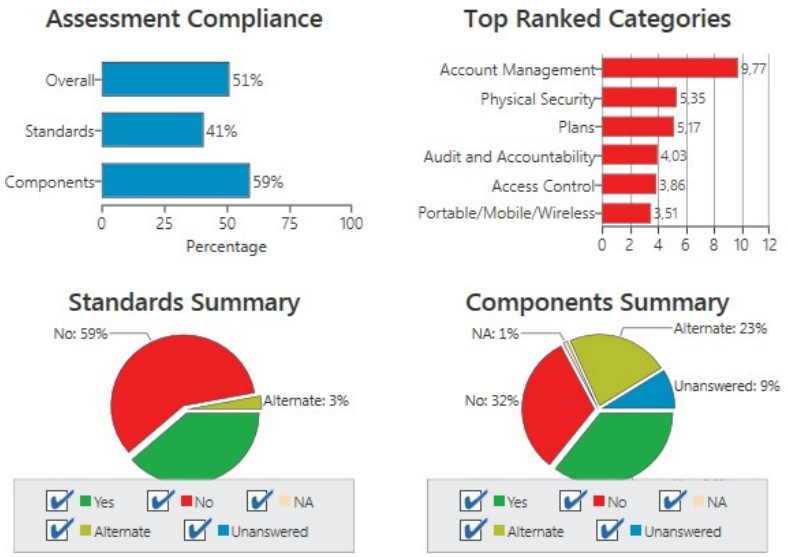


Figura 06 –Avaliação Cenário 02

2.4.3 Cenário 03: Avaliação no modo básico após a implementação teórica do plano de ação do GT Cyber

A média de atendimento aos requisitos básicos estabelecidos pelas questões padrões, foi de 73%, houve uma melhora significativa comparando com os cenários 01 e 02, devido ao fato de as questões serem respondidas, considerando hipoteticamente que todas as ações estabelecidas no plano de ação do GT Cibersegurança da Copel GET, estão concluídas.

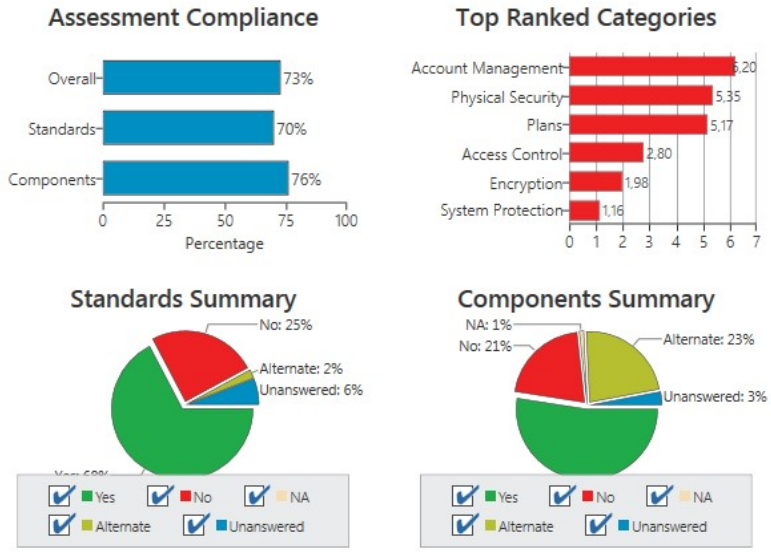


Figura 07 –Avaliação Cenário 03

2.4.4 Cenário 04: Avaliação no modo avançado considerando como referência o C2M2 (*Cybersecurity Capability Maturity Model*)

Um total de 52 questões compõem a avaliação considerando o modelo do C2M2. Considerando as questões padrões (*Key Questions*), foram respondidas 210 questões.

A média de atendimento aos requisitos básicos estabelecidos pelas questões padrões e C2M2, foi de 76%, houve um aumento comparado ao cenário 03, devido as 52 questões do C2M2 estarem no nível de maturidade MIL1 (Iniciado), ou seja, praticamente 100% dos itens estão atendidos se o plano de ação estiver implementado

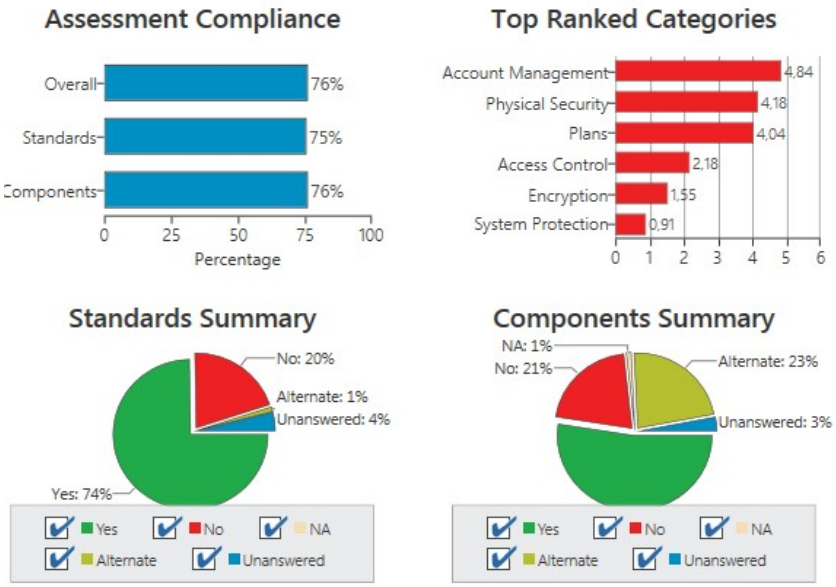


Figura 08 - Avaliação Cenário 04

2.5 – Procedimentos e Instruções Técnicas

Durante a realização das atividades em campo, percebeu-se a necessidade da criação de procedimentos para auxiliar na configuração dos equipamentos, considerando os requisitos de segurança da informação. Para atendê-los foi sugerido ao GT Procedimentos de Proteção e Automação a criação do:

- PM-AUT-013 Configuração e implementação de equipamentos para a rede operativa de automação;

Onde estão presentes algumas boas práticas apresentadas neste trabalho como:
- Alteração de senhas padrões dos equipamentos;
- Desabilitar todas as portas não utilizadas do switch;
- Aplicação de filtro de endereços MAC (*Media Access Control*);
- Habilitação do Agente SNMP;
Percebeu-se a necessidade de criação de Instruções Técnicas (IT´s) para a configuração de equipamentos *multivendor* presentes nos ativos da Copel Get, este tema será abordado nas próximas reuniões do GT Procedimentos de Proteção e Automação.

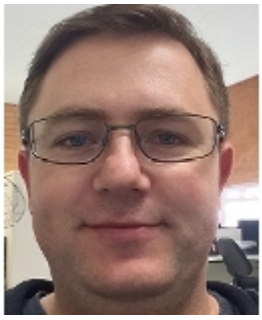
3.0 CONCLUSÕES

Uma autoavaliação com o CSET mostrou-se eficaz para quantificar em números como está a segurança cibernética de uma instalação da rede básica e como ficará após implementações em andamento, porém essa avaliação não pode revelar todos os tipos de deficiências de segurança e não deve ser o único meio de determinar a postura de segurança de uma organização. É recomendável que as avaliações do CSET sejam realizadas, por uma equipe multidisciplinar composta por representantes das áreas operacionais, de manutenção, tecnologia da informação, negócios e segurança da empresa. Na implementação de algumas das melhores práticas em campo, por exemplo, na criação da *Whitelist* de *mac address* para as portas de comunicação nos switches gerenciáveis, provavelmente devido ao RSTP (Rapid Spanning Tree Protocol) ocorreu um fluxo de *mac address* variável, o que causou a impossibilidade da ativação dessa funcionalidade, o problema está sendo estudado junto ao fabricante. Tal situação reforça a necessidade de constante aprimoramento do conhecimento e formação do corpo de técnico para atuação nas especificações e configurações destes equipamentos.

4.0 REFERÊNCIAS BIBLIOGRÁFICAS

(1) PORTAL O SETOR ELÉTRICO, Disponível em: osetoreletrico.com.br/desafios-da-seguranca-cibernetica-nas-subestacoes-de-energia-eletrica.
(2) C2M2 Cybersecurity Capability Maturity Model, Disponível em: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.
(3) White Paper ABB Security for Industrial Automation and Control Systems.
(4) SIEMENS e TI SAFE, *Como a Defesa em Profundidade Pode Aumentar a Segurança Cibernética em Instalações Críticas*, Paulo Antunes Souza Marcelo, Branquinho Andreas Kiefer .

5.0 DADOS BIOGRÁFICOS



Pedro Gustavo Schier nasceu em Curitiba, Paraná em 1981. Formado pelo Instituto Politécnico Estadual como Técnico em Eletrotécnica em 1999, graduou-se em 2007 como Tecnólogo em Automação Industrial pela Universidade Tecnológica Federal do Paraná e Engenharia Elétrica no ano de 2012 pela Universidade Tuiuti do Paraná, concluiu em 2015 a Pós Graduação Latu Sensu em Engenharia de Manutenção pela Pontifícia Universidade Católica do Paraná PUC-PR. Atua desde 2009 nas redes operativas de automação de subestações de transmissão pela Copel Geração e Transmissão participando em projetos de P&D ANEEL com integração de equipamentos de monitoramento, controle e proteção além de participar do Grupo de Segurança Cibernética da Copel GET.

Edgar Luciano Iubel nasceu em Curitiba, Paraná em 1969. Formado pelo Instituto Politécnico Estadual como Técnico em Eletrotécnica em 1987. Ingressou na Copel em 1989 e trabalhou em oficinas de recuperação de equipamentos da Distribuição e da Transmissão e na manutenção de Subestações da Transmissão. Desde 1999, atua na área de Proteção e Automação, onde participou da modernização tecnológica de diversas Subestações da Copel. Técnico Especializado em Manutenção de Subestações, atualmente está na área de Automação do Sistema em Comissionamento, Obras, Manutenção Corretiva e integração das Subestações da GET com os Centros de Operação da Copel e ONS . Participou do projeto P&D ANEEL de integração dos equipamentos de monitoramento, controle e proteção de Transformadores na parceria Copel e USP.

Alex Sandro Ivankio nasceu em Curitiba, Paraná em 1980. Formado pela Universidade Tecnológica do Paraná como Técnico em Eletrotécnica em 2000, graduou-se em Engenharia Elétrica no ano de 2011 pela Universidade Tuiuti do Paraná. concluiu em 2018 a Pós Graduação Latu Sensu em Automação Industrial pela Universidade Tecnológica do Paraná UTFPR. Atua desde 2005 na proteção e automação de subestações de transmissão pela Copel Geração e Transmissão.