XX SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

Versão 1.0
22 a 25 Novembro de 2009
Recife - PE

GRUPO XV

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

REDUZINDO A OBSCURIDADE DA SEGURANÇA DA INFORMAÇÃO NO SETOR ELÉTRICO. AÇÕES E MOTIVAÇÕES NA CHESF

Elton Bernardo Bandeira de Melo (*)
CHESF

RESUMO

No Setor Elétrico a convergência de segmentos tão distintos quanto os de Tecnologia da Informação, Telecomunicações, Supervisão, Proteção, Controle e Automação de Usinas e Subestações, todos adotando a mesma tecnologia, traz consigo um grande número de vantagens, mas também vulnerabilidades e ameaças bastante específicas para Segurança da Informação. Neste cenário, bastante atenção tem sido dedicada à construção de arcabouços para as Políticas de Segurança da Informação. A implementação destas políticas traz consigo uma série de desafios técnicos e culturais de difícil transposição.

Um das estratégias adotadas no enfrentamento destes desafios é o da Segurança por meio de Obscuridade. Neste Informe Técnico, além de explanar os argumentos em prol da redução da obscuridade e apontar propostas para uma melhor condução deste tema no Setor Elétrico, são mostradas ações adotadas e compartilhadas experiências adquiridas na CHESF em sua busca por prover máxima disponibilidade, integridade e confidencialidade às informações em uma plataforma IP Integrada, por onde trafegam juntos dados operacionais e administrativos.

A publicação deste trabalho visa criar um ambiente fértil para o debate franco sobre o tema da Segurança da Informação no Setor Elétrico, subsidiando técnicos e gestores, e argumentando que a postura de manter a obscuridade no tratamento deste tema não contribuirá para o incremento da segurança em cada empresa, e ao contrário do que se pode esperar, traz ameaças ao setor como um todo.

PALAVRAS-CHAVE

Segurança da Informação, Políticas de Segurança, Segurança por meio de Obscuridade

1.0 - INTRODUÇÃO

A Segurança da Informação nas empresas do Setor Elétrico é já reconhecida por sua importância e imprescindibilidade. É tema obrigatório em todos os fóruns dedicados às Telecomunicações e Tecnologia da Informação e alvo de crescentes investimentos por parte de todos os agentes do setor elétrico, fornecedores de equipamentos e serviços, órgãos nacionais e internacionais de padronização e regulamentação, pesquisa e desenvolvimento. Neste âmbito, muito tem se feito no sentido de desenvolver e divulgar um conjunto de melhores práticas para a proteção da informação e compartilhar avanços na busca pelas implementações de boas Políticas de Segurança (1). Apesar disso pode ser percebida uma forte componente de Segurança por meio de Obscuridade permeando o Setor Elétrico.

A Segurança por meio da Obscuridade é uma estratégia onde parte da proteção contra as possíveis ameaças é

(*) Rua Delmiro Gouveia, n˚ 333 – sala A107 - Anexo II – CEP 50761-901, Recife, PE, – Brasil
Tel: (+55 81) 3229 4095 – Fax: (+55 81) 3229 4217 – Email: eltonbm@chesf.gov.br

obtida através da omissão das tecnologias utilizadas e suas vulnerabilidades. Os responsáveis pela segurança acreditam que os atacantes não irão descobrir tais vulnerabilidades, por estarem escondidas. A aplicação desta estratégia é muitas vezes feita intuitivamente e pode ser útil em muitos casos, mas se mostra ineficaz contra ataques mais direcionados e especializados.

Este Informe Técnico tem como objetivo discutir estratégias para o Setor Elétrico no enfrentamento dos desafios colocados pela convergência tecnológica no tocante à Segurança da Informação. É discutida a viabilidade de se aplicar a Segurança por meio da Obscuridade, e como esta estratégia se faz presente no cenário atual. Não são abordados aqui aspectos técnicos e tampouco detalhes na elaboração de Políticas de Segurança. Na seção 2 é apresentado um quadro resumido do contexto atual do Setor Elétrico no tocante à Segurança da Informacão. A seção 3 apresenta uma breve discussão sobre a Segurança por meio da Obscuridade. A seção 4 trata das motivações e iniciativas da CHESF e finalmente na seção 5 são apresentadas conclusões e propostas para o melhor enfrentamento dos desafios da Segurança da Informação no Setor Elétrico.

2.0 - AVANÇOS DA SEGURANÇA DA INFORMAÇÃO NO SETOR ELÉTRICO

O Setor Elétrico já percebeu a importância da Segurança da Informação. A convergência tecnológica tem levado ao uso maciço dos protocolos da pilha TCP/IP em subestações e usinas, para interconexão de equipamentos específicos do setor elétrico, seja nas redes de telecomunicações que possibilitam a operação e manutenção destas instalações ou mesmo nos escritórios onde as informações financeiras e contábeis são processadas. Esta convergência é aceita como benéfica e tem proporcionado grandes avanços na melhoria dos processos do Setor Elétrico. Porém requer ao mesmo tempo investimentos e preocupações ligadas à segurança.

No Cigré, o Grupo de Trabalho Internacional (Joint Working Group D2/B3/C2.01), trabalhou de 2003 a 2006 com foco na Segurança Cibernética, publicou diversos artigos e uma brochura técnica cobrindo diversos aspectos da segurança dos Sistemas Elétricos de usinas e subestações. O objetivo do grupo foi trazer à tona a consciência da importância da Segurança Cibernética nos Sistemas Elétricos e fornecer algumas diretrizes para a solução do problema, com a modelagem de Domínios de Segurança, metodologias de avaliação de riscos e construção de arcabouços para as Políticas de Segurança (2).

A avaliação do estado da arte da segurança cibernética no controle industrial ainda mostra diversos desafios: arcabouços conceituais são necessários e metodologias específicas para o setor de energia têm ainda que ser desenvolvidos. A colaboração entre todos os envolvidos é necessária para lidar com a segurança da informação em larga escala (4).

Atualmente no Cigré, a Segurança da Informação permeia as atividades de grupos de trabalhos que foram estruturados para tratar de diferentes temas, aos quais não pode deixar de estar associada:

a. Comunicações para a proteção de subestações e aplicações de proteção em longas distâncias;
b. Modelos de Provisão de Serviços de Telecomunicações, suas arquiteturas, gerências e suportes para as empresas de energia;
c. Arquiteturas de comunicações para aplicações de subestações baseadas em IP, e;
d. Acessos de comunicação para consumidores e produtores de energia, já com vista ao suporte de *Smart Grids*.

Diversos órgãos, além do Cigré, promovem também importantes discussões e a publicação de diretrizes na área de Segurança da Informação de grande valia para o Setor Elétrico:

a. IEC / ISO – (International Organization for Standardization) ;
b. ISA – (*International Security Alliance*);
c. NERC – (*North American Reliability Corporation*);
d. FERC – (*Federal Energy Regulatory Comission);*
e. NIST – (*National Institute of Standards and Technology*);
f. IEEE – (*Institue of Electric and Electronic Engineering*);
g. AGA – (*American Gas Association*);
h. DHS – (*Department of Homeland Security);*
i. Kema – (*Keuring Electrotechnisch Materieel Arnhem*);

No entanto, nota-se que o foco destas organizações é o desenvolvimento de padrões e normas, promoção de encontros para discussão de temas afins, e regulamentação. Muito pouco tem se investido na divulgação de incidentes, compartilhamento de experiências práticas e soluções desenvolvidas sob demanda para ataques específicos. O próprio DHS confirma que apesar do número de relatórios de ocorrências de incidentes de segurança nas empresas federais americanas terem disparado nos últimos anos, ainda é muito baixo o nível de divulgação destes eventos (3).

2.1 Adequações imposta às normas de segurança – O Caso NERC-CIP

Em 1998, o Departamento de Energia dos Estados Unidos passou à *NERC* (*North American Reliability Corporation)* o papel de coordenador das atividades de proteção da infra-estrutura crítica do setor elétrico americano. Foi criado então o CIPC (*Critical Infrastructure Protection Committee*) para responder às ameaças e incidentes de segurança e suportar a produção de padrões e diretrizes.

Com o poder de impor padrões desenvolvidos para a segurança cibernética na América do Norte, o NERC desenvolveu oito padrões de confiabilidade (CIP 002 – 009) para infraestruturas críticas, cobrindo os seguintes aspectos:

- Identificação de Ativos Cibernéticos Críticos;
- Gerenciamento de Controles de Segurança;
- A Capacitação e Treinamento de Pessoal;
- Definição de Perímetros de Segurança Eletrônica;
- Segurança Física de Ativos Cibernéticos Críticos;
- Gerenciamento da Segurança de Sistemas;
- Relatórios de Incidentes e Planos de Resposta;
- Planos de Recuperação de Ativos Cibernéticos Críticos.

A agência reguladora dos Estados Unidos, FERC (*Federal Energy Regulatory Comission*), aprovou a regras, que estão em vias de entrarem em vigor a partir de agosto 2009 e serão obrigatórias para os todos os agentes do setor elétrico daquele país. O Canadá também irá adotar tal regulamentação a partir desta data, sendo também esperada a adesão do México. Este será o primeiro caso onde a adequação às normas de segurança foi forçada pelo direcionamento de uma agência regulamentadora. As empresas norte-americanas deparam-se então com uma situação ímpar: apesar da pressão, que certamente trará alguns transtornos para os responsáveis pelas implantações e adequações às normas, pode ser uma grande oportunidade de evoluir na abordagem da segurança cibernética e alavancar o setor (5, 6).

Caso a adequação a normas semelhantes às CIP 002 -009, imputadas por agências reguladoras com o objetivo de aumentar a confiabilidade do setor elétrico, seja confirmada como uma tendência, as empresas de energia brasileiras se depararão com a necessidade de, não só se adequarem às normas de segurança, mas também mostrarem suas estratégias e tecnologias de proteção contra incidentes e serem auditadas.

2.2 Impactos das mudanças no modelo do Setor Eletrico

A indústria de energia tem historicamente sido operada por meio de redes fechadas e controladas. A abertura do mercado, com o surgimento de novos agentes, acessantes e consumidores livres, com suas influências comerciais, têm colocado novas demandas de compartilhamento de recursos e de instalações na indústria de energia. Tradicionais entidades externas como fornecedores, agências reguladoras e, até mesmo, empresas concorrentes, têm agora acessos compartilhados a segmentos de rede de subestações ou até redes de longas distâncias (Wide Area Networks - WAN). Isto ocorre independentemente de se dispor de recursos particulares ou contratados para suportar estas WANs.

Tem-se então uma junção da convergência entre os diversos órgãos das empresas de energia, com a necessidade de compartilhamento de informações com outros agentes externos (4). Ficando cada vez mais difícil e mais importante a construção de redes seguras para a operação e manutenção das subestações, com domínios de segurança bem definidos e políticas de segurança bem estabelecidas.

Num futuro próximo, é possível que as redes das empresas sejam integradas em uma única rede administrativa e operacional, para o controle dos sistemas de potência (4). Na verdade, algumas empresas de energia, como é o caso da CHESF, já estão atualmente utilizando esta arquitetura. Além disso, será necessária a interconexão das redes dos diversos agentes do Setor Elétrico, com possíveis auditorias dos mecanismos de segurança inter e intradomínios.

2.3 Discussões no âmbito da Eletrobrás

No sistema Eletrobrás foi montado um grupo de estudos dedicado à Segurança da Informação das Redes Industriais (GTMI). Este grupo vem apontando uma série de recomendações para a consolidação das Políticas de Segurança nas empresas do Sistema, dentre as quais se destaca recomendação de constituir de um comitê multidisciplinar, em cada organização, para a elaboração da Política de Segurança da Informação, envolvendo pelo menos suas áreas de TI, Telecomunicações, e Proteção e Automação. Foi também proposta a criação de um Comitê da Eletrobrás para divulgação dos problemas de Segurança da Informação encontrados nas empresas do grupo e das medidas já adotadas.

Ainda no âmbito da Eletrobrás, em fevereiro de 2008, o MME (Ministério de Minas e Energia) apontou quatro grandes diretrizes para o Sistema: São elas:

a. Aperfeiçoamento da governança corporativa,
b. Reorientação dos negócios de distribuição,
c. Reformulação institucional da *holding* e
d. Reorganização do modelo de gestão empresarial.

A partir daí foi deflagrado o plano de Transformação da Eletrobrás, que inclui uma força-tarefa para definição de uma Política Integrada de Tecnologia da Informação e Comunicação (TIC) e aponta como metas a padronização e integração das áreas de TI e Telecomunicações (http://www.eletrobras.com/elb/transformacao/main.asp).

A situação desejada é uniformizar e integrar:

a. Processos de trabalho;
b. Estruturas organizacionais;
c. Metodologias de trabalho;
d. Normas e procedimentos;
e. Planos de capacitação de profissionais;
f. Tecnologias de telecomunicações, e;
g. Plataformas de hardware e software

O objetivo do grupo é elaborar e implantar uma Política integrada de TIC para o Sistema Eletrobrás, de modo a garantir:

a. A interoperabilidade, ou, pelo menos a conectividade dos sistemas de informação das empresas do Sistema;
b. O intercâmbio de sistemas de informação das empresas;
c. A unificação de aquisições de equipamentos, softwares, circuitos de telecomunicação, cursos de capacitação técnica e serviços de TIC;
d. O suporte técnico mútuo entre as áreas de TIC das empresas do Sistema Eletrobrás;
e. Que, em prazo a ser estabelecido, as áreas de TIC das empresas do Sistema uniformizem: processos de trabalho; estruturas organizacionais; tecnologias de hardware, telecomunicações e software; metodologias de trabalho; normas e procedimentos relativos à TIC; capacitação dos seus profissionais, requisitos para contratação de serviços de TIC, etc.;
f. Utilização de sistemas padronizados quando tal medida for considerada estratégica para atendimento aos requisitos do processo / negócio envolvido.

Por se tratar da convergência de Sistemas Críticos, fica clara a necessidade de considerar os aspectos de Segurança da Informação neste Plano de Transformação. Provavelmente aproveitando as experiências, constatações e recomendações desenvolvidas no GTMI. Também fica claro a partir dos objetivos declarados pela Eletrobrás, que não poderá haver discrepâncias entre as Políticas de Segurança da Informação das empresas do Sistema, com uma forte tendência a termos políticas abertas, claras e auditadas por órgãos externos. Nos moldes do Projeto de Adequação ao Ato Sarbanes-Oxley (1), nos quais a aderência possa ser recomendável, prevalecendo os interesses da produção. Daí cabe ressaltar as aplicabilidades dos padrões NERC - CIP ou de aspectos específicos que possam ser observados para os agentes atuantes no setor elétrico brasileiro.

3.0 - SEGURANÇA POR MEIO DE OBSCURIDADE

De acordo com a Wikipedia (http://en.wikipedia.org/wiki/Security_through_obscurity) a Segurança por meio de obscuridade é um princípio na engenharia de segurança que tenta usar o segredo (no projeto, implementação, etc.) para prover segurança. Um sistema que depende da segurança por meio da obscuridade pode conter vulnerabilidades de segurança, mas os proprietários acreditam não serem conhecidas, e que possíveis atacantes provavelmente não terão conhecimento. É como se para proteger uma casa, ao invés de se investir em uma porta com trancas e chaves reforçadas, se optasse por tentar esconder a maçaneta. Este princípio é antagônico ao princípio de Kerchoff, aplicado à criptografia, que prega que um sistema criptográfico deve ser seguro mesmo que tudo sobre o sistema, exceto a chave, seja de conhecimento público, ou, numa reformulação por Claude Shannon “o inimigo conhece o sistema”.

Existe de fato um grande debate sobre o tema, com argumentos favoráveis ou contrários à obscuridade como forma de incrementar a segurança. Quase a totalidade dos especialistas concorda, no entanto, que a obscuridade jamais deve ser a base da segurança, ou seja, não se pode confiar a segurança de um sistema apenas no fato de os atacantes desconhecerem suas vulnerabilidades. Mais cedo ou mais tarde o sistema acaba sendo conhecido. Já, quanto à sobreposição da obscuridade em um sistema intrinsecamente seguro, como forma de incrementar

ainda mais a segurança, as opiniões são menos unânimes. Em geral, os argumentos a favor da obscuridade sobreposta à segurança intrínseca do sistema afirmam que tal obscuridade jamais trará prejuízos, podendo, no entanto, dificultar a vida dos atacantes.

Por exemplo, se temos um determinado servidor que trabalha com uma porta TCP default conhecida, somente mudar a porta default evitaria uma série de ataques não direcionados, como por exemplo, os de alguns *malwares*, e dificultaria ataques de *hackers* menos dedicados, porém não evitaria um ataque mais elaborado, de um *hacker* persistente e capacitado, que fizesse uma varredura das portas, coletassse e analizasse o tráfego, falsificasse endereços etc. Mas se tivermos um bom sistema de autenticação e privacidade implementado, o trabalho deste mesmo *hacker* experiente pode ser inviável mesmo que estejamos utilizando a porta default. Neste caso, com um sistema de criptografia seguro, mudar a porta do servidor não traria nenhum prejuízo de segurança, e poderia sim, trazer benefícios, uma vez que evitaria ataques menos pretensiosos e dificultaria, mesmo que pouco, ataques mais elaborados.

O problema com a segurança por obscuridade surge quando em certo nível, crê-se que o atacante não irá descobrir o sistema e suas vulnerabilidades. Muda-se o foco da redução das vulnerabilidades, para o "escondimento" das vulnerabilidades. Afasta-se cada vez mais do princípio colocado por Kerchoff e ratificado por Shannon e coloca-se uma segurança baseada na fé de que o atacante não fará a engenharia reversa do sistema, não conhecerá suas vulnerabilidades. Este pensamento propiciou derrotas aos Impérios Japonês e Alemão durante a Segunda Guerra Mundial, uma vez que seus sistemas criptográficos *JN-25* e *Wehmarcht Enigma*, respectivamente, foram descobertos pelos americanos e aliados (8).

3.1 Obscuridade no Contexto do Setor Eletrico

Além dos problemas acima mencionados, num cenário de múltiplos atores, como por exemplo, no Setor Elétrico, se a postura dominante entre os atores for a de esconder os sistemas e tecnologias utilizadas, conseqüentemente serão omitidas também vulnerabilidades descobertas em tais sistemas, retardando ações para neutralizar tais vulnerabilidades e conseqüentemente reduzindo a segurança do setor como um todo. Neste caso, divulgar os sistemas utilizados e as vulnerabilidades encontradas, bem como incidentes ocorridos e ações corretivas, dentre as empresas do Setor, levariam a um ambiente de cooperação que protegeria o setor contra ataques externos.

Ora, se se acredita que a segurança da informação no Setor Elétrico é de fato imprescindível, não há razões para retardar o aperfeiçoamento dos mecanismos de segurança. Se as empresas e demais agentes estão de fato aplicando tecnologias seguras e confiáveis, o decremento de segurança com a divulgação destas seria bastante pequeno se comparado com os benefícios de se criar um ambiente compartilhado para o tratamento de incidentes, divulgação de vulnerabilidades, avanços tecnológicos etc.

No Setor Elétrico, a não adoção de uma postura de abertura e discussão franca sobre as tecnologias aplicadas e suas vulnerabilidades seria mais justificada em situações onde as tecnologias não são confiáveis, e a segurança está simplesmente no fato de não serem conhecidas. Situação não recomendada pela maioria dos especialistas em segurança.

3.2 A falta de realimentação na Engenharia de Segurança da Informação

A engenharia de segurança da informação possui uma grande diferença em relação a outras engenharias, como a aeronáutica, a naval ou a nuclear. Embora todas devam desenvolver produtos de altíssima confiabilidade, na área de segurança da informação quase não há realimentação sobre as falhas encontradas nos produtos e serviços desenvolvidos (7).

Quando um avião cai, é primeira página em jornal. Equipes de investigadores correm para a cena do incidente e averiguações são minunciosamente conduzidas e documentadas por especialistas de uma larga gama de organizações – a companhia, a seguradora, a união dos pilotos, agência reguladora, fabricantes do avião, parentes das vítimas, etc. Tudo sob forte cobrança da opinião pública, que examina cada descoberta atenciosamente e cobra providências para que os erros não se repitam. Resumindo, a comunidade da aviação possui um forte e institucionalizado mecanismo de aprendizado. Este talvez seja o maior responsável pela alta confiabilidade do setor (7).

No âmbito da Segurança da Informação, por outro lado, não existe este mecanismo de aprendizado eficaz. A história da criptografia mostra o mesmo erro repetindo-se várias vezes. Quando um erro acontece e algum ataque é bem sucedido, levando a prejuízos em áreas críticas como no setor elétrico, petrolífero, águas e esgoto (saneamento), transporte ou financeiro, as primeiras iniciativas depois de descoberto o incidente, são no sentido de escondê-lo. Os responsáveis pela segurança raramente admitem suas falhas, o que leva aos engenheiros de

segurança da informação e criptólogos uma imensa desvantagem, eles têm que evoluir no aprendizado e aperfeiçoamento dos sistemas de segurança por si, sem realimentação.

3.3 Aspectos Culturais do Setor Elétrico

Historicamente as áreas de proteção, automação e controle sempre utilizaram protocolos de comunicação específicos, desenvolvidos pelos fabricantes dos dispositivos, e que demandavam arquiteturas de comunicação específicas, com cabeamentos dedicados. Os engenheiros e técnicos destas áreas estão acostumados com plena autonomia para projetar, operar e manter estas redes de comunicação, dispositivos e aplicações, obedecendo aos requisitos de disponibilidade exigidos pelo Setor Elétrico.

Os responsáveis pelos serviços de Telecomunicações para as empresas de energia também estão acostumados com plena autonomia para projetar, operar e manter suas redes de telecomunicações. Serviços de transporte de voz, vídeo e dados entre subestações e usinas foram projetados para atender aos altos níveis de disponibilidade requeridos pelo setor, que aos poucos foi incrementando seu nível de dependência destes recursos, que se tornaram imprescindíveis para o gerenciamento, a operação e manutenção das instalações elétricas.

Paralelamente, à parte dos processos de geração e transmissão de energia, a área de TI administrativa das empresas de energia também foi acostumada com plena autonomia para projetar suas aplicações. Com requisitos menos exigentes de disponibilidade e conseqüentemente com *SLAs (Service Level Agreements)* de manutenção menos rigorosos, e ao mesmo tempo aplicações que requerem recursos maciços de comunicação, como por exemplo, a telefonia corporativa, videoconferências, correio eletrônico, intranets etc. Em boa parte das empresas estas aplicações foram segregadas da plataforma de comunicação que atendia às atividades operacionais, noutros casos, compartilhavam os mesmos meios de comunicação.

Com a crescente utilização da tecnologia IP, estes três segmentos viram-se utilizando os mesmos recursos. Com a convergência, um mesmo equipamento, por exemplo, um *switch* que faz parte da solução de Proteção e Automação de uma subestação, é ainda assim um equipamento de telecomunicação e serve igualmente para transportar informações administrativas a computadores que estão sob posse de funcionários da empresa.

Ora, é de se esperar que cada uma destas áreas relute para manter a autonomia de seus planejamentos, projetos, aquisições, implantações, operação e manutenção. E ao mesmo tempo fica clara a sobreposição de requisitos de sistemas, projetos e equipamentos que poderiam atender, simultaneamente, às três áreas, juntando esforços e economizando recursos.

Uma solução para este tipo de impasse passa pela cessão de autonomia em prol da maximização da utilização dos recursos e retorno dos investimentos da empresa como um todo. Mas isto nem sempre acontece, sobretudo quando ceder em autonomia implica perda liberdade para atuar fora de padrões, perda de orçamento e até de pessoal. Emerge então uma tendência natural à proteção da autonomia, à custa de se omitir aspectos técnicos que, se trazidos à tona revelariam a não otimalidade na aplicação dos recursos das empresas.

Podemos concluir então que existem explicações não técnicas que pesam a favor da manutenção e até incremento da obscuridade nas soluções tecnologicas propostas pelas empresas do Setor Elétrico. Poder-se-ia argumentar que a melhoria de desempenho advinda com a acomodação cultural poderia compensar de certa forma a ineficiência na utilização dos recursos. No entanto, quando são levados em consideração os aspectos de Segurança da Informação, pode-se com propriedade afirmar que, se há a conexão entre estes três segmentos, o que parece inevitável, falhas nas medidas de segurança de um domínio podem comprometer a segurança do sistema como um todo. Logo, é necessário colocar às claras as soluções técnicas e políticas adotadas. E com isto a obscuridade é reduzida, e conseqüentemente acontecerá a cessão de autonomia distribuída comentada acima. Enfrentar este desafio cultural será uma das missões mais difíceis na busca por um Setor Elétrico com sua produção mais segura.

4.0 - AÇÕES E MOTIVAÇÕES NA CHESF

Conforme já foi explicitado em (1), a CHESF possui uma Plataforma Integrada de dados, por onde trafegam aplicações operacionais e administrativas, disputando assim os mesmos recursos. Apesar disso, não está livre dos desafios culturais discutidos na seção 3.3. Ainda em (1) apontou-se como uma solução viável e recomendável, a formação de um comitê multidisciplinar para a construção de uma Política de Segurança da Informação Integrada.

Esta solução foi levada adiante pela Diretoria da empresa, e, embora no momento de fechamento deste Informe Técnico, não tenhamos o comitê funcionando, já está preparado o arcabouço formal para a constituição deste órgão e da Política de Segurança Corporativa, o que representará um grande avanço para a CHESF, Eletrobrás e Setor Elétrico nacional. O simples fato de passarmos a ter um fórum decisor, com representantes de cada diretoria da empresa, e, sobretudo das áreas de TI, Telecomunicações e Proteção e Automação, enfatiza-se a expectativa de reduzir a obscuridade e as chances de medidas ineficazes de segurança.

A Política de Segurança da CHESF é um conjunto de princípios e diretrizes que norteiam a gestão da segurança da informação e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As principais diretrizes desta Política são:

a. A proteção da Informação – garantindo níveis adequados de integridade, confidencialidade e disponibilidade;
b. A classificação da Informação – de acordo com sua relevância e criticidade para os processos empresariais;
c. O controle de Acesso às Informações - com mecanismos de autenticação, autorização e registros pessoais;
d. O direito de propriedade da CHESF;
e. A Gestão da Segurança da Informação – incluindo o gerenciamento de riscos, monitoramento, avaliação de conformidade, gerenciamento de incidentes e continuidade dos serviços;
f. Educação em Segurança da Informação, e;
g. Divulgação da Política, para todos que interagem com a CHESF e serão direta ou indiretamente afetados;

Ações no sentido de atender a estas diretrizes já estão sendo tomadas nas áreas de Proteção e Automação, Telecomunicações e TI, mas a partir da instituição do comitê multidisciplinar, passarão a ser mais bem divulgadas, esclarecidas, coordenadas e chanceladas pelo comitê.

4.1 Medidas de Segurança no Segmento de Telecomunicações da CHESF

As ações ligadas à Segurança da Informação no segmento de Telecomnunicações da CHESF foram classificadas e agrupadas em quatro grandes grupos, de acordo com sua principal finalidade:

a. Evitar indisponibilidades das informações por falhas aleatórias dos equipamentos e serviços – Onde se inserem as atividades de manutenção da infra-estrutura de telecomunicações e conectividade, os incrementos de confiabilidade das LANs, MANs e WANs, e o correto gerenciamento destas redes;
b. Garantir confidencialidade e privacidade nas trocas de informações – Aqui temos a aplicação de *VLANs* e *VPNs*, as ferramentas de *AAA* (*authentication, authorization and accounting*), e a criptografia em redes sem fio;
c. Proteger as informações contra ataques maliciosos, - com melhorias da Proteção física dos ativos de rede, a aplicação de *Firewall* e IDS/IPS (*Intrusion Detection System, Intrusion Prevention System*), a implantação de ferramentas e políticas de QoS (*Quality of Services*), e a definição das Ilhas de Automação (possivelmente com a aplicação do IEC 61850) – e finalmente;
d. Assegurar a eficácia da Política de Segurança da Informação – Inclui a construção de um ambiente propício para a discussão interna de soluções eficazes para a redução de ameaças, sendo esta talvez a mais importante e árdua das tarefas, pois exige o comprometimento e empenho de gerentes e técnicos de equipes com perfis muito distintos.

5.0 - CONCLUSÃO

A convergência tecnológica, sobretudo com a aplicação dos protocolos da pilha TCP/IP, aponta para cada vez maior integração das redes de diversos segmentos das empresas do Setor Elétrico, incluindo suas áreas administrativas e operacionais, o que traz grandes incrementos na eficiência dos processos destas empresas, mas ao mesmo tempo requerendo maiores investimentos e preocupações ligadas à Segurança da Informação.

A evolução do Setor Elétrico leva à necessidade de troca de informações entre diferentes agentes, através da interconexão de suas redes de dados. Cada um destes agentes possuirá um ou mais domínios de segurança interligados com domínios externos, levando à necessidade da declaração das Políticas de Segurança adotadas e seus responsáveis, e possivelmente a adequação a padrões definidos por ógãos reguladores, seguindo o modelo norte-americano, onde a NERC-CIP dita e audita os padrões de Seguranças que devem ser adotados pelas redes operacionais das empresas de Energia Elétrica. Sejam elas voltadas para aplicações convergentes ou não, embora se deva ter sempre em mente que, além dos aspectos de segurança, as soluções implementadas não devem perder o foco da eficiência para as finalidades a que se destinam.

Tendo em vista a importância da Segurança da Informação no Setor Elétrico, a necessidade de implantação de controles rígidos para garantir a proteção dos Sistemas Elétricos contra ataques maliciosos, e a interdependência entre diferentes segmentos das empresas de energia e entre diferentes agentes do setor para a garantia dos níveis adequados de proteção, seria de se esperar que as empresas e cada um de seus diferentes órgãos fossem transparentes quanto à adoção dos mecanismos de Segurança, que cada responsável por um domínio de segurança publicasse e discutisse seus níveis de proteção, suas medidas de segurança, tecnologias utilizadas, suas vulnerabilidades, ameaças e incidentes ocorridos, para que todos pudessem mitigar seus riscos conjuntamente. Infelizmente isto não ocorre.

Há uma cultura de preservação da autonomia, busca por espaço e competição entre os diferentes segmentos das

empresas e entre os agentes do setor elétrico que perpetuam a obscuridade no tocante às medidas de segurança adotadas. Constata-se que muito tem se evoluído no sentido de promover o debate sobre as peculiaridades das políticas de segurança para o setor elétrico e seus principais componentes num nível mais abstrato, mas há uma enorme carência de discussões francas sobre os aspectos práticos de implementação destas políticas, sobre os incidentes ocorridos e as soluções adotadas.

Na CHESF, o primeiro passo no sentido de construir uma Política de Segurança da Informação eficaz foi dado com a criação de um comitê multidisciplinar, envolvendo os segmentos de Telecomunicações, Proteção e Automação, TI e Recursos Humanos, além de contar com representantes da área financeira e de engenharia. Espera-se que neste fórum o debate seja franco entre os diversos especialistas de segurança, para que de fato sejam conhecidos e mitigados os riscos existentes. A postura da CHESF mostra adequação à tendência global na busca por Segurança da Informação com responsabilidade e clareza nos seus processos, e pode ser considerada exemplo no cenário nacional.

Fóruns com os mesmos princípios, interessados no enfretamento dos desafios de forma cooperativa, tanto em âmbito nacional como internacional, seriam de grande valia, sobretudo se os empecilhos culturais que promovem a obscuridade neste segmento forem derrubados. Caso isto não ocorra espontaneamente num futuro próximo, é provável que ocorra pela força de autoridades regulamentadoras, com um maior desgaste por parte dos agentes envolvidos e prejuízos para o Setor como um todo.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) Elton B. Bandeira de Melo – Política de Segurança da Informação e SOX em uma Rede de Dados Integrada, Diviso de Responsabilidades na CHESF – XIX SNPTEE – 2007.

(2) Cigré Joint Working Group D2/B3/C2.01 -Security for Information Systems and Intranets in Eletric Power Systems – 2007.

(3) Ben Bain –Number of reported cyber incidents jumps – Federal Computer Week, Feb, 17, 2009.

(4) Göran ERICSSON, Managing Information Security in an Electric Utility - On behalf of JWG D2-B3-C2.01 Security for Information Systems and Intranets in Electric Power Systems, 2007.

(5) John Shaw – NERC/CIP Compliance: Headache or Opportunity? - *Utility Automation & Engineering T&D* July, 2007.

(6) Jay Beale - ”Security Through Obscurity” Ain’t What They Think It Is em http://securityportal.com/beale/beale20010720.html

(7) Ross Anderson - Why Cryptosystems fail? – Proceedings of the 1st ACM Conference on Computer and communications security, 215 – 227, Fairfax, Virginia, USA, 1993.

(8) Hal Berghel – Faith-Based Security – Communications of the ACM, Vol.51, No. 4, 13-17, April 2008.

7.0 - DADOS BIOGRÁFICOS

Elton Bernardo Bandeira de Melo
Nascido no Caruaru, PE em 16 de junho de 1980.
Mestrando (previsto para Julho de 2009) em Ciência da Computação na UFPE e Graduado (2002) em Engenharia Elétrica, modalidade Eletrônica na UFPE.
Empresa: CHESF – Companhia Hidro Elétrica do São Francisco, desde 2002.
Atua na Divisão de Engenharia de Manutenção e Reparo de Telecomunicações - DOMT
Membro do CIGRÉ-Brasi