XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA

22 a 25 de outubro de 2017
Curitiba - PR

CB/GPC/10

GRUPO - V
GRUPO DE ESTUDO DE PROTEÇÃO, MEDIÇÃO, CONTROLE E AUTOMAÇÃO EM SISTEMAS DE POTÊNCIA - GPC

SEGURANÇA CIBERNÉTICA NA CHESF: UMA ANÁLISE DE VULNERABILIDADES NA ARQUITETURA DE REDE, SUPERVISÓRIO SAGE E PRINCIPAIS PROTOCOLOS UTILIZADOS NO SISTEMA DE PROTEÇÃO E CONTROLE DAS SUBESTAÇÕES

Pablo Mascarenhas de Araújo (*)
CHESF

Fábio André da Silva
CHESF

Paulo Ricardo L. de N. Coutinho
CHESF

RESUMO

Este trabalho tem como objetivo avaliar a atual situação dos Sistemas de Proteção, Controle e Supervisão (SPCS) da Chesf no que diz respeito à segurança cibernética. A arquitetura e tecnologias utilizadas nos sistemas existentes (redes de comunicação, sistema supervisório, dispositivos inteligentes) são analisadas com respeito às vulnerabilidades e riscos de ataques cibernéticos. Estratégias de mitigação e melhorias na arquitetura são apresentadas, assim como um guia para a implementação de uma política de segurança cibernética nos sistemas SPCS Chesf.

PALAVRAS-CHAVE

Segurança cibernética, Automação, Infraestruturas críticas, SCADA, Hacking

1.0 - INTRODUÇÃO

Os Sistemas de Proteção, Controle e Supervisão (SPCS) utilizados nas subestações (SE's) da Chesf passaram por uma mudança de paradigma nas últimas décadas que os tornaram extremamente dependentes de redes de comunicação, adotando a norma IEC 61850 nos projetos de expansão e revitalização do sistema de SPCS, com IEDs conectados em rede LAN (Local Area Network) IEEE 802.3 (Ethernet), trocando informações através de mensagens GOOSE (Gereric Object Oriented Substation Event) (1). Para supervisão e controle das subestações, a Chesf adota, como as demais subsidiárias da Eletrobrás, o Sistema Aberto de Gerenciamento de Energia (SAGE), desenvolvido pelo Cepel tendo como base o sistema operacional Linux CentOS, que se conecta aos IEDs via protocolo MMS, também parte da pilha de protocolos adotada pela norma IEC 61850. A comunicação de cada SE com o COR, por sua vez, passa por um processo de mudança de tecnologia, com a substituição de conexões seriais via modem por comunicação TCP/IP utilizando a infraestrutura de rede corporativa e o sistema de transmissão de alta capacidade SDH (Synchronous Digital Hierarchy). A adoção destas tecnologias na Chesf não vieram acompanhadas de ações coordenadas de modo a implementar políticas de segurança cibernética, como monitorar o sistema a fim de identificar possíveis tentativas de ataque, elaborar planos de contigência e treinar equipes capazes de responder rapidamente a incidentes.

O cenário mundial, no entanto, mostra que cada vez mais as empresas de energia são alvos de incindentes de segurança cibernética. Dados do governo norte-americano mostram que o setor de energia ficou em segundo lugar no número de incidentes reportados no país, com 46 de 295 no total (2) (3). O risco de ataque cibernético está atualmente entre as principais preocupações dos líderes do setor energético dos principais mercados (como EUA e Europa), pois "ataques a infraestrutura de energia têm o potencial de migrar do plano virtual para o físico [...], onde em especial há o risco de danos massivos oriundos de um efeito cascata que o ataque a grandes plantas pode provocar" (4). Para além do já bem conhecido caso do ataque Stuxnet ao Irã (5), exemplos recentes incluem: ataque

(*) Rua Delmiro Gouveia, n° 333 – Anexo III, Bloco A, sala 207 – CEP 50.761-901 Recife, PE – Brasil
Tel: (+55 81) 3229-3456 – Fax: (+55 81) 3229-3311 – Email: pablom@chesf.gov.br

à rede operacional de uma fábrica de aço na Alemanha em 2014, causando imenso dano aos equipamentos (6); ataque a um departamento estatal de energia em 2015 na Austrália, para roubo de projetos a serem licitados (7); ataque a três distribuidoras na Ucrância, em 2015, que causou uma grande disrupção ao desligar 30 subestações e deixar cerca de 230.000 pessoas sem energia por até 6h (8) (9). No Brasil, experiência realizada recentemente expôs propositalmente à Internet uma emulação de sistema SCADA a fim de monitorar os incidentes ocorridos (técnica conhecida como honeypot) (10). Os dados de ataques, monitorados durante 90 dias, mostram que houve no total 316 tentativas, com 218 (69%) delas sendo ataques de negação de serviço (Denial of Service – DoS). Como aspecto interessante do experimento, foi exposto também um terminal emulando um posto de operação comum com telefonia IP. Os dados coletados mostram que houve um interesse maior por ataques ao sistema SCADA, sendo que a maior diferença em frequência (200%) ocorreu em ataques de acesso remoto.

O presente trabalho visa fazer uma avaliação inicial das vulnerabilidades e possíveis vetores de ataques ao SPCS específico das subestações Chesf, abordando o estado atual da capacidade de resposta a incidentes cibernéticos da empresa. São propostas melhorias e um roteiro para o estabelecimento de uma política efetiva de defesa cibernética dos sistemas Chesf.

2.0 - AVALIAÇÃO DE RISCOS

A segurança dos SPCS's, até duas décadas atrás, era baseada no fato de poucos entenderem as arquiteturas intrincadas, muitas vezes com soluções proprietárias, dos sistemas. Esta "segurança por obscurantismo" funciona bem em ambientes sem conexões externas, no entanto a adoção de normas abertas como a IEC 61850 e as necessidades de redução de custos, integração e interoperabilidade mudaram o paradigma deste setor. O SPCS típico das subestações Chesf é composto, em termos gerais, por diversos IEDs (relés de proteção e unidades de controle) conectados a uma rede Ethernet (rede operacional), supervisionados e controlados por um conjunto de servidores SAGE (IHMs de operação), conforme pode ser visto na Figura 1.

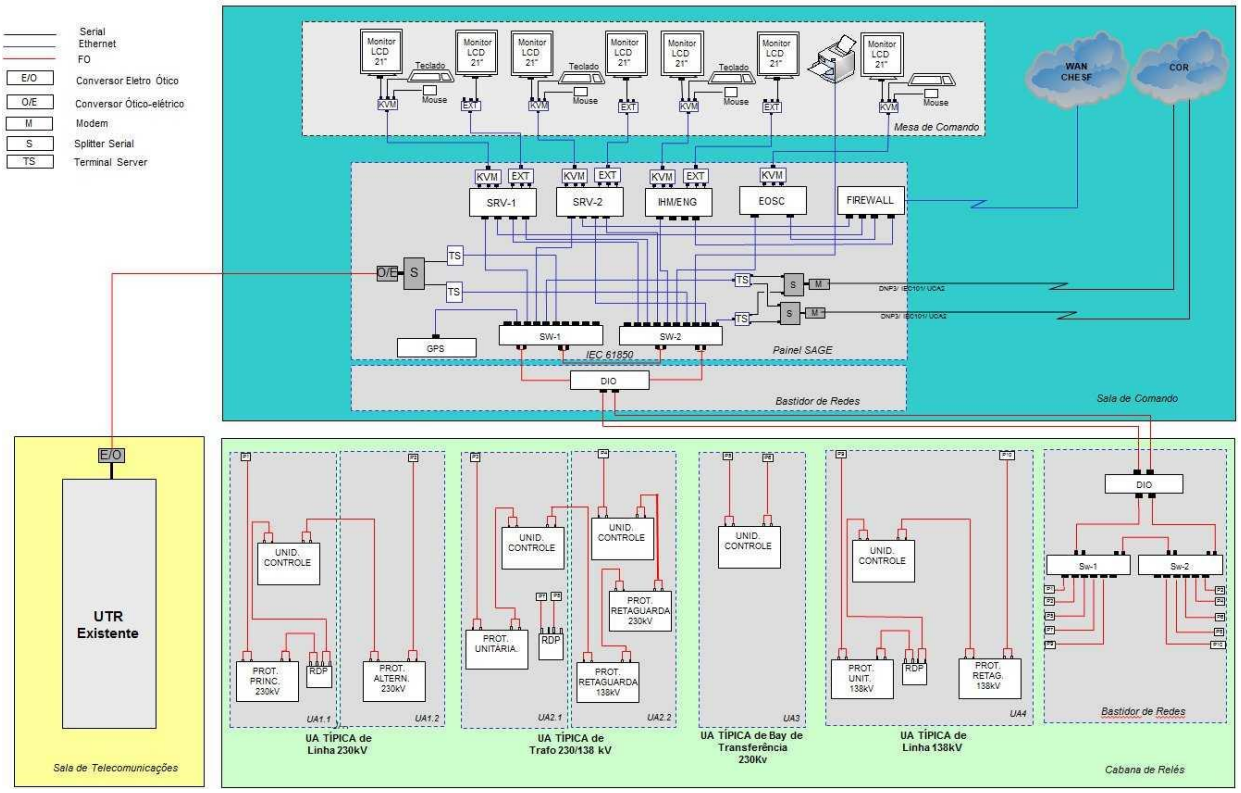

FIGURA 1 – Arquitetura típica de SPCS Chesf

A conexão com o restante da infraestrutura de telecomunicações da empresa (WAN Chesf) se faz necessária a fim de permitir a supervisão e controle pelos Centros de Operação Remota (COR), assim como o acesso remoto de dispositivos para equipes de manutenção. Neste cenário, ataques cibernéticos podem ser roteados por conexões à Internet, conexões à rede corporativa (intranet), por conexões diretas à rede de controle ou mesmo aos dispositivos diretamente. Os vetores de ataque de interesse para a análise de SPCS Chesf neste artigo são (11): backdoors e falhas na fronteira da rede; vulnerabilidades em protocolos; ataques a dispositivos de campo. Entender estes vetores é essencial para a construção de estratégias de mitigação efetivas. A segurança destes sistemas depende de quão bem as equipes da empresa, seus contratados e fornecedores compreendem a forma como o sistema pode ser comprometido.

2.1 Backdoors e falhas na fronteira da rede

Assim como todo ambiente de rede, sistemas de SPCS estão sujeitos a vulnerabilidades e brechas que podem prover ao atacante acesso não autorizado via uma backdoor (“porta dos fundos”). Normalmente estes backdoors são oriundos de pequenas falhas no perímetro da rede, de modo que não seja necessário conexão física direta à rede para obter acesso não autorizado. Na arquitetura Chesf típica, os ativos em risco e os impactos causados por atacantes são relacionados a seguir.

2.1.1. Firewall de fronteira

O comprometimento do firewall na fronteira entre a rede SPCS e o roteador da rede corporativa (ver Figura 1) permite o acesso de atacantes a todos os ativos do sistema de controle. O firewall deve evitar mapeamento de portas e serviços, assim como realizar o registro de atividades suspeitas. A correta configuração e monitoramento desta fronteira é de fundamental importância para a segurança do SPCS. Recentemente a Chesf tem empreendido um esforço entre suas equipes de manutenção e engenharia para definir e aplicar configurações mais efetivas a estes dispositivos..

2.1.2. Servidores SAGE

Os servidores baseados em Linux CentOS possuem vulnerabilidades que podem ser exploradas por malwares e hackers que consigam burlar o firewall para a abertura de backdoors. A conexão externa via intranet a estas máquinas é possível devido à manutenção remota existente na Chesf. Já funcionários e terceirizados, quando executando atividades fisicamente na subestação, têm acesso direto a estas máquinas e possuem maiores chances de comprometê-las, intencionalmente ou não. Acesso não autorizado a estas máquinas dá ao atacante possibilidade de obter controle total do sistema de supervisão e controle. Em laboratório, foi realizada uma análise de vulnerabilidades numa instalação típica do SAGE na Chesf, usando os softwares Nessus Vulnerability Scanner e Nexpose Community Edition. A versão do SAGE utilizada foi a baseada em CentOS 5.6, SAGE 2008 com o update 23.18, instalada numa máquina virtual, devido a ser a mais comum na Chesf. Os softwares de análise foram instalados e rodados em uma máquina Kali Linux. Os resultados encontram-se disponíveis na Tabela 1.

TABELA 1 – Análise de vulnerabilidades SAGE com ferramentas Nessus/Nexpose

SEVERIDADE	QUANTIDADE	EXEMPLOS
RELATÓRIO NESSUS		
Crítica	1	FreeBSD ‘telnetd’ Daemon Remote Buffer Overflow
Média	2	Unencrypted Telnet Server; SSH Weak Algorithms Supported
Baixa	3	SSH Weak MAC Algorithms Enabled; X Server Detection
Info	20	OS Identification; SSH Server Type and Version Information
RELATÓRIO NEXPOSE		
Crítica	2	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability; 'rsh' Remote Shell Service Enabled
Severa	14	FTP credentials transmitted unencrypted; Database Open Access; OpenSSL SSL/TLS MITM vulnerability; Unencrypted Telnet Service Available; TLS/SSL Server is enabling the POODLE attack
Moderada	10	FTP access with ftp account; OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability; ICMP timestamp response

Em ambos os relatórios é possível notar uma quantidade considerável de problemas de segurança, algumas críticas e com altas chances de êxito caso exploradas. Os resultados deixam evidente um problema crítico de, historicamente, se usar configurações padrões nos dispositivos do SPCS a fim de agilizar a resolução de problemas de manutenção. Esta é uma prática comum no setor e necessita ser tratada neste novo cenário de ameaça cibernética crescente. Ainda, é importante observar que alguns problemas relatados como mera informação são na verdade peças valiosas em etapas fundamentais de ataques cibernéticos: reconhecimento de alvos (reconaissance) e varredura de portas (port scanning). A coleta cuidadosa de informações é um fator crucial para ataques bem sucedidos. A Chesf tem empreendido esforços para reconfigurar sistemas antigos, fazer atualização automática de senhas e mitigar problemas deste tipo.

2.1.3. Estação de Engenharia e ativos remotos (COR e manutenção)

A estação de engenharia serve para configuração dos IEDs e acesso à base de dados local de oscilografia. São máquinas com o sistema operacional Windows e com softwares dos diversos fabricantes de dispositivos em uso no sistema (ex.: DIGSI, PCM600, Micom S1, etc). Da mesma forma que para os servidores SAGE, backdoors precisam abrir conexões remotas por portas não filtradas, e o controle não autorizado dá ao atacante possibilidade de tentar acesso aos servidores SAGE ou ter acesso direto aos IEDs via softwares de configuração dos mesmos.

Embora não seja um ataque direto ao sistema de controle da subestação, uma estratégia de pivotamento (12) pode envolver o comprometimento de máquinas do COR e das equipes de manutenção, usando backdoors para que a partir destas se ganhe acesso à rede da subestação, dado que estas máquinas podem ter acesso facilitado na fronteira da rede do SPCS (firewall). Uma vez comprometidas, podem ser usadas como origem de novos ataques. As equipes de manutenção têm acesso remoto aos sistemas de SPCS, e backdoors nestas máquinas provêm um método de evitar o firewall de fronteira. Outro possível método é usar o backdoor para instalação de código malicioso nos notebooks utilizados pelas equipes de manutenção em trabalhos de campo, de modo que estes infectem a rede de SPCS uma vez que estejam fisicamente conectados a estas.

2.2 Ataques usando vulnerabilidades em protocolos

A convergência de protocolos de rede na área de automação com os tradicionalmente utilizados nas redes corporativas abre um novo campo de exploração para ataques. As estratégias convencionais de mitigação usadas em redes comuns nem sempre são efetivas ou aplicáveis em arquiteturas de rede de sistemas críticos (13). A seguir é feita uma avaliação dos principais protocolos utilizados nas redes SPCS Chesf. É importante observar que os ataques descritos podem ser implementados com ferramentas facilmente disponíveis na Internet, como a biblioteca Scapy para Python e ferramentas como Metasploit, Cain & Abel, Macof e outros. Ainda, pelo fato de serem padrões abertos e amplamente utilizados na indústria, o conhecimento necessário para manipular estes protocolos pode ser facilmente obtido.

2.2.1. Generic Object Oriented Substation Event (GOOSE)

Boa parte da troca de sinais entre IEDs de uma subestação Chesf se dá através de datagramas GOOSE, definidos na norma IEC 61850, e transportados diretamente em frames Ethernet (14). São sinais que necessitam de alto desempenho da rede (atraso máximo de 4ms para uma mensagem do tipo 1A, relacionadas a trip), não utilizam mecanismo de confirmação e não foram projetadas originalmente para suportar mecanismos de segurança. Mensagens GOOSE carregam um conjunto de sinais definidos em datasets, e são enviadas periodicamente na rede por cada IED para endereços de destino MAC multicast configurados. O conjunto de dados de cada mensagem trafega na rede sem criptografia, sendo codificados utilizando apenas as regras definidas na Basic Encoding Rules (BER) da Abstract Syntax Notation One (ASN1). A identificação de origem é feita apenas pelo endereço MAC do emissor, e por campos de identificação da aplicação dentro do datagrama GOOSE (GoID, com identificador do IED emissor, e ConfRev para um controle de revisão da configuração). Tais características tornam o protocolo suscetível a ataques de spoofing. Um exemplo de ataque encontra-se nas etapas abaixo:

a. Monitorar as mensagens emitidas por determinado IED. De interesse para o software malicioso são os valores de status atuais dentro do dataset e os campos sequenciais de controle da comunicação: SqNum (Sequence Number), um contador que incrementa seu valor para cada mensagem emitida com os valores atuais do dataset; StNum (State Number), contador que incrementa cada vez que uma mensagem é emitida com qualquer valor de status alterado; e TimeAllowedToLive, o tempo máximo que o receptor deve esperar para receber a próxima mensagem antes de acusar um erro.
b. Alterar os sinais do dataset transportado nesta mensagem (usando a BER para decodificar e recodificar). Aqui cabe ressaltar que a priori o atacante não sabe o que significa cada valor dentro do dataset, visto que a mensagem GOOSE não transporta os identificadores, cabendo aos assinantes saber o que está recebendo. No entanto, basta que o atacante inverta ou adultere cada sinal dentro do dataset para causar impacto indesejado no sistema.
c. Atualizar os campos SqNum e StNum de acordo com as regras definidas no protocolo
d. Clonando o endereço MAC do IED de origem, o atacante pode então enviar sua mensagem GOOSE falsificada aproveitando o intervalo fixo de tempo entre mensagens GOOSE em condições normais, obedecido o TimeAllowedToLive.

Tal método foi demonstrado ser efetivo na simulação de ataques a comunicações GOOSE (15). Malware atuando desta forma pode tomar efetivamente controle sobre os equipamentos de uma subestação, causando indisponibilidades que podem ir de um simples disjuntor de linha até a ativação indevida de um esquema de proteção de barras. Somente em 2007, o IEC Technical Committee 57 (TC57), no Working Group 15 (WG15), responsável pelo desenvolvimento da norma, emitiu o padrão IEC 62351 a fim de prover segurança a diversos protocolos do TC57, incluindo GOOSE. O objetivo deste padrão é prover autenticação na troca de mensagens através de assinaturas digitais, evitar vazamento de informações, spoofing e permitir detecção de intrusos. A adoção e aplicação deste padrão, no entanto, ainda não é uma realidade nos sistemas do setor.

2.2.2. Manufacturing Message Specification (MMS)

O SAGE conecta-se aos IED's utilizando o mapeamento dos serviços definidos na Abstract Communications Service Interface (ACSI) da IEC 61850 (16) para o protocolo MMS (ISO 9506) (14). O MMS é um protocolo da camada OSI de aplicação, do tipo cliente/servidor, com menor requisito de desempenho, visto que sua função é supervisão e controle. As mensagens também transportam sinais definidos em datasets, codificados utilizando a ASN.1/BER, com opção de envio dos identificadores juntamente com os valores de status, permitindo ao receptor saber exatamente o

que cada sinal da lista significa. Devido à falta de criptografia e autenticação das mensagens, e por utilizar o modelo TCP/IP, que possui fraquezas bem conhecidas, o MMS está sujeito a ataques do tipo MITM (homem no meio), utilizando o ARP spoofing. O método de ataque é semelhante ao descrito para o GOOSE, com algum trabalho extra para lidar com as camadas adicionais da comunicação:

a. O atacante com acesso à rede do SPCS inicia um ataque do tipo ARP spoofing a fim de interceptar a comunicação entre o SAGE e um IED. Para isso ele envia mensagens ARP falsificadas que levam o SAGE e o IED a atualizarem suas tabelas ARP com o endereço MAC do atacante ao invés dos endereços MAC originais. Isso "roteia" todo o tráfego da camada 2 (Ethernet) entre SAGE/IED para a máquina do atacante.
b. Interceptando a comunicação, o atacante pode adulterar os valores dos pontos enviados antes de reencaminhar a mensagem, da mesma forma que no GOOSE, causando efeitos diversos: desde mudar medições para a operação até a atuação de controles indesejados. Após a alteração, o campo checksum do cabeçalho TCP deve ser recalculado antes da mensagem adultarada ser encaminhada.
c. Após qualquer alteração na comunicação, o atacante tem que lidar com alguns efeitos colaterais: pode haver alguma resposta da máquina alvo que o atacante deva descartar ou alterar antes de repassar para a contraparte; e toda informação de controle de sequência e confirmação deve ser corrigida durante o resto da comunicação, o que inclui os campos "Sequence" e "Acknowledgement" do cabeçalho TCP, e o campo "Invoke ID" das mensagens MMS. Sem este ajuste, a comunicação entre os dispositivos será abortada ou reiniciada.

Variações deste ataque também podem causar negação de serviço (DoS), bastando, por exemplo, que após concluir com sucesso o MITM o atacante não reencaminhe as mensagens entre IED e SAGE. Tais métodos foram explorados com sucesso na simulação de ataques a comunicações MMS (17).

2.2.3. Distributed Network Protocol (DNP3)

O DNP3 é um protocolo bidirecional entre dispositivos mestre e escravo, provendo comunicação confiável e eficiente, com baixos consumo de banda e poder de processamento. Na arquitetura Chesf, o protocolo é utilizado na comunicação dos servidores SAGE locais com o COR. Historicamente estas conexões eram feitas através de links seriais se utilizando de modens conectados a canais de fonia do sistema de transmissão SDH. Em 2016, no entanto, a Chesf começou a migração destas conexões para links DNP3 sobre TCP/IP, via roteador local da SE, o que elevou de forma significativa os riscos de segurança para este serviço. Da mesma forma que o GOOSE e o MMS, mecanismos de segurança não foram considerados originalmente no projeto do protocolo. A sua utilização em TCP/IP herda as fraquezas destas camadas, sendo igualmente possível lançar ataques do mesmo tipo descrito para os protocolos IEC 61850: escuta, interceptação, alteração de pacotes e encaminhamento das mensagens adulteradas (18) (19). Ataques neste protocolo têm o potencial de afetar Centros Regionais, inclusive levando, através da representação de um estado falso do sistema, a uma sequência de erros humanos à medida que os operadores do sistema tomam medidas para tentar "reparar" a falsa ocorrência.

2.2.4. Rapid Spanning Tree Protocol (RSTP)

Datagramas do tipo Bridge Protocol Data Unit (BPDU) são utilizados pelo protocolo RSTP para o gerenciamento de redundância (loops) na rede, permitindo o bloqueio/desbloqueio dinâmico de caminhos alternativos entre switches numa rede em que há loops lógicos. São mensagens trocadas constantemente entre dispositivos da rede habilitados para RSTP (switches e alguns IED's), enviadas diretamente em frames Ethernet com endereço multicast definido. Trata-se de um serviço básico de redes e sua interrupção pode levar ao desbloqueio indevido de portas em switches, causando loop e consequentemente indisponibilidade da rede. Como não há criptografia ou segurança intrínseca no protocolo, formas de ataques possíveis são: forjar Topology Change BPDUs; forjar BPDUs com baixa prioridade para causar mudança de root; inundar a rede com BPDUs de configuração falsas, e forçar a rede a ficar em permanente estado de eleição de root (20). Todos os ataques visam causar DoS na rede, e embora existam formas de se precaver de alguns através de configurações nos switches, é preciso ter em mente que um acesso não autorizado a qualquer switch pode causar DoS em toda a rede, caso o atacante faça uma simples má configuração do RSTP.

2.3 Ataques a dispositivos de campo

Embora normalmente o acesso remoto a dispositivos como IEDs se dê através de uma porta de entrada única (firewall de fronteira), há casos em que atacantes podem ter contato direto com dispositivos de campo. Exemplos são atividades executadas fisicamente na subestação, onde terceirizados se conectam diretamente aos dispositivos para descarregar configurações, ou sistemas de acesso remotos que acessam diretamente os dispositivos via canal dedicado, contornando o firewall. Nestes casos, um atacante pode tentar ganhar acesso a serviços rodando no sistema operacional destes dispositivos para, a partir daí, escalar privilégios e obter acesso à rede operacional, a fim de lançar ataques a demais dispositivos da rede. Desta forma, é importante monitorar e implementar políticas de segurança levando em conta a exploração de vulnerabilidades destes dispositivos e softwares. No cenário dos sistemas Chesf, foi realizada uma pesquisa sobre notificações de segurança considerando os fornecedores mais comuns de IEDs e ativos de redes, com o resultado mostrado na Tabela 2. A pesquisa levou em conta bancos de dados de vulnerabilidades na Internet como o Security Focus e o Exploits Database, assim como os sites dos próprios fabricantes, que em geral possuem seções específicas para alertas de segurança (21) (22) (23).

TABELA 2 – Ameaças relatadas em dispositivos e softwares utilizados no SPCS Chesf

NOTIFICAÇÕES DE FABRICANTES	QUANTIDADES
Denial of Service	7
Bypass de segurança	6
Bypass de autenticação	3
Vazamento de informações	3
Vazamento de informações com risco de ataque MITM	2
Bypass de segurança com risco de ataque MITM	2
Corrupção de memória	1
Buffer Overflow	1
Acesso a arquivo	1
Execução de código remoto, protocolo MMS	1
Execução de código remoto, protocolo SSH	1
Denial of Service, protocolo DNP3	1
Integer Overflow	1
Hash de senha inseguro	1
Armazenamento inseguro de senha	1
Ataque POODLE em SSL 3.0	1
Previsibilidade no TCP	1

Exemplos de produtos afetados incluem: SICAM PAS, SIPROTEC 4, ROS/ROX (Siemens), Micom S1, D60/L90 (GE), Px40/C264 (Schneider Electric), PCM600, família Rellion 670 (ABB). É importante frisar que os resultados mostram apenas questões relacionadas a equipamentos identificados como existentes na Chesf, sendo que na maioria dos casos updates estão disponíveis para correção do problema nas páginas de notificações de segurança dos fabricantes**.**

3.0 - ESTRATÉGIAS DE MITIGAÇÃO

De uma perspectiva de mitigação, simplesmente aplicar tecnologias de segurança de TI a SPCS pode não ser uma solução viável. Embora os sistemas de controle modernos usem os mesmos protocolos que são usados em redes corporativas, a própria natureza da funcionalidade do sistema pode tornar ineficazes tecnologias de segurança bem estabelecidas. O setor de energia tem características distintas que o de TI, como por exemplo: vida útil de 20 anos; dependência de poucos fornecedores; dificuldade de inventórios precisos; aplicação de atualizações é de difícil implementação e necessitam ser testadas; não é simples indispor o sistema; soluções de antivírus não são diretamente aplicáveis; auditoria necessita ser customizada e testes podem impactar na operação, entre outras (13).

Uma estratégia de defesa em profundidade (defense-in-depth) consiste em dividir o sistema em zonas (camadas), onde cada uma requer um foco diferente de segurança, sendo uma abordagem mais apropriada a SPCS. Originalmente um conceito de estratégia militar, o objetivo é reduzir as oportunidades para um atacante obter sucesso ao mover-se pela rede comprometida, e forçá-lo a despender maior esforço para atingir seus objetivos, enquanto seu avanço é monitorado e estratégias de mitigação são postas em práticas. Embora a abordagem de defesa em pronfudidade deva possuir um escopo mais abrangente na empresa, no âmbito do SPCS e tema deste trabalho foram identificadas as seguintes atividades como ponto inicial de implementação desta estratégia na Chesf, que se refletem em alterações na arquitetura e definições de projeto atuais:

- Configuração do Firewall: configurar de modo a segregar os tipos de comunicação estritamente necessárias no sistema. O tráfego deve ser monitorado e avaliado periodicamente, com regras para permitir acesso apenas de origens autorizadas. Deve-se restringir tráfego de saída, originado de dentro da rede SPCS, com exceção óbvia para a comunicação com o COR.
- Criação de DMZ para acesso remoto: qualquer acesso aos servidores SAGE deve passar necessariamente via terminal de engenharia e manutenção, localizado em uma DMZ (demilitarized zone) (13). Conexões iniciadas a partir da intranet Chesf com destino aos servidores SAGE, hoje permitidas, devem ser bloqueadas. Uma vez acessado o terminal de engenharia remotamente, conexão ao SAGE deve ser feita via SSH e/ou SFTP através da rede operativa.
- Uso de sistema de detetecção de intrusos (IDS): o firewall de fonteira comumente utilizado na Chesf possui IDS embutido, que deve ser habilitado e configurado para criar logs detalhados e emitir alertas às equipes ao detectar tráfego suspeito.
- Hardening: o terminal de engenharia e manutenção deve ser o mesmo que o de oscilografia, diminuindo o número de máquinas. Deve-se permitir logins remotos apenas de usuários autorizados, com autenticação no domínio Chesf. Atualizações de segurança devem ser aplicadas a esta máquina com prioridade, e antivírus devem ser testados e instalados. Softwares de configuração de IEDs devem estar acessíveis através de virtualização como o VirtualBox. A rede de difusão entre os servidores SAGE, crucial para a atualização em tempo real das IHMs, deve ser implementada via cabo direto entre placas dedicadas das máquinas.Todos os serviços de acesso inseguros como Telnet, FTP, etc, devem ser desabilitados em todas as máquinas da rede.

Deve ser implementada white lists para bloquear a execução de todos os softwares não declarados. As portas de switches não utilizadas devem ser desabilitadas.

- VLANs: devem ser criadas VLANs para tráfego de GOOSE de cada vão, isolando comunicação entre IEDs de vãos distintos. As conexões aos IEDs do vão de transferência e aos servidores SAGE devem estar em todas as VLANs. Na arquitetura atual, não há segregação por VLANs.

Atualmente as mudanças estão em discussão em um grupo formado no âmbito da engenharia para análise da arquitetura e segurança cibernética. A expectativa é que novos processos passem a adotar este modelo.

Por último, a adoção de políticas de segurança é um passo fundamental para proteger redes de SPCS. Algumas políticas de TI podem ser adaptadas a redes do SPCS, mas enquanto normas específicas para o sistema elétrico brasileiro não forem definidas (24), convém utilizar como base para elaboração de políticas recomendações e padrões existentes como NBR ISO/IEC 27002, ISA99/IEC 62443, NIST SP 800-82 e NIST SP 800-61. O setor elétrico precisa definir um caminho a seguir para a aplicação de um programa abrangente de segurança cibernética. A seguir é apresentado um guia para a implantação desta política na Chesf:

a. Mostrar a necessidade da segurança cibernética para o negócio: o apoio das gerências superiores é a primeiro e mais importante aspecto para o sucesso de uma política de segurança cibernética. Definir possíveis impactos econômicos, ambientais e à segurança física ajuda a entender a necessidade do tema. Deve ser criado um plano que inclua os custos estimados para desenvolver um programa de segurança em SPCS.
b. Criar e treinar uma equipe interdisciplinar: a criação de um grupo de resposta especializado em SPCS deve envolver pessoas de comunicação, automação, operação e segurança física. O grupo deve interagir e eventualmente ter apoio temporário de outras áreas como o jurídico e RH.
c. Definir atribuições e escopo: é imprescindível que a equipe tenha suas responsabilidades e poderes bem definidos, de modo que possa implementar as políticas de modo eficaz. Todas as partes interessadas devem ser consultadas e ter suas responsabilidades definidas no que concerne ao plano de segurança cibernética.
d. Definição de procedimentos e políticas específicas para SPCS: estas diretivas são a raiz de todo programa de segurança. Sempre que possível, políticas de segurança para SPCS devem ser integradas aos procedimentos operacionais existentes. Gerenciamento de atualizações críticas, gestão de senhas, checagem de logs, são exemplos de ações que devem constar nestes procedimentos.
e. Implementar um plano de gerenciamento de risco cibernético para SPCS: gerenciamento de risco implica uma robusta capacidade de responder a incidentes. É preciso fazer um inventório de ativos críticos e avaliar o impacto de diversos cenários; definindo atividades para reconhecer, responder, mitigar e restabelecer o sistema no caso de incidentes. Análise de risco e vulnerabilidades deve ser feita periodicamente.
f. Implementar treinamentos de segurança específicos: frequentemente, as equipes responsáveis por manter as redes do SPCS não possuem treinamento de segurança adequado, em geral por questões orçamentárias e por ainda não haver uma sensibilização das gerências envolvidas em relação ao tema. Um programa abrangente de treinamentos é um componente central de uma política de segurança cibernética robusta.

4.0 - CONCLUSÃO

No vasto espectro de sistemas de infraestruturas críticas como os de energia, finanças, abastecimento de água, transportes, etc., especialistas de segurança afirmam que não é uma questão de “se”, mas de “quando” haverá um ataque cibernético (25). A ameaça a redes operativas de empresas de energia é uma realidade que precisa ser internalizada na cultura do setor elétrico. Antes isolados e com protocolos fechados, estes sistemas hoje se utilizam de tecnologias bem estabelecidas em TI, protocolos abertos, e estão conectados às demais redes e sistemas da empresa, o que significa um enorme aumento do risco de incidentes. Por, historicamente, não haver no setor uma preocupação com a segurança cibernética, diversos vetores de ataques podem ser explorados por agentes mal intencionados. No sistema Chesf, foram identificadas vulnerabilidades no supervisório, protocolos e dispositivos frequentemente utilizados no SPCS das subestações. Como medidas de mitigação, melhorias na arquitetura, projeto e configuração dos sistemas estão em andamento, aplicando os conceitos de defesa em profundidade. Há um longo caminho, no entanto, para a Chesf implementar um programa abrangente de segurança em SPCS, que inclui definir políticas, procedimentos, e um plano de resposta a incidentes. Exemplos de questões a serem respondidas por tal programa incluem: como o sistema será operado em caso de indisponibilidade causada por uma invasão? Como backups podem ser restaurados rapidamente caso um ataque apague bases de dados e configurações? Quais dispositivos podem ser retirados de operação durante um ataque, quais são críticos? Que equipe é capaz de investigar e colher evidências de um incidente no SPCS? Que medidas serão tomadas pela empresa caso se detecte que um funcionário ou terceirizado foi o causador de um incidente? Que medidas judiciais são previstas? Que equipe está autorizada pela gerência a fazer análise de vulnerabilidades no sistema? Este trabalho é um pequeno passo para responder estas questões.

5.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850 Communication networks and systems in substations - Part 7-1: Basic communication for substation and feeder equipment - Principles and models. Geneva, 2003.

(2) IDAHO NATIONAL LABORATORY. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. Ago. 2016. Disponível em: <https://energy.gov/epsa/downloads/cyber-threat-and-vulnerability-analysis-us-electric-sector>. Acesso em 20 Jan. 2017.

(3) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER. Year in Review FIY 2015. US Department of Homeland Security. Disponível em: <https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf>. Acesso em 16 Jan. 2017.

(4) WORLD ENERGY COUNCIL. The road to resilience: managing cyber risks. Set. 2016. Disponível em: <https://www.worldenergy.org/publications/2016/the-road-to-resilience-managing-cyber-risks/>. Acesso em 16 Jan. 2017.

(5) LANGNER, R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy, v. IX, n. 3, 23 Mai. 2011. Disponível em: <http://ieeexplore.ieee.org/document/5772960/>. Acesso em 14 Fev. 2016.

(6) BBC. Hack attack causes 'massive damage' at steel works. BBC. 22 Dez. 2014. Disponível em: <http://www.bbc.com/news/technology-30575104>. Acesso em 6 Fev. 2017.

(7) LAVOIPIERRE, A. Cyber attack on NSW Government department raises security fears, ABC News. 3 Fev. 2016. Disponível em: <http://www.abc.net.au/news/2016-02-03/hackers-target-state-government-department/7136076>. Acesso em 6 Fev. 2017.

(8) ZETTER, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired Magazine. 3 Mar. 2016. Disponível em: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>. Acesso em 6 Fev. 2017.

(9) GOODIN, D. Hackers trigger yet another power outage in Ukraine. ArsTechnica. 11 Jan. 2017. Disponível em: <https://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/>. Acesso em 6 Fev. 2017.

(10) CARVALHO, R. S. Proposta de Arquitetura para Coleta de Ataques Cibernéticos às Infraestruturas Críticas. Dissertação (Mestrado) - Instituto Militar de Engenharia. Rio de Janeiro, 2014.

(11) ZHU, B.; JOSEPH, A.; SASTRY, S. A Taxonomy of Cyber Attacks on SCADA Systems. In: International Conference on Cyber, Physical and Social Computing, 4., 2011, Dalian. IEEE, 2011.

(12) FRASER, G. Tunneling, Pivoting, and Web Application Penetration Testing. 27 Jul. 2015. Disponível: <https://www.sans.org/reading-room/whitepapers/testing/tunneling-pivoting-web-application-penetration-testing-36117>. Acesso em 10 Nov. 2016.

(13) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Set. 2016. Disponível em: < https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf> . Acesso em 10 Jan. 2017.

(14) INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850 Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. Geneva, 2004.

(15) HOYOS, J.; DEHUS, M.; BROWN, T. X. Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure. In: Globecom Workshops, 2012. IEEE, 2012.

(16) INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850 Communication networks and systems - Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI). Geneva, 2003.

(17) KANG , B. et al. Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations. IEEE Conference on Emerging Technologies & Factory Automation, 20., 2015. IEEE, 2015.

(18) RODOFILE, N. R.; RADKE, K.; FOO, E. Real-Time and Interactive Attacks on DNP3 Critical Infrastructure Using Scapy. In: Proceedings of the Australian Information Security Conference, 13., 2015. Sydney: Australian Computer Society Inc, 2015.

(19) LEE, D. et al. Simulated Attack on DNP3 Protocol in SCADA System. In: Symposium on Cryptography and Information Security, 31., 2014. Kagoshima: The Institute of Electronics, Information and Communication Engineers, 2014.

(20) VYNCKE, E.; PAGGEN, C. Attacking the Spanning Tree Protocol. CISCO. 4 Jun 2008. Disponível em: <http://www.ciscopress.com/articles/article.asp?p=1016582&seqNum=2>. Acesso em 24 Fev. 2017.

(21) ABB. Cyber security alerts and notifications. ABB Website. Disponível em: < http://new.abb.com/about/technology/cyber-security/alerts-and-notifications>. Acesso em 7 Mar. 2017.

(22) SIEMENS. ProductCERT Security Advisories. Siemens Website. Disponível em: <http://www.siemens.com/cert/en/cert-security-advisories.htm>. Acesso em 7 Mar. 2017.

(23) SCHNEIDER ELECTRIC. Security Notifications. Schneider Electric Website. Disponível em: <http://www.schneider-electric.com/b2b/en/support/cybersecurity/security-notifications.jsp>. Acesso em 7 Mar 2017.

(24) FRANCESCHETT, A. L.; SOUZA JUNIOR, P. R. A.; KIEFER, A. Conceito de Defesa em Profundidade na Segurança Cibernética de Sistemas de Automação de Energia. In: Seminário Técnico de Proteção e Controle, 13., 2016. Brasília: Cigré-Brasil, 2016.

(25) LYLE, A. “Not If, But When”: NSA Official Discusses Importance of Cyber Vigilance. U.S. Department of Defense Website. 20 Out. 2016. Disponível em: <https://www.defense.gov/News/Article/Article/980031/not-if-but-when-nsa-official-discusses-importance-of-cyber-vigilance>. Acesso em 10 Janeiro 2017.

6.0 - DADOS BIOGRÁFICOS

Pablo Mascarenhas de Araújo

Nascido em Recife, Pernambuco, em 1978, é formado em Engenharia Elétrica com ênfase em Eletrônica pela Universidade Federal de Pernambuco - UFPE (2002), e possui Especialização em Sistemas de Proteção pela Universidade Federal do Rio de Janeiro – UFRJ (2005). Possui 15 anos de experiência na Companhia Hidro Elétrica do São Francisco – Chesf atuando nas áreas de projeto e implantação de sistemas de proteção, controle, supervisão, teleproteção e redes internas de subestações, com ênfase em sistemas SAGE e protocolos de redes de automação.

Fabio Andre da Silva

Nascido em Recife, Pernambuco, em 1980. É graduado em Engenharia Eletrônica na Universidade Federal de Pernambuco – UFPE (2006). Possui especialização em Engenharia de Testes pelo Centro de Informática da UFPE (2007), e Engenharia de Instrumentação pela UFPE (2009). Trabalhou na Motorola/Brazil no desenvolvimento de ferramentas automatizadas de testes para sistemas móveis, em 2007. A partir de 2008, trabalhou na Petrobras na operação e manutenção da planta de Coqueamento Retardamento da REPLAN. Desde 2012, trabalha na Companhia Hidro Elétrica do São Francisco – Chesf, na área de engenharia de proteção, controle e supervisão de subestações.

Paulo Ricardo Lopes de Navarro Coutinho

Nascido em João Pessoa, Paraíba, em 1978. É graduado em Engenharia Elétrica na Universidade Federal de Campina Grande – UFCG (2002), e Mestre em Sistemas Elétricos de Potência pela UFCG (2012). Desde 2002, trabalha na Companhia Hidro Elétrica do São Francisco – Chesf, na área de engenharia de proteção, controle, e supervisão de subestações, tendo trabalhado na elaboração de especificações técnicas, testes de fábrica e comissionamento de diversas subestações de níveis de tensão 69, 230 e 500kV do SIN. Desde 2015, assumiu a gerência da divisão responsável pela emissão de projetos básicos e padrões de proteção e controle, pela validação dos testes de modelo e pela homologação de novas tecnologias a serem implementadas no sistema elétrico da Chesf.