RISCOS CIBERNÉTICOS EM SUBESTAÇÕES DO SISTEMA ELÉTRICO DE POTÊNCIA (SEP): UMA REVISÃO DE LITERATURA

CYBERNETIC RISKS IN SUBSTATIONS OF THE ELECTRICAL POWER SYSTEM (EPS): A LITERATURE REVIEW

[1]Diego Aquino Gomes
[2]Oberdan Rocha Pinheiro

RESUMO

Atualmente, os ataques cibernéticos são motivo de grande preocupação, sobretudo para instituições, bancos e governos. No entanto, os sistemas de geração e distribuição de energia também estão sendo um dos principais alvos desses ataques. Por esse motivo, o artigo tem como principal objetivo apresentar os riscos da segurança da informação às redes de automação de subestação, assim como, as soluções atualmente encontradas para redução das vulnerabilidades aos ataques cibernéticos. A metodologia utilizada foi a revisão de literatura, que teve como característica selecionar, identificar e avaliar criticamente os estudos considerados relevantes sobre a questão já formulada.

Palavras – Chave: Segurança Cibernética, Sistema Elétrico de Potência, Segurança em Sistema Elétrico, Infra-estrutura Crítica, Controle de Acesso.

ABSTRACT

Currently, the Cyber Attacks are reason of major concern, especially for institutions, banks and governments. However, the generation system and energy distribution are also being one of the main targets of these attacks. For this reason, the main objective of this article is show the risks of information security to substation automation networks, as well as the solutions currently found to reduce vulnerabilities to cyber attacks. The methodology used was the literature review, which had how characteristic to select, identify and critically evaluate the studies considered relevant on the question already formulated.

Keywords: Cyber Security, Electrical Power System, Security in Electrical System, Critical Infrastructure, Access control.

[1] Acadêmico do curso de Pós-Graduação em Automação em Sistemas Elétricos de Potência pelo SENAI CIMATEC.
[2] Coordenador do curso de Pós-Graduação em Automação em Sistemas Elétricos de Potência pelo SENAI CIMATEC e Professor orientador.

1. INTRODUÇÃO

O consumo de energia elétrica é um importante parâmetro adotado para indicar o desenvolvimento socioeconômico de um Estado, servindo de subsídio para refletir os avanços nos setores industriais, comerciais e de serviços. Sendo a eletricidade imprescindível para o aumento das taxas de crescimento de um país, nas ultimas décadas, empresas oriundas do setor elétrico começaram a investir na sofisticação de seus equipamentos no intuito de assegurar a qualidade da energia comercializada e tornar sua disponibilidade mais eficiente.

> Os recursos tecnológicos voltados para os sistemas de energia elétrica vêm evoluindo significativamente nas últimas décadas, propondo soluções inteligentes para o atual modelo, tanto no campo da automação, gerenciamento do consumo de energia e dos sistemas de comunicação, principalmente para as distribuidoras de energia elétrica e seus clientes (ABOBOREIRA e CRUZ, 2016).

Esses novos modelos de redes elétricas denominam-se de *Smart Grids*, também conhecidos como Redes Inteligentes. A elas atribuem-se a junção dos equipamentos elétricos microprocessados e a tecnologia voltada à área de telecomunicação, tendo como objetivo o processamento dos dados coletados em postos automatizados. Segundo Cernev (2015), os novos recursos aplicados aos equipamentos elétricos, como por exemplo, acesso a portas de comunicação via *Ethernet* e aceitação de múltiplos protocolos de rede, contribui para a interconectividade do sistema elétrico que conhecemos hoje.

Os avanços tecnológicos no setor elétrico facilitam de maneira significativa a sua automatização e a conectividade entre as áreas de geração, transmissão e distribuição de energia que compõe o Sistema Elétrico de Potência – SEP. A entronização de canais de comunicação aberta, como a *Ethernet*, contribuiu para o surgimento de um novo conceito de segurança no ramo da eletricidade: a Segurança Cibernética.

> Essa nova infraestrutura pode aumentar significativamente a eficiência e confiabilidade da rede de distribuição de energia, mas também pode criar muitas vulnerabilidades caso não seja concebida com os controles de segurança apropriados (HEINISCH et al., 2011).

Segundo Oliveira e Abboud (2013), na década de 90 não existiam preocupações com a segurança cibernética, pois os processos de

automatização das subestações ocorriam de forma isolada e sem conexão com as redes externas, os protocolos de comunicação eram privados e o tráfego de dados entre os dispositivos davam-se por meio de canais seriais. Somando-se as possibilidades de falhas dos equipamentos e as intempéries naturais que o SEP fica exposto, com a modernização dos dispositivos elétricos e a popularização da *internet*, a confiabilidade conferida à matriz energética passará pela capacidade que o sistema tem de se proteger contra cyber-ataques.

De acordo com o artigo de Oliveira e Abboud (2013):

> Em 2011, a empresa McAfee publicou um relatório intitulado de "Global Energy Cyber Attacks: Night Dragon" que alertava para diversas tentativas de ataques a empresas de energia elétrica, gás e óleo utilizando ferramentas de administração remota.

A tendência por ataques cibernéticos em empresas voltadas ao setor energético justifica-se por elas estarem inseridas no conceito de Infraestruturas Críticas, ou seja, "instalações, bens, e ativos que possuem serviços que, se interrompidos, provocam sérios impactos sociais, econômicos e políticos" (BRANQUINHO et al., 2014).

Em 2010 um ciberataque atrasou em dois anos o programa nuclear iraniano. Um vírus de computador denominado *Stuxnet* foi elaborado com a finalidade de causar danos físicos nas plantas de enriquecimento de urânio do Irã. No ano de 2013, o Governo brasileiro sofreu uma invasão cibernética promovida pelos Estados Unidos, no qual dados de setores estratégicos do Brasil foram roubados causando desconforto no relacionamento entre as duas nações.

Atualmente, os ataques cibernéticos não são só promovidos por pessoas que agem isoladamente, mas podem ser motivado por questões militares ou interesses governamentais. Diante desse cenário, a segurança da informação, antes atribuída somente aos ambientes da Tecnologia da Informação – TI, ganham espaço e importância no setor elétrico. Os conceitos de cyber segurança passam a agregar os procedimentos operacionais do SEP e tornam-se requisitos desejáveis no desenvolvimento de equipamentos e softwares aplicados aos setores de energia.

2. METODOLOGIA

A metodologia utilizada neste artigo foi a revisão de literatura, onde são selecionados artigos, por meio de uma revisão bibliográfica, com a finalidade de destacar os objetivos, metodologias e resultados de cada um deles para, a partir de então, utilizá-los no trabalho como referência. Para análise dos artigos adotou-se o método da análise de conteúdo, que busca sua lógica na interpretação do material.

A pesquisa foi realizada de forma qualitativa através do levantamento de artigos indexados no Google Acadêmico, nas bases de dados do Portal Lattes e no Scientific Electronic Library Online (SciELO). A seleção das publicações foi realizada a partir da associação das seguintes palavras chaves: Segurança Cibernética, Sistema Elétrico de Potência e Segurança em Sistema Elétrico. Foram selecionados 10 artigos, destes foram escolhidos 6.

Tabela. Trabalhos selecionados

PUBLICAÇÃO	AUTOR
Segurança Cibernética e Controle de Acesso em Sistemas Elétricos de Potência (2015)	CERNEV, R. A.
Desafios da Segurança Cibernética nas Subestações de Energia Elétrica (2013)	OLIVEIRA, C.; ABBOUD, R.
A Importância do Smart Grid na Rede Elétrica de Distribuição do Brasil (2016)	ABOBOREIRA, F.L.; CRUZ, A.F. dos S.
Segurança Cibernética em Redes de Automação e Controle (2016)	CAMPELO, L.A.K; BRASIL, A.H.
Segurança Cibernética para Processos Operativos em Sistemas de Energia Elétrica (2011)	HEINISCH, A.; LEITE, L.; SPYER, B.; RABELLO, M.
Cyber Security para Sistemas de Automação de Energia – Como a Defesa em Profundidade Pode Aumentar a Segurança Cibernética em Instalações Críticas (2016)	SOUZA, P.A.; BRANQUINHO, M.; KIEFER, A.; SANTOS, C.; VIDEIRA, E.

3. RISCOS CIBERNÉTICOS EM SUBESTAÇÕES AUTOMATIZADAS

O papel assumido pelas subestações na malha de distribuição de energia confere às redes elétricas a segurança e a confiabilidade necessária para a contínua operação do sistema. Devido à grande densidade de cargas que por elas circulam, os avanços tecnológicos atribuídos ao SEP são notoriamente encontrados em seus domínios, objetivando uma melhor qualidade da energia comercializada.

Atribui-se ao processo de automatização das subestações o aumento de equipamentos elétricos digitalizados, capazes de fornecer dados para controle e monitoramento em tempo real, auxiliando nas tomadas de decisões, especialmente em regimes de contingência, onde uma decisão equivocada pode contribuir para propagação da falha e interromper o fornecimento de energia.

Com a popularização da norma IEC 61850 e a flexibilidade para desenvolvimento de protocolos baseados no modelo OSI (*Open System Interconnection*), é comum encontrar redes *Ethernets* para conectividade dos equipamentos elétricos digitais instalados no SEP. A utilização de redes de comunicação para o tráfego de dados entre os dispositivos e os centros de operações, passa pela aplicação de protocolos baseados em redes TCP/IP.

> Por diversos motivos (ex. conectividade, capacidade de endereçamento, padronização, etc.), adotam-se tecnologias baseadas em protocolo IP (Internet Protocol), como forma de permitir a interação entre diversas tecnologias de acesso em uma única solução de comunicação em consonância com as tendências das redes de próxima geração. A principal característica a ser alcançada com essa arquitetura baseada em IP é a separação dos serviços e das aplicações, do transporte das informações a eles relacionadas (HEINISCH et al., 2011).

No início da década de 90, com a incorporação dos dispositivos elétricos digitais em substituição aos equipamentos eletromecânicos, não havia uma preocupação voltada à segurança da informação, tendo em vista que as redes automatizadas trabalhavam de forma isolada e conectavam-se por meio de canais seriais, dificultando o acesso não autorizado por terceiros ou programas maliciosos.

As evoluções provenientes da comunicação por meio dos protocolos de *internet* e a utilização de dispositivos elétricos microprocessados, trouxeram às redes elétricas inteligentes (*Smart Grids*) vulnerabilidades para a qual não foram projetadas a se defender. Segundo Souza et al. (2015) a expansão dessas tecnologias como solução para o tráfego de dados e controle remoto do sistema elétrico, contribui para o surgimento das ameaças cibernéticas, antes atribuídas as áreas de TI. Os projetos para os softwares e hardwares aplicados no SEP não tinham como premissa a segurança cibernética, mas

exclusivamente, apoiavam-se na eficiência, confiabilidade e disponibilidade para atuação em tempo real.

Os novos equipamentos digitais utilizados, em sua maioria, disponibilizam portas de acesso para comunicação com a *internet*, estando em sintonia com os avanços tecnológicos proporcionados pela área e as facilidades em sua implementação. Por esse aspecto, em projetos de subestações modernas a arquitetura adotada para comunicação dos dados é baseada pela norma IEC 61850.

A figura abaixo ajuda a ilustrar de forma didática a disposição dos equipamentos e da rede de comunicação em uma subestação automatizada. Observa-se que, desde o centro de controle local até o centro de operação e supervisão externo à subestação, utiliza-se da *internet* para entradas e saídas de dados.

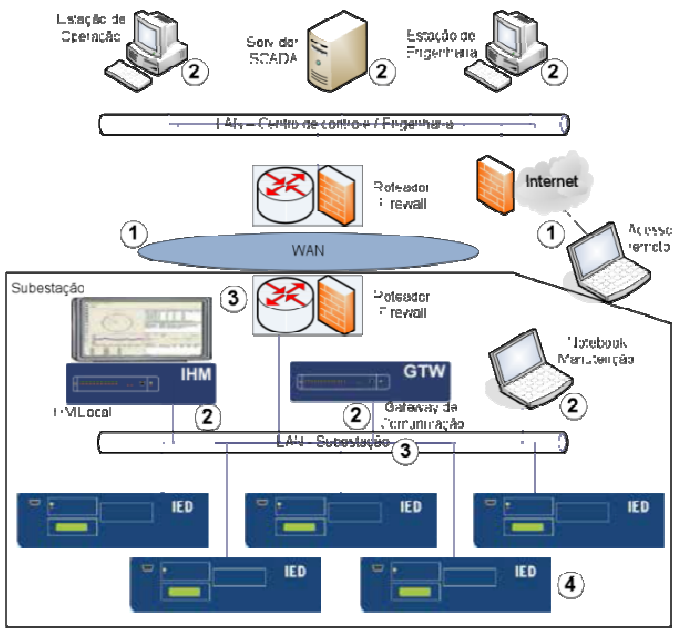

Figura 1. Arquitetura de uma subestação automatizada. Fonte: Oliveira & Abboud.

Segundo Heinisch et al. (2011), o emprego dessas novas tecnologias e o conhecimento possível de se adquirir sobre os dispositivos e dados relacionados ao sistema elétrico, torna o sistema vulnerável a potenciais ataques cibernéticos.

Em subestações automatizadas há vários níveis de comunicação via rede *Ethernet* e para cada nível suas fragilidades. Conforme demonstra a arquitetura, podemos subdividi-la em quatro partes no que se refere aos riscos cibernéticos. São elas: enlaces de comunicação externa, enlaces de comunicação interna, plataformas computacionais e ativos (IED - *Intelligent Electronic Device*). As vulnerabilidades encontradas serão abordadas nos tópicos a seguir.

3.1 ENLACES DE COMUNICAÇÃO EXTERNA

Os enlaces de comunicação externa (WAN – *Wide Area Network*) são responsáveis por disponibilizar canais de comunicação para o tráfego de dados que entram e saem de um sistema elétrico automatizado. O primeiro caminho adotado para uma invasão cibernética ocorre por meio dos enlaces externos. “Estes enlaces possuem uma exposição física e lógica sendo a porta de entrada de diversos ataques” (OLIVEIRA e ABBOUD, 2013).

A utilização da *internet* para comunicação dos dados torna os enlaces mais vulneráveis a cybers-ataque. Atualmente é comum a prática do acesso remoto aos equipamentos internos a uma subestação, o que facilita a interceptação de informações sigilosas, como por exemplo, senhas de colaboradores, ou em situações mais críticas, senhas de acessos aos IED’s, possibilitando alteração das configurações gerando danos físicos aos equipamentos protegidos por eles.

De acordo com os autores Oliveira e Abboud (2013) “A invasão é o primeiro passo para diversas outras ações danosas”, por esse motivo, a proteção dos enlaces externos deve ser a primeira barreira de segurança imposta contra os ataques cibernéticos. O *firewall* é comumente utilizado para essa finalidade. Sua aplicação ocorre pelo bloqueio de todos os pacotes “julgados” prejudiciais a operação do sistema, liberando somente os pacotes conhecidos e confiáveis.

> O firewall é uma solução de segurança baseada em hardware, que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas (BRANQUINHO et al., 2014).

A criptografia é a principal medida adotada para evitar a interceptação de dados sigilosos trafegados na rede. Sua funcionalidade consiste na codificação das informações através de caracteres reconhecido somente pelo emissor e receptor das mensagens. Segundo Branquinho et al., 2014, no processo de criptografia, as mensagens digitais são realizadas por algoritmos que embaralham os bits, a partir de uma chave ou par de chaves, tendo como objetivo principal manter um nível de segurança suficiente aos dados armazenados em computadores.

3.2 ENLACES DE COMUNICAÇÃO INTERNOS

A troca de mensagens entre os equipamentos dispostos nas subestações ocorrem por meio dos enlaces internos. Em projetos modernos os *switches* são importantes facilitadores para construção desses enlaces, funcionado como concentradores de canais *ethernet* da rede de comunicação. Sua aplicação é baseada em endereçamentos via protocolo TCP/IP.

Em subestações antigas, as UTR's (Unidade Terminal Remota) assumem o papel que hoje é atribuído aos *switches*. Devido a sua arquitetura de construção, o acesso não autorizado através das portas seriais disponíveis torna-se inviável, uma vez que, para cada porta há uma lógica de programação específica para o seu funcionamento. "Estes dispositivos possuíam várias interfaces seriais com funcionalidades programadas de acordo com a aplicação" (OLIVEIRA e ABBOUD, 2013).

Com a entronização dos switches como "chaves" de comunicação *ethernet*, o acesso mal intencionado é facilitado quando se sabe a faixa de operação IP de portas ociosas, ou seja, portas sem funcionalidade no projeto de automação da subestação. A não configuração dos *switches* gerenciáveis é um facilitador para atuação dos *hackers*. Após a invasão da rede, as senhas padrões de parametrização são utilizadas na tentativa de inviabilizar a operação do sistema e interceptar informações trafegadas.

Para redução dos problemas aconselha-se utilizar *switches* gerenciáveis com configurações baseadas em criptografias. A construção de VLAN's (*Virtual*

LAN) também contribui para a segurança cibernética em sistemas automatizados. Seu funcionamento consiste na segregação da rede física em múltiplas redes virtuais, restringindo o fluxo de mensagens a portas específicas dos *switches*. “Isso é justificado pelo fato de que, utilizando VLAN’s, as diversas classes de tráfego (serviços) circulam pela rede em domínios de Broadcast separados, mesmo estando localizados num mesmo switch” (CAMPELO e BRASIL, 2015).

Outro mecanismo de segurança é o filtro de endereço MAC (*Media Access Control*) nas portas *ethernets*, permitindo o acesso somente ao equipamento detentor do endereço.

3.3 PLATAFORMAS COMPUTACIONAIS

A popularização dos computadores e a redução dos custos para sua fabricação permitiu a entrada de plataformas computacionais em quase todos os níveis da automação de subestação. As soluções encontradas para confecção de computadores mais robustos e resistentes as interferências eletromagnéticas, comum aos ambientes de forte densidade de carga, passa pelas inovações dos sistemas operacionais aplicados em computadores pessoais.

Os problemas relacionados às vulnerabilidades encontradas nos PC’s (*Personal Computer*) são também motivos de preocupação para as plataformas computacionais empregadas nas subestações de energia. Fragilidades como vírus e erros operacionais do sistema podem ocorrer nos computadores utilizados no SEP.

Para Branquinho et al. (2014), o *malware* (*Malicious Software*) “[...] agrupa todo software ou programa criado com a intenção de abrigar funções para penetrar em sistemas, quebrar regras de segurança, roubar informações e servir de base para demais operações ilegais e/ou prejudiciais”. A ploriferação de programas maliciosos à rede de automação possui como vetores alguns elementos, como: portas USB; pastas compartilhadas, comunicação de servidores de diferentes plantas de automação, rede de *internet* sem fio e colaboradores mal intencionados ou sem preparo para executar determinadas funções.

De acordo com Oliveira e Abboud (2013) “Em um mundo globalizado e principalmente interconectado, a cada instante um tipo diferente de vírus é disseminado”. Assim como os PC’s, pode-se utilizar antivírus como medida de bloqueio para os *malware*. Seu uso deve sofrer algumas restrições, pois sua aplicação pode impactar no desempenho da rede e seus recursos são mais voltados para consumidores domésticos.

Para evitar que programas infectados se alojem na rede ou se espalhe em casos de sistemas já infectados, o acesso as informações através de mídias removíveis (pendrives ou HD externo) devem ser bloqueadas por meio de políticas operacionais ou sua utilização controlada através de senhas e antivírus embarcados.

Outro aspecto relevante que abre brechas à segurança da informação é o compartilhamento de senhas que dão acesso aos equipamentos, como por exemplo, IED’s, IHM, *gateway* ou *switches*. Essa prática bastante comum entre os operadores, embora tenha o propósito de tornas mais dinâmicas as tomadas de decisões, abre margem para que funcionários não autorizados acessem determinadas funções sem ter a capacitação necessária para lidar com elas. O hábito de compartilhamento de senha inviabiliza a política de controle de acesso, não sendo possível rastrear colaboradores que mudaram algum tipo de parametrização ou tomaram decisões equivocadas em situações críticas.

Segundo o artigo de Oliveira e Abboud (2013) “Basicamente a ação preventiva neste caso é a integração de um servidor de acesso a todas as plataformas computacionais em todos os níveis do sistema de automação de subestações”. Com essa conduta, a mesma identificação utilizada em ambientes coorporativos (*login* e senha) é absorvida pelo servidor de acesso possibilitando sua autenticação em ambientes externos, como é o exemplo das subestações.

3.4 ATIVOS (IED’s)

Os ricos cibernéticos encontrados nos IED’s são semelhantes às fragilidades abordadas nas plataformas computacionais, tendo em vista que, sistemas

operacionais estão embarcados em sua arquitetura possibilitando seu funcionamento. Por consequência, as práticas adotadas para mitigar as vulnerabilidades em plataformas computacionais podem ser aplicadas aos IED's.

A criação de barreiras para operacionalidade do IED pode ser um fator prejudicial a sua atuação devido à dinâmica do processo, mas quando usada de forma comedida e consciente torna-se uma poderosa arma para o controle de acesso, autenticação, autorização e auditoria das informações.

4. SEGURANÇA CIBERNÉTICA A PARTIR DO CONTROLE DE ACESSO

A arquitetura de subestações modernas, conforme demonstrado até aqui, apresenta vários pontos de fragilidades e suscetíveis a um ataque cibernético promovidos por *hackers*. Há uma técnica de defesa militar bastante difundida entre os profissionais de TI e atualmente aplicada nos sistemas de automação de SEP. Seu funcionamento é baseado na elaboração de sucessivas camadas de segurança, atuando de forma redundante a fim de garantir a segurança em caso de falha de uma das camadas anteriores, por esse motivo, denomina-se a esse método de Defesa em Profundidade.

> Adaptando ao cenário de automação de energia, o esquema visa não apenas prevenir brechas de segurança, mas garantir tempo à organização para detectar e responder ao ataque. Assim, reduzir e mitigar as consequências da exploração de uma vulnerabilidade de segurança (SOUZA et al., 2015).

No ponto de vista de automação de SEP, a camada mais externa para se promover a segurança é o ambiente coorporativo e a camada mais interna de defesa é a patrimonial, ou seja, dos equipamentos primários.

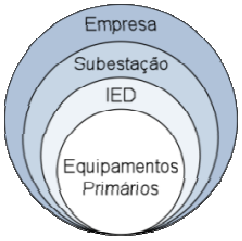

Figura 2. Defesa em Camadas. Fonte: Oliveira & Abboud.

O bloqueio às ações de programas maliciosos e funcionários mal intencionados aplica-se com a introdução de uma política organizacional voltada ao Controle de Acesso dos equipamentos e as informações organizacionais. O NIST (*National Institute of Standards and Technology*), conjunto de resoluções Americana para aplicação de redes inteligentes, divide o Controle de Acesso em quatro níveis básicos. São eles: Identificação e Autenticação; Controle de Acesso; Auditoria; e Proteção do Sistema de Comunicação.

A Identificação e Autenticação do usuário ocorrem no momento da requisição de acesso ao IED. Sua atuação visa garantir que a pessoa que está fazendo a solicitação é ela mesma e não um *malware*, como também, prevenir que o acesso seja realizado por terceiros não autorizados.

> Esta identificação pode ser realizada de diversas formas: baseado em algum objeto que a pessoa possua (por exemplo, um cartão de acesso ou chave física); algum conhecimento específico (número de identificação ou senha) ou alguma característica pessoal, tais como as biométricas (CERNEV, 2015).

O Controle de Acesso, como o próprio nome sugere, é dado às permissões necessárias para o acesso aos equipamentos baseando-se na função que o colaborador exerce na empresa. Essa distribuição dos potenciais usuários, de acordo com o papel que cada um assume na concessionária, é de grande importância para aplicação do próximo nível de controle: a Auditoria. A partir dela há possibilidade de rastreamento de todas as ações tomadas pelos colaboradores pode ser verificada a partir dela.

O último nível para o controle de acesso, segundo o NIST, é a Proteção do Sistema de Comunicação. Como já mencionado nos tópicos anteriores, a segurança para o tráfego de mensagem entre as subestações e os centros de controle remoto podem ser promovidos com a utilização de firewalls, proteção dos enlaces, utilização de protocolos seguros ou mesmo a criação de VPN (*Virtual Private Networks*).

Todos esses esforços atribuídos ao Controle de Acesso para permitir que os equipamentos das subestações não sejam manuseados por profissionais não habilitados ou programas maliciosos camuflados, pode acabar esbarrando na impossibilidade no gerenciamento de senhas. Há um número muito elevado de

dispositivos instalados nas subestações e para cada um há uma senha padrão de uso. Esse fator acaba influenciando para o compartilhamento das senhas e fragilizando a segurança cibernética da instalação.

O LDAP (*Lightweight Directory Access Protocolo*) é um protocolo de comunicação utilizado no ambiente coorporativo para gerenciamento de usuários e dispositivos da rede.

> Dentro de uma concessionária de energia elétrica já existe um diretório com os usuários que acessam a rede corporativa da empresa, esta estrutura também pode ser utilizada como o servidor central para os usuários acessarem o sistema de proteção e controle. Os equipamentos utilizados para proteção e controle do sistema elétrico tradicionalmente não possuem o recurso de autenticação junto a um diretório via LDAP, dessa forma é necessário utilizar, por exemplo, nas subestações, uma Central de Autenticação Cliente para interface entre o Servidor de Acesso Centralizado e os IED`s (CERNEV, 2015).

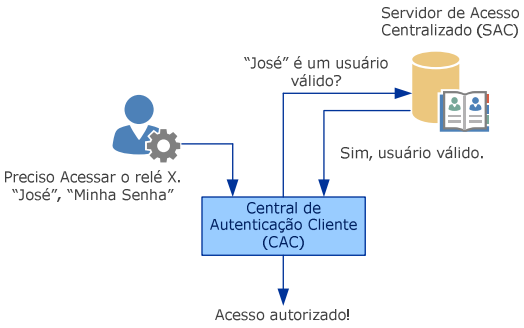

Figura 3. Autenticação no servidor de acesso centralizado (SAC). Fonte: CERNEV.

A utilização do LDAP traz como principal vantagem a utilização de senha única, para cada usuário, no acesso aos equipamentos da rede da subestação, não sendo mais necessário gravar várias senhas e permite a realização da auditoria.

5. CONSIDERAÇÕES FINAIS

A popularização da norma IEC 61850, propulsor da automação aplicada nos setores de geração, transmissão e distribuição de energia, permitiu a conectividade entre as diversas áreas do setor elétrico, facilitando seu gerenciamento e a melhorando o suprimento da energia comercializada. Os avanços tecnológicos voltados ao SEP, bastante difundida nos novos projetos

de subestações de energia, contribuíram também para abordagem de um novo tema voltado a segurança em seus domínios: A Segurança Cibernética.

Pôde-se observar no terceiro capítulo desse artigo, que, a entronização de novas tecnologias com a missão de tornar o sistema mais inteligente, trouxe junto com seus benefícios as fragilidades antes atribuídas às áreas de TI. A utilização de equipamentos elétricos microprocessados e o acesso a *internet* por meio deles, em todos os níveis da automação de SEP, mais especificamente nas fronteiras que regem a modernização das subestações, apresentam vulnerabilidades a ataques cibernéticos ou a conduta má intencional dos colaboradores que atuam no seu gerenciamento.

As motivações ao ciberterrorismo são variadas, mas há um desejo em comum nos ataques em atingir infraestruturas críticas, como estão enquadradas os setores de energia. Assim como o *Stuxnet*, um ataque cibernético pode não só roubar informações sigilosas como também causas danos a equipamentos e colocar em risco a vida da população.

No desenvolvimento do trabalho foram apresentados modos básicos para a prevenção e mitigação aos ciberataques. A aplicação de *firewall* nas portas de entrada e saída de dados da subestação, utilização de VPN's e adoção de técnicas de criptografia em todos os níveis de mensagens contribuem para redução da vulnerabilidade externas a área de automação. O gerenciamento de switches, a criação de VLAN's e o filtro por endereço MAC são instrumentos importantes na blindagem das redes internas (LAN – Local Area Network) contra os hackers. Abordou-se também no artigo que, assim como os computadores pessoais, é possível a adaptação de antivírus no combate aos *malwares* em plataformas computacionais.

Aliado a todos os mecanismos apresentados nesse artigo para blindar as redes automatizadas, de nada vale o investimento financeiro se não houver uma mudança na política organizacional das empresas. Como exposto no quarto capítulo, baseando-se na técnica de Defesa em Profundidade, a criação de procedimentos coorporativos voltados ao Controle de Acesso ao patrimônio empresarial é de fundamental importância para se ter êxito no combate ao ciberataque.

Por fim, o Controle de Acesso promovido pela autenticação, autorização e auditoria das informações possibilita garantir que a segurança cibernética atinja níveis satisfatórios, com baixos investimentos quando comparados a modernização, em todos os aspectos, de uma planta de subestação. A política de controle de acesso contribui para uma mudança comportamental dos colaboradores, evitando a ploriferação da Engenharia Social, onde informações sigilosas são disseminadas entre eles, por meio de mídias removíveis ou por enganação e exploração da confiança das pessoas.

6. REFERÊNCIAS

ABOBOREIRA, F.L.; CRUZ, A.F. dos S. **A importância do smart grid na rede elétrica de distribuição do Brasil.** XV SEPA - Seminário Estudantil de Produção Acadêmica, UNIFACS, 2016. Disponível em: http://www.revistas.unifacs.br/index.php/sepa.

BRANQUINHO, M.A; SEIDL, J. **Segurança de Automação Industrial e SCADA.** Editora Elsevier, 2014.

CAMPELO, L.A.K; BRASIL, A.H. **Segurança Cibernética em Redes de Automação e Controle**. XI Simpósio de Automação de Sistemas Elétricos (XI SIMPASE), realizado em Campinas/PR, no período de 16 a 19 de Agosto de 2015.

CERNEV, R. A. **Segurança Cibernética e Controle de Acesso em Sistemas Elétricos de Potência,** 2015, p. 1.

HEINISCH, A.; LEITE, L.; SPYER, B.; RABELLO, M. **Segurança Cibernética para Processos Operativos em Sistemas de Energia Elétrica.** VI Congresso de Inovação Tecnológica em Energia Elétrica (VI CITENEL), realizado em Fortaleza/CE, no período de 17 a 19 de Agosto de 2011.

OLIVEIRA, C.; ABBOUD, R. **Desafios da segurança cibernética nas subestações de energia elétrica.** Portal o Setor Elétrico, Edição 91 – agosto de 2013. Disponível em: https://www.osetoreletrico.com.br/desafios-da-seguranca-cibernetica-nas-subestacoes-de-energia-eletrica/

SOUZA, P.A.; BRANQUINHO, M.; KIEFER, A.; SANTOS, C.; VIDEIRA, E. **Cyber Security para Sistemas de Automação de Energia – Como a Defesa em Profundidade Pode Aumentar a Segurança Cibernética em Instalações Críticas.** XI Simpósio de Automação de Sistemas Elétricos (XI SIMPASE), realizado em Campinas/PR, no período de 16 a 19 de Agosto de 2015.