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

Hardening: Reduzindo a superfície de ataque de um servidor SAGE

ANDRE LUIS FRANCESCHETT(1); FABIO LEANDRO PEREIRA DE BARROS(2); NILSON TINASSI PERES(3); PAULO ROBERTO ANTUNES DE SOUZA JUNIOR(4);
Siemens (1);Siemens (2);USP(3);Siemens (4);

RESUMO

Os componentes em geral, equipamentos e softwares de uma infraestrutura crítica de energia, geralmente são fornecidos com uma configuração inicial de uso geral que enfatiza as características e facilidade de uso, às custas da segurança. Sabe-se que quanto maior o número de funções, programas, interfaces físicas e opções de comunicação ou acesso um sistema possui, consequentemente, mais vulnerabilidades e "brechas" ele pode apresentar, ficando, portanto, mais exposto a ameaças cibernéticas. O Hardening é um mecanismo de segurança que consiste em aumentar a segurança de um sistema reduzindo as vulnerabilidades existentes através da aplicação de configurações seguras e técnicas capazes de limitar a sua superfície exposta de ataque tornando o sistema mais robusto e resiliente a vulnerabilidades.
O objeto de estudo deste trabalho é o SAGE (Sistema Aberto de Gerenciamento de Energia) cuja presença é abundante e marcante nas principais empresas do setor elétrico brasileiro, selecionado por sua relevância nos sistemas críticos de energia e criticidade no que concerne a preocupação com o tema de segurança cibernética. O trabalho demonstra que a aplicação do Hardening em um servidor SAGE com sistema operacional Linux (CentOS) eleva significativamente a segurança sistêmica, de tal maneira que, com pouco esforço de engenharia, o servidor torna-se mais seguro, confiável, robusto e de difícil penetração, limitando a probabilidade de que algum malware ou ataque direcionado invada e contamine o sistema.
Pensando na importância que os sistemas críticos de energia representam e nas consequências negativas e no grande impacto que um possível ataque a esses sistemas trariam, não há dúvida de que é válida a abordagem de prevenção através da utilização de técnicas e conceitos de proteção com a aplicação de Hardening. Por fim, conclui-se que o Hardening é um mecanismo cujo conceito pode e deve ser expandido e extrapolado para todos os componentes que fazem parte de um sistema crítico de energia.

PALAVRAS-CHAVE

Segurança Cibernética, Hardening, SAGE, Linux, Infraestrutura Crítica

1.0 - INTRODUÇÃO

Esse trabalho define inicialmente o sistema SAGE e sua relevância no que concerne à segurança cibernética para os sistemas críticos de energia brasileiros.
Este trabalho se concentra no Hardening aplicado ao SAGE (Sistema Aberto de Gerenciamento de Energia), uma

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

peça de estrema importância e presente em abundância em todo o setor elétrico brasileiro. Portanto, o foco principal deste trabalho será aplicar em um servidor SAGE um mecanismo de segurança cibernética conhecido como Hardening cuja finalidade técnica é elevar o nível de segurança do sistema. Como resultado da aplicação do Hardening no servidor SAGE espera-se provar a viabilidade desse mecanismo para elevar a segurança cibernética geral do sistema e provar a sua eficácia como peça integrante de um conceito mais amplo conhecido como Defesa em Profundidade (Defense In-Depth), que se baseia na aplicação de diversas camadas de controles de segurança em um sistema, seus ativos e informações. Este é um ponto muito importante que deve ser salientado para evitar interpretações incorretas de que o Hardening seria a resposta definitiva na prevenção de riscos cibernéticos. O Hardening, apesar de extremamente necessário como medida de proteção do ponto de vista de uma solução segura, é apenas uma medida dentre outras igualmente importantes que devem ser empregadas em camadas e em conjunto para garantir um nível de segurança adequado, entre elas podemos citar como exemplo: Arquitetura Segura, Controle de Acesso e Gerenciamento de Contas de Usuários, Privilégio Mínimo, Proteção contra Malware, Backup e Restauração, Logs e Monitoramento, Patching, Acesso Remoto Seguro, etc. Para manter o foco do trabalho e possibilitar um aprofundamento técnico detalhado outras medidas que não estejam relacionadas ao Hardening serão desconsideradas ao longo deste trabalho.

Um dos objetivos deste trabalho é mensurar o esforço necessário para aplicar as recomendações de Hardening no SAGE e observar a efetividade da proteção alcançada.

Sabe-se que grande parte da base instalada de SAGE em operação no ambiente produtivo tem versões desatualizadas de Sistema Operacional e Software, não contemplando assim as atualizações de segurança mais

recentes, estando a mercê de vulnerabilidades muito antigas e primitivas. Essas versões estão fora do escopo de análise deste trabalho, pois apresentariam lacunas de segurança muito básicas que teoricamente já foram corrigidas por patches nas versões mais recentes. Portanto, adotou-se como premissa utilizar as versões mais recentes do pacote de distribuição SAGE com o Sistema Operacional Linux CentOS e a partir dessa linha de base analisar, mensurar e aplicar medidas para mitigar as vulnerabilidades ainda remanescentes.

O trabalho descreve a aplicação de um guia de configuração segura do sistema e traz recomendações específicas que serão aplicadas durante a sua engenharia, discutindo também a melhor fase para implementação durante o projeto (Parametrização, Teste em Fábrica e/ou Comissionamento). Além disso, é considerado o esforço de engenharia necessário para aplicar tais configurações.

Ferramentas são utilizadas para mensurar, antes da aplicação do Hardening, a saúde geral do sistema através do mapeamento de pontos vulneráveis e levantamento das possibilidades de uso de exploits, gerando uma classificação do nível de segurança do sistema. Após a aplicação dos mecanismos de defesa recomendados pelo Benchmark de referência fornecido pelo CIS, a análise é refeita, para provar que ataques que outrora poderiam ser realizados agora não surtem mais efeito (foram mitigados) ou cuja complexidade é tão alta que a probabilidade de que ocorram e causem algum impacto significativo é muito baixa.

2.0 - O SAGE NO CENÁRIO DAS INFRAESTRUTURAS CRÍTICAS DE ENERGIA

O SAGE (Sistema Aberto de Gerenciamento de Energia) [1] é um sistema SCADA/EMS (*Supervisory Control and Data Acquisition/Energy Management System*) de grande porte e alto desempenho, desenvolvido e constantemente atualizado pelo Cepel [2]. O software SAGE é uma aplicação executada no sistema operacional Linux, distribuição CentOS. É utilizado por dezenas de concessionárias de geração, transmissão e distribuição de energia elétrica no Brasil, em especial as empresas fundadoras do Cepel (Chesf, Furnas, Eletronorte e Eletrosul), além do Operador Nacional do Sistema Elétrico (ONS), em todos os seus centros de controle. Atualmente, o SAGE é o sistema SCADA/EMS preferido por mais de 230 empresas e controla mais de 1.300 instalações (Subestações, Usinas e sistemas elétricos) em todo o Brasil, tendo presença em 8 das 9 maiores empresas brasileiras de transmissão de energia (dados de 2018). Portanto, não há dúvidas da relevância desse sistema

para o setor de energia no Brasil e sua relevância no que concerne aos aspectos de segurança e proteção dos sistemas críticos de energia do país.
Qualquer vulnerabilidade que possa ser maliciosamente explorada no SAGE poderia ser de grande impacto trazendo consequências catastróficas e danos irreparáveis às empresas do setor elétrico como, por exemplo, degradação e interrupção dos negócios, comprometimento da segurança resultando em perda de vida humana, impactos ambientais indiretos, perda de reputação e degradação da imagem da empresa, perdas financeiras diretas devido à indisponibilidade do sistema e tempo de recuperação do mesmo (se for possível), além de multas contratuais e desvalorização das ações da empresa no mercado. Portanto, é inquestionável a necessidade de proteger esses sistemas a todo custo, aplicando medidas técnicas capazes de elevar o nível geral de segurança do sistema, reduzindo assim a probabilidade de exploração e limitando o impacto de um possível ataque bem sucedido.

3.0 - HARDENING

De acordo com o NIST (*National Institute of Standards and Technology*) [3], o termo "Hardening" é definido como: "Um processo destinado a eliminar meios de ataque, corrigindo vulnerabilidades e desativando serviços não essenciais."
De acordo com os requisitos apresentados na NERC CIP (*North American Electric Reliability Corporation Critical Infrastructure Protection*) [4]: "O Hardening do sistema, também chamado de Hardening do sistema operacional, ajuda a minimizar as vulnerabilidades de segurança removendo todos os programas e utilitários de software não essenciais e instalando apenas as necessidades básicas que o computador precisa para funcionar. Embora outros programas possam fornecer recursos úteis, eles podem fornecer acesso clandestino (back-door) ao sistema e devem ser removidos para proteger o sistema."
Outra definição bastante completa pode ser encontrada em [5]: "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. Além disso, o Hardening é somente uma das medidas de segurança cibernética recomendadas e faz parte de um conjunto completo de defesa em camadas, um conceito conhecido como defesa em profundidade, onde técnicas são empregadas em conjunto para fortalecer a segurança geral do sistema e atrasar a ação do atacante."

Assim, o Hardening pode ser entendido como o processo de proteger um sistema reduzindo sua superfície de vulnerabilidade, que é maior quando um sistema executa mais funções; em princípio, um sistema de função única é mais seguro que um sistema polivalente. Partindo dessas definições e olhando o sistema sob a perspectiva de um atacante a redução das formas de ataque disponíveis se dariam, por exemplo, através de: alteração de senhas padrão e criação de senhas fortes; remoção de software desnecessário e vulnerável; remoção de usuários padrão e contas de usuário desnecessárias; desativação ou remoção de serviços e programas desnecessários como, por exemplo, protocolos vulneráveis (ex: Telnet, RSH, TFTP, HTTP) ou não utilizados, fechamento de portas não utilizadas, remoção de aplicativos não necessários para as funções críticas do ambiente; mudanças rigorosas nas permissões do sistema de arquivos e do sistema operacional; configuração de hardware segura; remoção de configurações padrão inseguras de fábrica; etc.
Utilizando e extrapolando o conceito de defesa em profundidade orientado ao processo de Hardening busca-se elevar os níveis de segurança de um sistema SAGE em multiplas camadas. O conceito de defesa em profundidade estabelece que as atividades de Hardening são necessárias em diferentes camadas para barrar a ação dos atacantes (ver Figura 1).

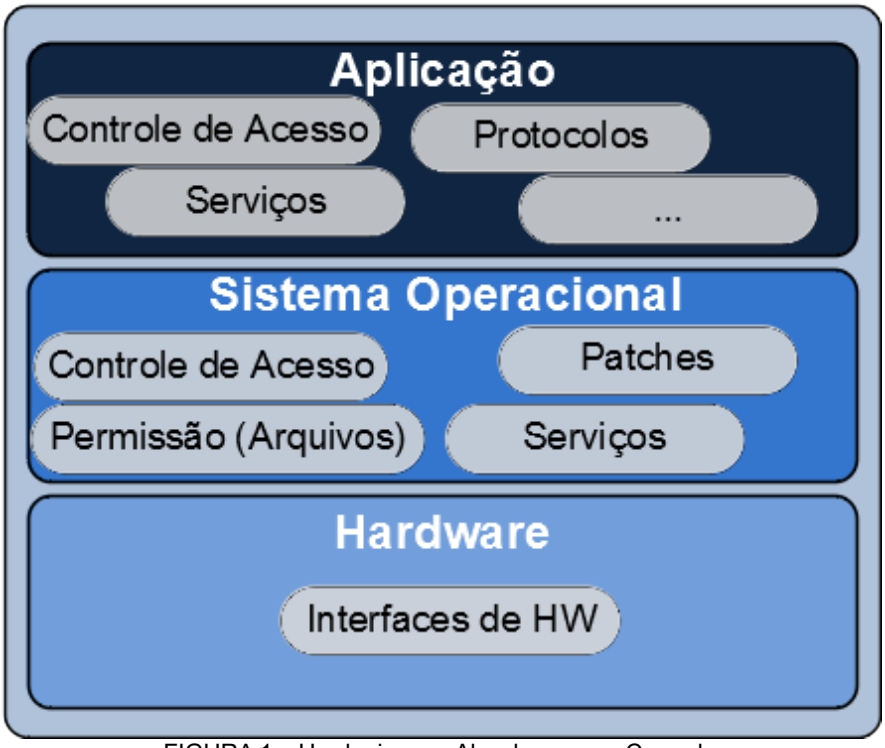

FIGURA 1 – Hardening e a Abordagem em Camadas

Camada 1: Hardware (ex: Computador Industrial): Interfaces de HW;
Camada 2: Sistema Operacional (ex: Linux): Serviços, Controle de Acesso, Atualizações (Patches), Permissões (Sistema de Arquivos e Pastas);
Camada 3: Aplicação (ex: SAGE e outras estritamente necessárias): Serviços, Controle de Acesso, Protocolos;

Começar da camada mais baixa e evoluir progressivamente até a última camada é importante porque, do contrário, uma superfície aberta para atacantes pode ser criada durante o processo de Hardening. Portanto, a restrição ou desativação de acordo com o princípio da menor funcionalidade deve ser aplicada nas três camadas: aplicativos, sistema operacional e interfaces físicas da máquina.
Interfaces físicas incluem portas, interfaces de comunicação local (Placas de rede ethernet, USB, DVD, serial, bluetooth, comunicação sem fio, etc) e interfaces de configuração local e de diagnóstico em todos os componentes e dispositivos. A utilização destas interfaces para serviço ou manutenção, deve ser especificado e restrito de acordo com a função do usuário. Todas as interfaces que não estão sendo usadas na solução devem ser removidas ou desativados e todas as interfaces de depuração e teste devem ser desativadas após o comissionamento do sistema.
A BIOS (Basic Input / Output System) também é considerada no processo de Hardening, para alterar as configurações padrão inseguras, como por exemplo, seqüência de inicialização, senha de inicialização, LAN de ativação (boot), horário do sistema, etc.
Para que o Hardening na camada de Sistema Operacional seja bem-sucedido considera-se o conceito de uma instalação mínima funcional, na qual somente as funcionalidades necessárias para a aplicação final (por exemplo, serviços necessários do sistema operacional e portas de comunicação de rede) devem estar ativadas.
O controle de acesso aos sistemas e aplicações é tratado através do conceito de gerenciamento de conta de usuários e deve ser adaptado aos requisitos do projeto. O gerenciamento de contas deve ser estabelecido com base no princípio “necessidade de saber”, ou seja, apenas às informações necessárias para executar a tarefa atribuída devem ser concedidas aos usuários dependendo do seu papel e função no sistema.
O Hardening da aplicação SAGE (Incluindo também a camada do Sistema Operacional Linux) visa garantir que todas as partes dessa solução sejam concebidas e estejam, principalmente, configuradas de forma segura.
Na prática, o Hardening garante que, em todos os sub-componentes de um sistema, somente o que é estritamente necessário para a operação e manutenção do sistema está ativado.
O Hardening tem um benefício adicional se conseguir reduzir o impacto de uma vulnerabilidade de software. Em outras palavras, um sistema com Hardening aplicado basicamente não está exposto diretamente a vulnerabilidades que afetam os protocolos desativados ou componentes de software desinstalados e, portanto, é menos provável que haja esforço e consumo de tempo para aplicação de patches e correções, uma vantagem clara em especial para as instalações legado desatualizadas e infraestruturas críticas em geral.
Entende-se que o conceito de Hardening é amplo, o que significa que todos os equipamentos de uma solução

podem e devem ser personalizados e customizados de acordo com boas práticas, recomendações e *Guidelines* de segurança cibernética para reduzir a sua superfície de ataque e aumentar a proteção geral do sistema.

4.0 - RECOMENDAÇÕES E BENCHMARK PARA HARDENING

O CIS (Center for Internet Security) [6] é uma entidade sem fins lucrativos, com visão de futuro que aproveita o poder de uma comunidade global de TI para proteger organizações públicas e privadas contra ameaças cibernéticas por meio de práticas recomendadas para proteger sistemas e dados de TI contra os ataques mais difundidos. A missão dessa organização é identificar, desenvolver, validar, promover e sustentar soluções de melhores práticas para defesa cibernética e liderar comunidades para permitir um ambiente de confiança no ciberespaço.
O CIS fornece um "Kit de Remediação" [7] para atualizar e incrementar a segurança de diversos sistemas e aplicações moldando-os de acordo com um Benchmark estabelecido. Neste trabalho foi selecionado um kit específico capaz de fortalecer e proteger um sistema operacional Linux (CentOS versão 7) através de recomendações de segurança. Os kits de remediação fornecidos pelo CIS trazem recomendações e sugestões para corrigir e atualizar o sistema operacional com multiplas medidas de segurança de uma só vez, evitando o consumo excessivo de tempo e minimizando erros humanos com implementações individuais. A aplicação dessas recomendações é feita de maneira automática através de shell script. Porém, exceções durante o projeto devem ser tratadas, mapeadas e consideradas pontualmente para que as aplicações executadas no sistema mantenham as funções necessárias e essenciais funcionando corretamente e não sejam afetadas ou bloqueadas por alguma medida de proteção incompatível presente no Benchmark.

5.0 - APLICAÇÃO DE HARDENING NO SAGE

Foi utilizada nesse trabalho, para elencar o nível de aderência às recomendações antes e após aplicação do kit de remediação no SAGE, a ferramenta CIS-CAT Pro, desenvolvida pelo CIS, que compara rapidamente a configuração de um sistema de destino às recomendações do Benchmark e informa a conformidade em uma escala de 0 a 100 do sistema Linux alvo auditado. O sistema SAGE foi auditado considerando o nível 1, cujo perfil sugere uma abordagem prática e prudente, provendo um benefício de segurança claro e aceitável, sem que haja inibição de utilidades e funcionalidades. O resultado alcançado na varredura do sistema Linux/SAGE antes de aplicar as medidas recomendadas em percentual alcançado foi de 53%, ou seja, o sistema passou por 83 testes com êxito e falhou em 75 recomendações de segurança, conforme figura abaixo (Ver Figura 2):

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Initial Setup	**15**	**17**	**0**	**0**	**15.0**	**32.0**	**47%**
1.1 Filesystem Configuration	10	9	0	0	10.0	19.0	53%
1.1.1 Disable unused filesystems	0	7	0	0	0.0	7.0	0%
1.2 Configure Software Updates	1	0	0	0	1.0	1.0	100%
1.3 Filesystem Integrity Checking	0	2	0	0	0.0	2.0	0%
1.4 Secure Boot Settings	1	2	0	0	1.0	3.0	33%
1.5 Additional Process Hardening	1	2	0	0	1.0	3.0	33%
1.6 Mandatory Access Control	0	0	0	0	0.0	0.0	0%
1.6.1 Configure SELinux	0	0	0	0	0.0	0.0	0%
1.7 Warning Banners	2	1	0	0	2.0	3.0	67%
1.7.1 Command Line Warning Banners	2	0	0	0	2.0	2.0	100%
2 Services	**28**	**6**	**0**	**0**	**28.0**	**34.0**	**82%**
2.1 inetd Services	7	0	0	0	7.0	7.0	100%
2.2 Special Purpose Services	18	4	0	0	18.0	22.0	82%
2.2.1 Time Synchronization	1	1	0	0	1.0	2.0	50%
2.3 Service Clients	3	2	0	0	3.0	5.0	60%
3 Network Configuration	**5**	**14**	**0**	**0**	**5.0**	**19.0**	**26%**
3.1 Network Parameters (Host Only)	0	2	0	0	0.0	2.0	0%
3.2 Network Parameters (Host and Router)	0	8	0	0	0.0	8.0	0%
3.3 IPv6	0	0	0	0	0.0	0.0	0%
3.4 TCP Wrappers	4	1	0	0	4.0	5.0	80%
3.5 Uncommon Network Protocols	0	0	0	0	0.0	0.0	0%
3.6 Firewall Configuration	1	3	0	0	1.0	4.0	25%
4 Logging and Auditing	**4**	**3**	**0**	**0**	**4.0**	**7.0**	**57%**
4.1 Configure System Accounting (auditd)	0	0	0	0	0.0	0.0	0%
4.1.1 Configure Data Retention	0	0	0	0	0.0	0.0	0%
4.2 Configure Logging	4	3	0	0	4.0	7.0	57%
4.2.1 Configure rsyslog	1	2	0	0	1.0	3.0	33%
4.2.2 Configure syslog-ng	2	0	0	0	2.0	2.0	100%
5 Access, Authentication and Authorization	**6**	**30**	**0**	**0**	**6.0**	**36.0**	**17%**
5.1 Configure cron	1	7	0	0	1.0	8.0	12%
5.2 SSH Server Configuration	1	14	0	0	1.0	15.0	7%
5.3 Configure PAM	1	3	0	0	1.0	4.0	25%
5.4 User Accounts and Environment	3	5	0	0	3.0	8.0	38%
5.4.1 Set Shadow Password Suite Parameters	2	3	0	0	2.0	5.0	40%
6 System Maintenance	**25**	**5**	**0**	**0**	**25.0**	**30.0**	**83%**
6.1 System File Permissions	9	2	0	0	9.0	11.0	82%
6.2 User and Group Settings	16	3	0	0	16.0	19.0	84%
Total	**83**	**75**	**0**	**0**	**83.0**	**158.0**	**53%**

FIGURA 2 – Nível de Conformidade com o CIS Benchmark de Hardening antes da aplicação das recomendações

O resultado alcançado nessa primeira auditoria foi surpreendente, sabendo-se que muitos sistemas e aplicativos de "prateleira" sem nenhuma configuração de segurança adicional raramente alcançam um nível de segurança num patamar acima dos 50%.
O próximo passo foi executar o kit de remediação via shell script no servidor SAGE para que as medidas de segurança sejam aplicadas automaticamente em quase toda a totalidade. Algumas medidas sugeridas exigem

configuração manual, portanto não são configuradas pelo script e serão tratadas como exceção neste trabalho, por exigirem um esforço manual e horas adicionais de parametrização. O intuito deste trabalho é sugerir recomendações de segurança que sejam facilmente aplicáveis sem que haja um esforço significativo de engenharia e consequentemente custos altos envolvidos nos projetos.
Após aplicado o kit de remediação os resultados alcançados chegaram a um patamar de segurança elevado, com um percentual de 84%, conforme figura abaixo (Ver Figura 3):

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Initial Setup	**26**	**6**	**0**	**0**	**26.0**	**32.0**	**81%**
1.1 Filesystem Configuration	18	1	0	0	18.0	19.0	95%
1.1.1 Disable unused filesystems	7	0	0	0	7.0	7.0	100%
1.2 Configure Software Updates	1	0	0	0	1.0	1.0	100%
1.3 Filesystem Integrity Checking	1	1	0	0	1.0	2.0	50%
1.4 Secure Boot Settings	1	2	0	0	1.0	3.0	33%
1.5 Additional Process Hardening	3	0	0	0	3.0	3.0	100%
1.6 Mandatory Access Control	0	0	0	0	0.0	0.0	0%
1.6.1 Configure SELinux	0	0	0	0	0.0	0.0	0%
1.7 Warning Banners	2	1	0	0	2.0	3.0	67%
1.7.1 Command Line Warning Banners	2	0	0	0	2.0	2.0	100%
2 Services	**32**	**2**	**0**	**0**	**32.0**	**34.0**	**94%**
2.1 inetd Services	7	0	0	0	7.0	7.0	100%
2.2 Special Purpose Services	20	2	0	0	20.0	22.0	91%
2.2.1 Time Synchronization	2	0	0	0	2.0	2.0	100%
2.3 Service Clients	5	0	0	0	5.0	5.0	100%
3 Network Configuration	**11**	**8**	**0**	**0**	**11.0**	**19.0**	**58%**
3.1 Network Parameters (Host Only)	0	2	0	0	0.0	2.0	0%
3.2 Network Parameters (Host and Router)	6	2	0	0	6.0	8.0	75%
3.3 IPv6	0	0	0	0	0.0	0.0	0%
3.4 TCP Wrappers	4	1	0	0	4.0	5.0	80%
3.5 Uncommon Network Protocols	0	0	0	0	0.0	0.0	0%
3.6 Firewall Configuration	1	3	0	0	1.0	4.0	25%
4 Logging and Auditing	**5**	**2**	**0**	**0**	**5.0**	**7.0**	**71%**
4.1 Configure System Accounting (auditd)	0	0	0	0	0.0	0.0	0%
4.1.1 Configure Data Retention	0	0	0	0	0.0	0.0	0%
4.2 Configure Logging	5	2	0	0	5.0	7.0	71%
4.2.1 Configure rsyslog	1	2	0	0	1.0	3.0	33%
4.2.2 Configure syslog-ng	2	0	0	0	2.0	2.0	100%
5 Access, Authentication and Authorization	**33**	**3**	**0**	**0**	**33.0**	**36.0**	**92%**
5.1 Configure cron	7	1	0	0	7.0	8.0	88%
5.2 SSH Server Configuration	14	1	0	0	14.0	15.0	93%
5.3 Configure PAM	3	1	0	0	3.0	4.0	75%
5.4 User Accounts and Environment	8	0	0	0	8.0	8.0	100%
5.4.1 Set Shadow Password Suite Parameters	5	0	0	0	5.0	5.0	100%
6 System Maintenance	**25**	**5**	**0**	**0**	**25.0**	**30.0**	**83%**
6.1 System File Permissions	9	2	0	0	9.0	11.0	82%
6.2 User and Group Settings	16	3	0	0	16.0	19.0	84%
Total	**132**	**26**	**0**	**0**	**132.0**	**158.0**	**84%**

FIGURA 3 – Nível de Conformidade com o CIS Benchmark de Hardening após a aplicação das recomendações

NOTA: Detalhes sobre cada recomendação, com a descrição, fundamentação e orientação de como aplicá-las no sistema podem ser obtidas no site do CIS [8].

Percebe-se que para cada tipo e camada de Hardening no dispositivo, geralmente há muitas opções de configuração, especialmente para as recomendações associadas aos sistemas operacionais. Para evitar configurações incorretas, é importante usar ferramentas automáticas para configurar e para verificar se as configurações estão corretas após o processo de aplicação. Um outro fator muito importante é garantir que testes pontuais e frequentes sejam realizados durante todo o processo de Hardening para garantir que todas as funcionalidades necessárias ou críticas ao funcionamento correto do sistema não sejam afetadas pelas medidas aplicadas. Levando em consideração o risco de acidentalmente bloquear ou tornar indisponível alguma função essencial do sistema recomenda-se aplicar as recomendações de Hardening desde o princípio, durante a fase de implementação e parametrização inicial dos equipamentos do projeto, garantindo tempo hábil para investigação e ajuste de alguma medida caso necessário. Ferramentas automáticas para verificação da correta configuração do sistema assim como testes funcionais e de performance devem ser aplicados durante as fases de validação, aceitação em fábrica e implantação do sistema em campo. Por fim, todas as medidas aplicadas devem ser documentadas e entregues ao cliente final que irá operar o sistema no encerramento do projeto.

6.0 - CLASSIFICAÇÃO DE VULNERABILIDADES NO SAGE SEM O HARDENING APLICADO

As vulnerabilidades de um sistema podem se originar de uma má configuração, falhas de hardwares ou softwares ou erros de codificação dos desenvolvedores. A mesma vulnerabilidade, identificada por diferentes fontes, terá sempre uma identificação única “CVE” (*Common Vulnerabilities and Exposures*), cujo objetivo é padronizar a descrição das ameaças conhecidas e auxiliar administradores de sistema na aplicação das correções pertinentes. Os registros de CVE formam uma base de dados pública sobre falhas de segurança e são mantidos pela “Mitre corporation” [9] desde 1999 com a colaboração de diversas entidades como instituições acadêmicas, governos, fornecedores de ferramentas comerciais e especialistas de segurança cibernética.
As vulnerabilidades existentes no servidor SAGE, antes da aplicação do Hardening, são descobertas e listadas através do scanner OpenVAS (*Open Vulnerability Assessment System*) [10], uma ferramenta mantida pela Greenbone Networks desde 2009. A seguir é demonstrada a exposição à vulnerabilidades no servidor SAGE alvo, sem as medidas de hardening aplicadas, de acordo com a classificação de vulnerabilidades NVTs (Network Vulnerabilities Tests), totalizando 97 (ver Figura 4) e de CVEs, totalizando 29 (ver Figura 5).

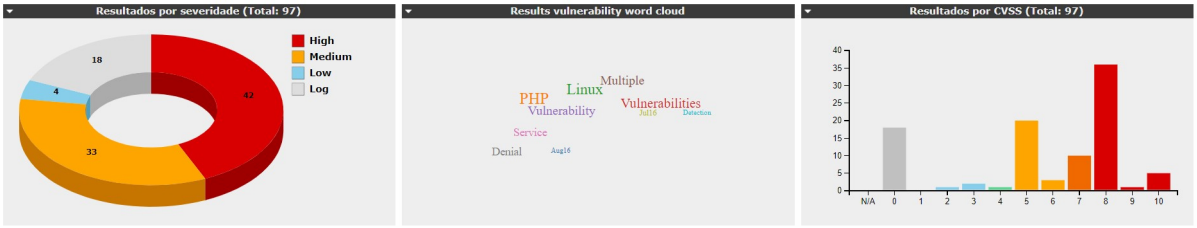

FIGURA 4 – OpenVAS NVTs (Network Vulnerabilities Tests) no servidor SAGE

FIGURA 5 – OpenVAS CVE (Common Vulnerabilities and Exposures) no servidor SAGE

Observa-se que dos CVEs encontrados 7 são classificadas com grau de severidade alto e 21 médio. Uma vez elencadas as vulnerabilidades é possível explorá-las facilmente com o software Metasploit (Um projeto de segurança da informação com o objetivo de análise de vulnerabilidades de segurança) [11].
Por serem muito críticas, essas vulnerabilidades são de fácil exploração e podem gerar um alto impacto, culminando, por exemplo, em negação de serviço, abuso de direitos, ganho de acesso à máquina alvo, execução de código malicioso, etc.

Um sistema após a aplicação do Hardening apresenta um número significativamente menor de vulnerabilidades, cuja criticidade é menos relevante. Portanto a facilidade e probabilidade de exploração caem drasticamente, tornando o sistema menos susceptível a ataques.

7.0 - CONCLUSÃO

O trabalho traz a tona a fragilidade de um sistema SAGE/Linux sem mecanismos de Hardening e sem customizações adequadas com o foco em segurança cibernética. A preocupação é iminente estando claras as possibilidades de fácil exploração de um componente fundamental largamente utilizado em infraestruturas críticas de energia do Brasil.

A aplicação dos conceitos e recomendações de Hardening apresentados nesse trabalho com foco no SAGE/Linux mostra-se possível, eficiente e extremamente viável, sendo fundamental para a mitigação de ataques, redução da superfície de exposição desses sistemas e na limitação de possíveis danos e riscos aos sistemas críticos de energia.

Demostrou-se também que o Hardening aplicado em várias camadas reduz as opções de acesso e, consequentemente, reduz consideravelmente a superfície exposta do sistema SAGE, limitando as possibilidades de acesso indevido e ataque ao dispositivo, porem sem limitar de maneira alguma as suas funcionalidades.
O Hardening é, portanto, um mecanismo bastante eficaz que requer um esforço bastante aceitável de implementação, com consumo de horas de engenharia para definições, planejamento, implementação e posterior manutenção. Pensando na importância que os sistemas críticos em questão representam ao país e nas consequências negativas advindas do enorme impacto que um possível ataque à esses sistemas trariam, não há dúvida de que uma abordagem efetiva e viável é a prevenção através da utilização de técnicas e conceitos apresentados durante esse trabalho. Por fim, o Hardening é um mecanismo cujo conceito deve ser expandido e extrapolado para todos os componentes que fazem parte do sistema crítico de energia em questão, principalmente para aqueles que não são concebidos com o foco em segurança cibernética e cuja importância no sistema tem grande representatividade. Portanto, aconselha-se expandir o conceito de Hardening priorizando os elementos mais críticos, aqueles que podem se tornar um vetor de ataque e trazer prejuízos e indisponibilidade à solução quando afetados. Para garantir um alto nível de segurança de toda solução, é importante focar individualmente em todas as peças e produtos que a compõe e garantir que sejam concebidas e configuradas de maneira segura, pois uma vez que a segurança geral depende de todos os componentes que a compõe, os atacantes geralmente exploram as partes não protegidas ou negligenciadas do ponto de vista de segurança cibernética.

Portanto, a abordagem sugerida provê de forma simples e completa uma estratégia para melhoria do nível de segurança geral sistêmica e auxilia na implementação de um sistema SAGE/Linux robusto, seguro e funcional.
O Hardening é um mecanismo de segurança muito importante, mas que por si só não é suficiente do ponto de vista holístico, onde a segurança cibernética deve ser vista de um foco mais amplo que considera outros aspectos tecnológicos e um conjunto completo de medidas técnicas empregadas em camadas (defesa em profundidade), processos bem definidos e estruturados além de conscientização do corpo técnico envolvido.

Um fator fundamental que não pode ser negligenciado tratando-se de Hardening na área computacional é o pilar conhecido como “Peopleware”, ou seja, a parte humana, o usuário que irá configurar, operar e manter o sistema. Para que as pessoas não sejam o elo mais fraco de uma cadeia que é composta por processos e produtos (tecnologia empregada) e não comprometam a proteção geral do sistema, a conscientização através de treinamentos e simulações deve ser tratada com prioridade, pois de nada adianta criar um sistema robusto que seja colocado em risco quando acessado e operado por pessoas não capacitadas.

8.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) SAGE (Sistema Aberto de Gerenciamento de Energia). <sage.cepel.br/index.php/pt/sage/visao-geral>. Acesso em: 15/11/2018.

(2) CEPEL (Centro de Pesquisas de Energia Elétrica). </www.cepel.br/pt_br/>. Acesso em: 15/11/2018.

(3) NIST (National Institute of Standards and Technology). <csrc.nist.gov/glossary/term/Hardening>. Acesso em: 15/11/2018.

(4) NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) <www.nerc.com/pa/stand/Pages/default.aspx>. Acesso em: 15/11/2018.

(5) Franceschett, André L., "Conceito de Defesa em Profundidade Aplicada na Segurança Cibernética de Sistemas de Automação de Energia", XXIV SNPTEE, 2017.

(6) CIS (Center for Internet Security). <www.cisecurity.org/>. Acesso em: 15/11/2018.

(7) CIS Remediation Content (CentOS Linux 7). <www.cisecurity.org/cis-securesuite/cis-securesuite-remediation-content/>. Acesso em: 15/11/2018.

(8) CIS Benchmarks (CentOS Linux). <www.cisecurity.org/cis-benchmarks/>. Acesso em: 15/11/2018.

(9) Mitre Database (CVEs). <cve.mitre.org>. Acesso em: 15/11/2018.

(10) OpenVAS (Open Vulnerability Assessment System). <www.openvas.org/>. Acesso em: 15/11/2018.

(11) Metasploit (Open Vulnerability Assessment System). <www.metasploit.com/>. Acesso em: 15/11/2018.

9.0 - 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); Cyber Security Expert, Siemens Power Academy – Alemanha (2017)

Experiência Profissional:
Iniciou a carreira como Arquiteto e Desenvolvedor de Software no Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) nos anos de 2007. Engenheiro de Desenvolvimento de Sistemas Sênior na Siemens desde 2010 (Jundiaí/SP) atua em projetos de proteção e controle de sistemas de energia de concessionárias e indústrias. Faz parte da equipe de Engenharia de Aplicação, suportando tecnicamente as áreas de Vendas, Projetos e Comissionamento. É responsável por temas técnicos relacionados a redes de computadores, protocolos, sistemas SCADA, SAGE e referência em Segurança Cibernética na Siemens. É membro ativo do CIGRÉ (GT B5-01 "Aplicações da Norma IEC 61850 - Sistemas de Automação Operando com Redes de Comunicação" e GT D2 "Grupo Técnico de Segurança Cibernética"). Atualmente atua junto à Siemens Alemanha em projetos pioneiros de P&D em Segurança Cibernética para Sistemas de Automação de Subestações e é instrutor de Segurança Cibernética certificado pela Siemens Power Academy Alemanha.