XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA

22 a 25 de outubro de 2017
Curitiba - PR

CB/GTL/23

GRUPO – XV

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL

CONCEITO DE DEFESA EM PROFUNDIDADE APLICADA NA SEGURANÇA CIBERNÉTICA DE SISTEMAS DE AUTOMAÇÃO DE ENERGIA

André Luís Franceschett (*) **Paulo Roberto Antunes de Souza Junior** **Alexandre Fernandes Onca**

RESUMO

A expansão das redes das organizações, seja na adição de novos ativos, seja na acomodação de novos serviços, ou mesmo no oferecimento de acesso aos ativos a parceiros no negócio, tem aumentado o risco de exposição a ataques cibernéticos.
Este problema, embora mais comum no ambiente de Tecnologia da Informação, ainda não recebeu a devida atenção em instalações críticas do setor de Energia, caracterizado pela presença de sistemas legados inseguros, utilização de protocolos ultrapassados e uma topologia de rede com muitas vulnerabilidades. Para eliminar vulnerabilidades e aumentar a segurança cibernética em instalações críticas aplica-se o conceito de defesa em profundidade. A funcionalidade da defesa em camadas garante redundância de proteção caso uma das camadas de proteção falhe ou apresente alguma vulnerabilidade, consistindo em um processo contínuo de Proteção, Detecção e Reação frente a uma ameaça.

PALAVRAS-CHAVE

Arquitetura de Rede Segura, Defesa em Profundidade, Firewall, Infraestrutura Crítica, Segurança Cibernética

1.0 - INTRODUÇÃO

Nesse artigo, definem-se por infraestrutura crítica instalações, bens e ativos que possuem serviços que, se interrompidos, provocam sérios impactos sociais, econômicos e políticos (BRANQUINHO et al., 2014). Infraestruturas críticas também são definidas como os ativos que se afetados por fenômenos da natureza, como terremotos, inundações ou por ações de terrorismo, causam grandes impactos em toda uma nação e sua sociedade (CANONGIA, 2009). São definidas também como os subconjuntos de ativos que afetam a continuidade da missão do Estado e a segurança da sociedade (MANDARINO, 2010). O texto apresentado trata o aspecto de segurança cibernética para uma parte das instalações criticas existentes no Brasil, sendo estas as unidades de Geração, Transmissão e Distribuição de Energia Elétrica.

Com a publicação da norma IEC-61850 no ano de 2003, cada vez mais sistemas de automação de energia de infraestruturas críticas começaram a contar com redes Ethernets e conectividade com o segmento Intranet das empresas de geração, transmissão e distribuição de energia. Diversos benefícios apareceram com a aplicação da norma IEC-61850 nesses ambientes, tais como: facilidade no acesso remoto aos IEDs instalados nas subestações, agilidade na obtenção dos arquivos de oscilografia, facilidade de obter diagnósticos de problemas remotamente, etc.

No entanto, essa expansão do perímetro de rede dos ativos das empresas que atuam no segmento de energia elétrica tem aumentado o risco de exposição desses sistemas e, consequentemente, a possibilidade de ataques

(*) Av. Dois, n° 281 – Bloco 4 – CEP 13.213-000 Jundiaí, SP, – Brasil Tel: (+55 11) 97303-1512 – Email: andre.franceschett@siemens.com

cibernéticos. Este problema, embora mais comum e já bastante discutido no ambiente de Tecnologia da Informação, ainda não recebeu a devida atenção nos ambientes industriais e nas instalações críticas.
Durante os últimos anos, casos conhecidos de ataques a infraestruturas críticas no mundo mostraram que esses tipos de sistemas são de elevado interesse no espaço cibernético, seja por motivações ideológicas, militares, pessoais ou financeiras (ramsonware – sequestro de dados).

Tendo em vista os pontos já expostos, esse documento aborda soluções de segurança cibernética e mecanismos de mitigação de vulnerabilidades de maneira a tornar o sistema de automação de energia mais seguro e confiável, seja ele aplicado a unidades de geração, transmissão ou distribuição de energia. Um conceito bastante efetivo, e já aplicado em sistemas de TI, é a defesa em profundidade (Defense In-Depth). Esse princípio será discutido e os mecanismos associados apresentados no decorrer dos capítulos.

2.0 - CASOS DE ATAQUES A INFRAESTRUTURAS CRÍTICAS

O primeiro ataque a uma infraestrutura crítica conhecido ocorreu no ano de 2000 na Austrália, em uma estação de tratamento de água e esgoto. Deste então, o tema tem sido monitorado mundialmente e os casos registrados por diversas entidades internacionais. A tabela abaixo ilustra um pequeno resumo dos casos mais conhecidos e pertinentes ao tema (CARVALHO, 2014):

Tabela 1 – Quadro Comparativo de ataques a Infraestruturas Críticas

LOCAL	INFRAESTRUTURA	AGENTE	CONSEQUÊNCIA
AUS (Queensland)	Estação de Água	Humano	Vazamento de esgoto em rios
EUA (Ohio)	Usina Nuclear	SQL Slammer	Indisponibilidade da rede de operação (6h)
EUA (Alabama)	Usina Nuclear	-	DoS – Desligamento da Usina
IRÃ	Usina Nuclear	Stuxnet	Aumento de 40% na rotação da centrífuga
Hungria	-	Duqu	Roubo de dados dos ativos industriais
IRÃ	Indústria Petrolifera	Flame	Ciber espionagem
Oriente Médio	Usina Energia	Shamoon	Destruição de dados de 30.000 máquinas
25 países	Setor Energia	Havex	Roubo de dados dos ativos industriais
Ucrânia	Distribuidora Energia	KillDisk	Interrupções de Energia (225 mil)

Em dezembro de 2015 distribuidoras de energia na Ucrânia sofreram ataques cibernéticos, resultando em interrupções de energia que impactaram aproximadamente 225 mil consumidores. Os ataques foram realizados remotamente através de acessos VPN, provocando manobras de disjuntores. O ataque foi finalizado com a infecção dos ativos com o malware “KillDisk”, comprometendo a recomposição do sistema elétrico. Em paralelo, ligações telefônicas falsas foram feitas para o SAC (Sistema de Atendimento ao Cliente), impedindo que clientes reais informassem a falta de energia.

Um experimento interessante realizado no Brasil recentemente, e que colabora com as estatísticas sobre o tema, é a exposição de um sistema SCADA à internet com o monitoramento das tentativas de acesso realizadas por (CARVALHO, 2014). Esse experimento é definido como Honeypot.

Tabela 2 – Ataques ao HoneyPot SCADA no Brasil

FAIXA IP PROVENIENTE DO PAÍS	ATAQUE	TOTAL
BRASIL, EUA, ALEMANHA, ARGÉLIA, INDONÉSIA	TCP SYN – PORT SCAN	14
EUA	UDP – PORT SCAN	1
BRASIL, EUA, PARAGUAI	MODBUS – Fluxo inválido de gravação	82
BRASIL	MODBUS – leitura de requisição ao CLP	
BRASIL, RÚSSIA, ROMÊNIA, SUÍÇA, SUÉCIA	MODBUS – leitura de identificação do CLP	
EUA, BRASIL, CANADÁ, ESPANHA	CONFICKER	6
ARGENTINA, CHINA, ESPANHA, INDONÉSIA, ÍNDIA, SUÍÇA	SQL SLAMMER	40
ALEMANHA, CORÉIA DO SUL, EUA, FRANÇA, HOLANDA, REP. TCHECA, SUÉCIA, UCRÂNIA	DoS	218

Analisando a quantidade total de ataques (361 ataques no total), com o período de tempo de exposição do sistema (90 dias), tem-se uma média de 4,01 ataques por dia. O que indica claramente o interesse de indivíduos no espaço cibernético quanto a sistemas do tipo de automação.
Ataques cibernéticos numa escala global podem ser observados on-line acessando o site da empresa americana NORSE (http://www.norsecorp.com/) que mantém a maior rede dedicada à detecção de ameaças do mundo, através de honeypots, agentes, sensores e rastreadores espalhados pelo globo (ver Figura 1). A empresa russa Kaspersky Lab também mantêm uma base on-line para consulta, com diversos tipos de ameaças. Através das ferramentas vendidas pela empresa são detectados malwares em varreduras de arquivos em disco, download de

arquivos da internet, anexos de e-mail. Além disso, sistemas com vulnerabilidades ou infectados por algum malware são identificados.

FIGURA 1 – Mapa interativo global com ataques em tempo real (Fonte: NORSE)

3.0 - DEFESA EM PROFUNDIDADE (“DEFENSE IN-DEPTH”)

O Conceito de Defesa em Profundidade (Defense In-Depth) se baseia na aplicação de diversas camadas de controles de segurança em um sistema, seus ativos e informações. O mecanismo, inicialmente aplicado a sistemas de Tecnologia da Informação, é totalmente adaptado a arquiteturas de rede de instalações críticas em sistemas de automação de energia.

A funcionalidade da defesa em camadas garante redundância de proteção caso uma das camadas de proteção falhe ou apresente alguma vulnerabilidade, que possa ser eventualmente explorada por ataques maliciosos para realizar acessos não autorizados a sistemas de automação de energia. A ideia por trás desse mecanismo é defender o sistema contra qualquer ataque particular, independente do método de ataque utilizado. É uma tática de utilização de camadas, concebida pelo NSA – National Security Agency, como uma abordagem compreensiva para segurança da informação e de sistemas eletrônicos.

A defesa em profundidade é originalmente uma estratégia militar, que tenta atrasar o ataque, ao invés de preveni-lo. Assim, o atacante leva mais tempo para chegar ao alvo, garantindo que o sistema de defesa tenha um intervalo maior para detectar o atacante e tomar as providências necessárias. 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.

A aplicação direta dessa filosofia em uma arquitetura de um sistema de automação de energia consiste na aplicação de diversos mecanismos de proteção, desde o ponto de acesso da subestação com a Intranet da empresa, até os IEDs (Intelligent Electronic Devices) instalados para a proteção e controle do sistema de energia elétrica. Junto com esse conceito, diversos mecanismos são empregados de maneira a garantir camadas de segurança na rede Ethernet de uma subestação:

- Segmentação de rede via DMZ (Demilitarized Zone)
- Uso de Firewalls para proteger as zonas de segurança da rede de automação de energia
- Hardening dos equipamentos conectados à rede Ethernet de automação de energia
- Protocolos de comunicação com criptografia
- Firmwares e softwares dos equipamentos assinados digitalmente
- Monitoramento de acessos aos dispositivos e controle centralizado de autenticação dos usuários no sistema
- Definição de grupos de usuários e seus respectivos privilégios e gestão de senhas
- Blacklisting (Antivírus) e Whitelisting (Somente programas confiáveis/aprovados são executados no sistema)
- Atualizações de segurança para correção de vulnerabilidades encontradas como parte integrante da constante manutenção e garantia de segurança no sistema
- Plano de backup e recuperação
- Elaboração de um plano de resposta a incidentes e recuperação de desastre parcial/total do sistema

4.0 - TIPOS DE AMEAÇAS PARA SISTEMAS BASEADOS EM IEC-61850

As instalações de energia e outras em geral estão expostas a uma série de ameaças. Algumas delas estão relacionadas a falhas não intencionais, ocasionadas por equipamentos defeituosos ou até mesmo desastres naturais. De um modo geral, tais falhas podem ter um impacto ainda mais significativo nas instalações e

demandam soluções que envolvam outras questões, como robustez da estrutura e confiabilidade das instalações físicas por exemplo.

Outras ameaças estão relacionadas a ataques realizados deliberadamente por agentes internos ou externos ao sistema, de forma similar ao descrito no experimento Honeypot. Podemos listar as seguintes ameaças às instalações mais comuns: Terrorismo, Vandalismo à instalação, Espionagem industrial, Roubo, Sequestro de dados, Interrupção do serviço.

Para o correto entendimento das ameaças existentes em sistemas de automação em unidades de Geração, Transmissão e Distribuição de energia, apresenta-se uma arquitetura de comunicação genérica com elementos presentes na maioria das aplicações que utilizam redes Ethernet (ver Figura 2):

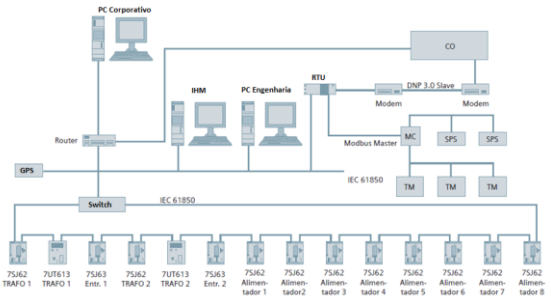

FIGURA 2 – Arquitetura de Comunicação Típica em Redes de Energia

Todos esses dispositivos apresentam vulnerabilidades que podem ser exploradas para interferências não autorizadas ao sistema de automação. Alguns tipos de ataques são apresentados na sequencia (CARVALHO, 2014):

- Acesso não autorizado ou violação de acesso: quando uma pessoa não autorizada utiliza métodos para acessar equipamentos do sistema de automação de energia, podendo executar comandos em equipamentos primários (disjuntores, seccionadoras, etc) sem autorização do operador do sistema
- Backdoor – Neste ataque o acesso remoto ao dispositivo ocorre através do uso de um programa malicioso ou devido a uma falha de desenvolvimento do produto de automação de energia (CERT.BR, 2012)
- Cavalo de tróia – São programas desenvolvidos para uma função específica e aparentemente normais, entretanto que executam funções normalmente maliciosas, sem o conhecimento do usuário (CERT.BR, 2012)
- Interceptação – Neste ataque são capturados dados de acessos legais trafegados em rede, de forma a atuar na comunicação, originalmente iniciada pela vítima
- Interferência em consulta na base de dados – Este ataque consiste na interferência em processos de consulta na base de dados, podendo causar indisponibilidade de informações
- Modificação de dados – O atacante age de forma a alterar as informações válidas por outras, de forma ilegal
- Negação de Serviço - Ocorre quando o atacante consegue interromper a disponibilidade de um serviço
- Sniffers de rede - Utilização de ferramentas para capturar pacotes de dados trafegados na rede, ocorrendo a análise do seu conteúdo
- Uso ilegítimo – Uso de dados válidos de forma ilegítima, geralmente após a captura das informações válidas de forma ilegal
- Vírus - Programa ou parte de um programa malicioso, que se propaga, se tornando parte de outros programas e arquivos (CERT.BR, 2012)
- Ramsonware – Programa que impede o acesso do usuário ao sistema infectado e força a vítima a pagar um resgate para ter acesso novamente ao sistema

Introduzidas algumas das ameaças existentes, apresenta-se na sequencia desse documento medidas de mitigação dos riscos através de mecanismos que aumentam a segurança cibernética.

5.0 - MEDIDAS DE MITIGAÇÃO DE RISCOS

A solução de defesa em profundidade ajuda a mitigar significativamente as vulnerabilidades dos sistemas e assim, aumentar a segurança cibernética de uma infraestrutura crítica. Na sequencia, são apresentados alguns conceitos e sua função dentro da solução completa:

a. Segmentação de rede via DMZ: o termo significa “Demilitarized Zone” e consiste em agrupar elementos de rede com necessidades frequentes e sensíveis de comunicação. Trata-se de uma rede física ou lógica que contém e expõe serviços de rede de acesso externo a uma rede não segura, como por exemplo, a Intranet da empresa ou a própria internet. O propósito é adicionar uma camada de segurança à LAN (Local Area Network) de maneira que redes externas, como a Intranet da empresa de energia, tenham acesso somente aos equipamentos localizados no segmento DMZ, sem acesso direto aos IEDs que protegem o sistema elétrico.
b. Uso de Firewalls Industriais para proteger as zonas de segurança da rede de automação: o uso de firewalls industriais como os da família Siemens Scalance S estabelece proteção contra ataques que explorem

vulnerabilidades em protocolos de comunicação de energia e também oferece funcionalidades para comunicação segura entre zonas via VPN.

c. Hardening: um processo que consiste em aumentar a segurança de um sistema reduzindo as vulnerabilidades existentes. Quanto mais funções e opções de comunicação e acesso um sistema possui, consequentemente, mais vulnerabilidade pode apresentar. Logo, diminuir as opções de acesso a equipamentos, IHMs, IEDs, resulta em reduzir as possibilidades de acesso indevido ao dispositivo. Desta forma, todas as portas de comunicação não utilizadas devem ser bloqueadas e todos os serviços não utilizados devem ser desligados por exemplo, reduzindo-se a superfície exposta de ataque. Esse conceito se aplica a qualquer equipamento e/ou dispositivo conectado na rede da infraestrutura critica.

d. 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.). Atualmente, os protocolos IEC-104 e DNP 3.0 já apresentam versões que utilizam o conceito de criptografia.

e. Firmwares de IEDs com assinatura digital: alguns IEDs disponíveis no mercado (como o Siprotec 5 da Siemens) apresentam uma assinatura digital do fabricante no firmware. Isso evita que o IED seja atualizado com firmwares que possam ter sido “modificados” para operarem de maneira indevida (por exemplo, realizando uma abertura de disjuntor de proteção sem a existência de falta no sistema elétrico).

f. Uso de Radius Server (Remote Authentication Dial In User Service): para permitir a conexão nas IHMs, Gateways, notebooks e dispositivos nas portas dos Switches, é possível realizar uma validação remota através de um servidor Radius. Sempre que um dispositivo é conectado ao Switch industrial (por exemplo, Siemens RuggedCom), o switch estabelece comunicação com o servidor Radius verificando se o usuário e a senha do sistema operacional do componente é cadastrado na base da dados da empresa. Existe a possibilidade de realizar a mesma validação através do MAC Address, para dispositivos que apresentam sistema operacional próprio (como IEDs, Merging Unit, etc); Deve existir um monitoramento do login dos usuários no sistema e uma auditoria dos logs com o intuito de identificar e rastrear tentativas indevidas de acesso.

g. Gestão de Senhas: metodologia que depende da ação do usuário do sistema de automação de energia e consiste em alterar as senhas “default” dos dispositivos para reduzir a possibilidade de acessos indevidos aos mesmos. A troca das senhas deve ser feita periodicamente obedecendo-se regras e requisitos mínimos para garantir a criação de senhas fortes. A utilização da autenticação multifator é recomendada, ou seja, a utilização da senha pessoal somada a outro requisito para verificação e identificação do usuário (Ex: Senha pessoal ou amostra biométrica combinada com uma chave privada armazenada em um smart card ou token).

h. A criação de políticas específicas por grupos de usuários visa definir ações claras para cada usuário do sistema, limitando ao máximo os seus privilégios. Limitando as ações dos usuários protege-se o sistema inclusive de usuários legítimos e bem intencionados que poderiam provocar danos acidentais por falta de conhecimento

i. Utilização de Blacklisting: A utilização de antivírus é recomendada em sistemas cujas instalações ou atualizações de software são constantes. Para evitar uma conexão permanente com repositórios externos através da internet, recomenda-se a atualização do antivírus manualmente.

j. Utilização de Whitelisting: Essa abordagem é preferencialmente utilizada em sistemas que não demandam atualizações constantes. O Whitelisting baseia-se numa lista de permissões, ou seja, somente programas e aplicativos confiáveis e aprovados são executados no sistema. A natureza estática de alguns sistemas, como por exemplo computadores IHM, é ideal para utilização de AWL (Application Whitelisting)

k. É extremamente importante a utilização de ferramentas para mapear todos os ativos de hardware e software do sistema, a fim de aplicar atualizações de segurança testadas e aprovadas para corrigir em tempo hábil vulnerabilidades encontradas

l. Deve existir um procedimento detalhado para backup das configurações dos equipamentos, permitindo a recuperação confiável e atualizada em caso de comprometimento total ou perdas parciais no sistema

m. A recuperação de desastres é a capacidade dos elementos de uma organização para apoiar as suas funções críticas do negócio a um nível aceitável dentro de um determinado período de tempo após uma interrupção. Portanto, devem existir procedimentos de recuperação de incidentes e planos de contingência que permitam o funcionamento degradado e seguro do sistema nos casos de violação e ataques. Frente a uma ameaça em sistemas críticos, recomenda-se, num primeiro momento, traçar estratégias imediatas de resposta e em seguida estratégias de recuperação do sistema para o estado inicial, como por exemplo:

Tabela 3 – Estratégia de Resposta a Incidentes

SISTEMA CRÍTICO	Servidor IHM
AMEAÇA	Malware
ESTRATÉGIA DE RESPOSTA	- Isolar o sistema infectado
AÇÕES DE RESPOSTA	- Verificar que o computador está isolado da rede para evitar que a infecção se espalhe para outros sistemas
ESTRATÉGIA DE RECUPERAÇÃO	- Reparar o computador infectado e retorná-lo a rede
AÇÕES DE RECUPERAÇÃO	- Executar uma varredura completa no sistema para remover a infecção. - Restaurar os dados apagados ou corrompidos. - Se não for possível recuperar o sistema, restaure as últimas configurações. - Confirme que o computador está livre do malware e o reconecte a rede.

6.0 - EXEMPLO DE ARQUITETURA GENÉRICA SEGURA

A figura seguinte (ver Figura 3) ilustra um modelo de arquitetura genérica que utiliza o conceito de defesa em profundidade associado aos mecanismos de mitigação apresentados no capítulo 5. Trata-se de uma situação simplificada que deve ser adaptada para as características do sistema de automação da infraestrutura crítica.

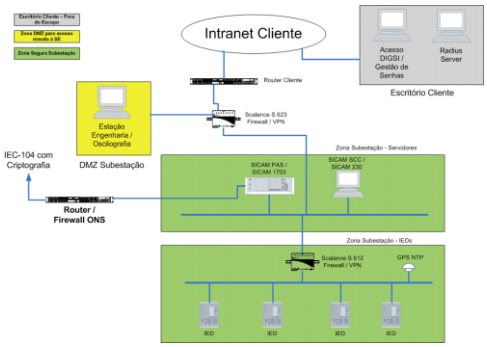

FIGURA 3 – Arquitetura Básica de Automação de Energia com Segurança Cibernética em Profundidade

7.0 - NORMAS VIGENTES

Ainda não há um documento unificado e utilizado por todos os envolvidos no desenvolvimento, operação e manutenção de instalações críticas. Existe uma série de normas, guidelines e recomendações criadas por comitês e organizações de diferentes setores e países que tratam do tema. Um esforço contínuo tem sido feito com o intuito de reconhecer novos potencias de ameaças, gaps nos padrões criados e aplicações ainda não cobertas por tais normas.
Os principais padrões pertinentes ao universo de automação de energia são IEC 62351, IEC 62443, NERC-CIP/IEEE 1686 e CIGRE D2.22.
Os padrões IEC 62351 e NERC-CIP/IEEE 1686 costumam ter uma relevância maior para os desenvolvedores de tecnologia. O primeiro pelo fato de ter sido criado por uma organização internacional, com o intuito de endereçar questões de segurança da norma IEC 61850. A norma IEC 62443 tem foco nos Sistemas de Controle e Automação Industrial e provê orientações para design e procedimentos para operação do sistema, a fim de garantir a disponibilidade, integridade e segurança de todos os componentes envolvidos. Já a norma NERC-CIP/IEEE 1686, por ser um padrão desenvolvido por uma organização norte-americana e estar associada ao maior mercado consumidor mundial.

A diferença nos requisitos entre sistemas de TI comuns e sistemas de instalações críticas exige que suas peculiaridades sejam tratadas de forma diferenciada. Mesmo com tais discrepâncias, é possível utilizar definições estabelecidas em normas de outros setores, como é o caso dos padrões do NIST SP 800-82 (Guia para segurança de sistemas de controle industriais) e ISO 27000 (TI - Padrões de Segurança da Informação). A figura abaixo (ver Figura 4)resume as principais normas vigentes, indicando o seu propósito e a quem se aplicam (ao fabricante do sistema, ao integrador ou ao operador):

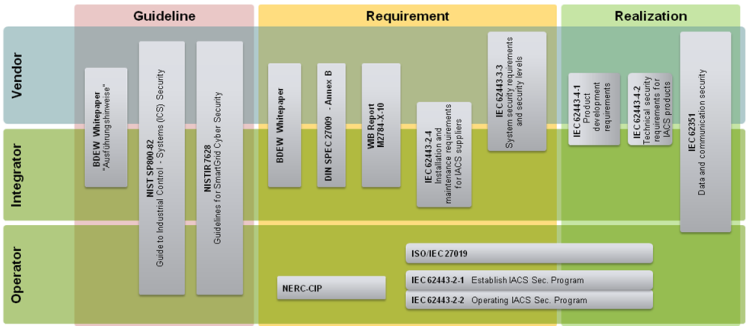

FIGURA 4 – Normas vigentes, com o propósito e o grupo de aplicação

8.0 - SITUAÇÃO DAS EMPRESAS BRASILEIRAS

No Brasil, o sistema de energia elétrica é parte do que chamamos de Infraestrutura Crítica. Tal sistema é hoje controlado pelo Sistema Interligado Nacional (SIN) que é um sistema de coordenação e controle, formado por empresas estatais e privadas das regiões Sul, Sudeste, Centro-Oeste, Nordeste e parte da região Norte e que congrega o sistema de produção e transmissão de energia elétrica do Brasil. Por sua vez, o Operador Nacional do

Sistema Elétrico (ONS) é uma entidade brasileira de direito privado sem fins lucrativos que é responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica do SIN e está sob a fiscalização e regulação da Agência Nacional de Energia Elétrica (ANEEL) do Brasil.
No que diz respeito aos aspectos legais, a responsabilidade pela segurança patrimonial de usinas hidrelétricas no Brasil, segundo a legislação do Setor (Decreto Lei 4.295, de 13 de Maio de 1942, que "estabelece medidas de emergência, transitórias, relativas à indústria de energia elétrica"), é das concessionárias de geração de energia. O artigo 5º deste decreto, que se encontra em pleno vigor, delegou ao Conselho Nacional de Águas e Energia Elétrica – CNAEE - as prerrogativas para definir as instruções necessárias para "garantir a segurança das instalações referentes à indústria da energia elétrica, bem como assegurar a continuidade ou, pelo menos, reduzir ao mínimo a interrupção dos fornecimentos respectivos". Neste sentido, observa-se que a legislação brasileira, e sua consequente aplicação regulatória, tem construção bastante antiga, no que se refere a medidas de segurança para a integridade das instalações elétricas e, portanto, defasada em termos do contexto atual de segurança cibernética. O Gabinete de Segurança Institucional da Presidência da República (GSIPR), por meio do CREDEN (6) (Câmera de Relações Exteriores e Defesa Nacional), coordena o trabalho de identificação das Infraestruturas Críticas do País. Por meio da Portaria do GSIPR no. 2/2008, foram instituídos Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIEC) para propor a implementação de medidas e ações relacionadas com a segurança das Infraestruturas Críticas nas áreas prioritárias de energia, transportes, comunicações, finanças e água. Dentre as atribuições de cada GTSIEC, estão: - pesquisar e propor um método de identificação de Infraestruturas Críticas; - articular estudos no sentido de levantar as vulnerabilidades e as ameaças das Infraestruturas Críticas identificadas e sua interdependência com outras Infraestruturas Críticas; - articular estudos e propor medidas necessárias à segurança das Infraestruturas Críticas; e - estudar, propor e implementar um sistema de informações que conterá dados atualizados das Infraestruturas Críticas para apoio a decisões. Do ponto de vista de requerimentos regulatórios e planos de ações, vemos que ainda há uma carência de tais definições, o que tem dificultado a aplicação de tais práticas pelas empresas e órgãos que atuam com Infraestruturas Críticas.
Por outro lado vemos um movimento crescente pelos setores envolvidos, no sentido de mitigar ao máximo os danos causados por problemas de segurança cibernética, como exemplo podemos citar: PNSIEC (Plano Nacional de Segurança das Infraestruturas Críticas); Os Grupos Técnicos de Segurança das Infraestruturas Críticas de Energia, Transportes, Comunicações, Água, e Finanças; O Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação; Existência de equipes de resposta e tratamento de incidentes como o CERT.br; e a criação da Rede Nacional de Segurança da Informação e Criptografia (RENASIC), gerenciada pelo CDCiber do Ministério da Defesa.

Destacam-se os trabalhos no contexto do RENASIC (7), um conjunto de ação práticas aplicadas às Infraestruturas Críticas como:):

- Desenvolvimento de mapa de rota para segurança SCADA no Brasil
- Plano de capacitação
- Normatização e aspectos regulatórios, aspectos de certificação e homologação
- Iniciativas de P&D
- Criação de um ICS-CERT Nacional

Segundo o RENASIC, estes planos de ação serão desenvolvidos por grupos de trabalho multidisciplinares que terão como objetivo comum gerar normas e boas práticas para a melhoria imediata, a curto, médio e longo prazo do nível de segurança cibernética da infraestrutura crítica nacional.

9.0 - CONCLUSÃO

Esse documento indicou no capitulo 2.0 casos reais de ataques a infraestruturas críticas e o resultado do experimento denominado "Honey Pot SCADA", esse ultimo indicando claramente o interesse internacional do mundo cibernético em sistemas SCADA no Brasil, com a marca de quatro ataques por dia a esse tipo de infraestrutura.
Fica claro assim que já existe um interesse cibernético mundial em sistemas de infraestrutura critica e a necessidade de adequar o quanto antes a legislação vigente para regulamentar e fiscalizar os sistemas de automação de energia no âmbito da segurança cibernética e garantir que sejam instalados com as devidas medidas de segurança, mitigando as vulnerabilidades existentes, como já vem sido feito por algumas entidades e ilustrado no capitulo 8.0 desse texto.
Quanto aos recursos que garantem maior segurança cibernética, os capítulos 5.0 e 6.0 abordam a aplicação da defesa em profundidade. Essa última, quando associada a outros elementos de segurança, cria uma arquitetura de rede para sistemas de automação de energia muito mais segura do que as que vêm sendo aplicadas atualmente nas empresas de energia elétrica no Brasil.
No entanto, é importante ressaltar que Segurança Cibernética não depende apenas da instalação de equipamentos ou mudança na arquitetura de rede. É necessário também associar essas medidas com a capacitação do corpo técnico que opera e mantém sistemas de infraestrutura critica. Grande parte dos ataques a sistemas se iniciam com a chamada "Engenharia Social", e somente treinamento pode combater esse tipo de abordagem.

10.0 - REFERÊNCIAS BIBLIOGRÁFICAS

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

(2) CANONGIA, C. International Critical Information Infrastructures Protection Handbook 2009. Center for Security Studies, ETH Zurich, p. 36-37, 2009.

(3) MANDARINO JR, R. Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, p. 37-38, 2010.

(4) CARVALHO, R. S. Proposta de Arquitetura Para Coleta de Ataques Cibernéticos às Infraestruturas Críticas, Instituto Militar de Engenharia, 2014.

(5) CERT.BR Cartilha de Segurança para Internet – Códigos Maliciosos, 2012. URL: http://cartilha.cert.br/malware/.

(6) CREDEN. Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), Agosto. 2010. (ainda não sancionada pela Presidência da República).

(7) RENASIC - Rede Nacional de Segurança da Informação e Criptografia Centro de Defesa Cibernética do Exército Brasileiro – CDCiber. http://www.renasic.org.br Acesso em 17/03/2017.

(8) NORSE – Site: http://www.norsecorp.com Acesso em 17/03/2017

(9) KAPERSKY – Site: https://cybermap.kaspersky.com Acesso em 17/03/2017

11.0 - DADOS BIOGRÁFICOS

ANDRE LUIS FRANCESCHETT

Nascimento: 09/09/1983
Cidade: Campinas / SP

Formação Acadêmica:

Engenharia Elétrica – Ênfase em Informática Industrial, UNESP – Bauru/SP (2002-2007)
Especialização em Redes de Computadores, UNICAMP – Campinas/SP (2008-2009)
Certificados: Cybersecurity and Its Ten Domains, Kennesaw State University – EUA (2015)

Experiência Profissional:

Engenheiro de Desenvolvimento de Sistemas Pleno na Siemens desde 2010. Especialista em protocolos e referência em SAGE (Sistema Aberto de Gerenciamento de Energia - CEPEL).
Arquiteto e Desenvolvedor de Software para Centrais Telefônicas e Redes de Nova Geração no CPqD nos anos de 2007-2010.