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

Avaliação de Vulnerabilidades Cibernéticas Para Acesso Remoto aos IEDs Utilizando Árvore de Ataques

MAURICIO SILVEIRA(1); FELIPE MELCHERT(1); EDUARDO GONÇALVES(1)
Schweitzer Engineering Laboratories(1);

RESUMO

Este artigo apresenta como desenvolver técnicas de acesso seguras aos IEDs (Intelligent Electronic Devices) de proteção para segregar a rede operativa da subestação da rede corporativa de acesso remoto. A implementação possibilita o acesso remoto seguro por meio de autenticação, autorização e rastreabilidade de usuários, controle de acesso centralizado e gerenciamento de senhas dos IEDs. A técnica é fundamentada na conexão indireta dos IEDs de proteção através de proxies de acessos seguros e a construção de perímetros de segurança cibernéticas utilizando ESP (Electronic Security Perimeters). Ao final do artigo é apresentado um método de análise comparativa entre os métodos de acesso direto e o método de acesso utilizando servidores proxies. Através desse artigo busca-se demonstrar os requisitos mínimos que um Proxy de IEDs de proteção deve possuir, assim como demonstrar topologias de redes seguras para o acesso remoto aos IEDs de proteção e controle.

As conexões remotas aos IEDs de proteção trazem diversas vantagens, como: download de oscilografias e eventos, verificação e modificação de ajustes, verificação de sequencial de eventos entre outros benefícios. O acesso remoto entre os centros de engenharia e os IEDs das subestações normalmente é feito através de infraestruturas de redes compartilhadas, como a internet, e portanto, é um canal de comunicação não seguro e facilitador para ataques cibernéticos. Além do risco cibernético, o risco humano também é presente. A falta de controle de acesso e rastreabilidade dos usuários dos IEDs de proteção é um risco e pode ser mitigado através da criação de perfis e níveis de acesso para cada tipo de usuários gerenciados pelo Proxy de acesso.

A utilização de proxies para conexões indiretas dos IEDs de proteção pode trazer diversos benefícios capazes de solucionar as lacunas de segurança cibernética, além de minimizar e rastrear o risco humano envolvido na operação remota dos IEDs de proteção. O Proxy funciona como uma porta de acesso ao perímetro cibernético delimitado por um ESP, através do qual é possível autenticar os usuários e assim autorizar, bloquear e rastrear operações efetuadas nos IEDs de proteção. A utilização de proxies e redes ESP também facilita a configuração de firewalls e VPNs (Virtual Private Networks) garantindo uma camada extra de segurança cibernética nas subestações de energia elétrica. Além disso, possibilita monitoramento dos acessos, identificação de tentativas de invasão de maneira centralizada e a possibilidade de responsabilização de alterações feitas durante um acesso específico.

A técnica de conexão indireta já é amplamente utilizada para a conexão entre subestações e o sistema SCADA e efetuada através dos gateways de comunicação, porém não é aplicada para o acesso remoto aos IEDs de proteção que muitas vezes é feita de forma direta ou utilizando computadores não auditados periodicamente, acarretando em riscos para a operação e confiabilidade dos dados do sistema elétrico de potência. Diversas diretrizes internacionais, como a NERC/CIP recomendam propostas semelhantes de arquiteturas de redes seguras. O artigo utiliza uma árvore de ataques para avaliar, de forma comparativa, o grau de segurança cibernética entre as arquiteturas mais comuns para o acesso remoto aos IEDs.
PALAVRAS-CHAVE

Segurança Cibernética, Árvore de Ataques, DMZ, IEDs, Subestação

(*) Avenida Pierre Simon de Laplace, n° 633 – TechnoPark – CEP 13.069-32 - Campinas, SP, – Brasil
Tel: (+55 19) 3515-2000 – Fax: (+55 19) 3515-2001 – Email: marketing_br@selinc.com

1.0 - INTRODUÇÃO

1.1 Análise de vulnerabilidade utilizando árvore de ataques

Uma árvore de ataque é um método de visualização gráfica capaz de conectar e mensurar as ameaças de um sistema cibernético [1] [2] [3]. A árvore de ataques consiste em uma arquitetura hierárquica capaz de estruturar os riscos e ameaças em um sistema de defesa cibernético. A Figura 1 apresenta a árvore de ataques utilizada para o estudo de vulnerabilidade deste artigo. Na parte superior da árvore de ataques estão os objetivos finais capazes de corromper os requisitos de segurança (confidencialidade, integridade e disponibilidade) cibernéticos do sistema. Para cada evento da árvore de ataque, existem métodos capazes de mitigar e minimizar os efeitos dos eventos de ataques. Os métodos de mitigação são implementados de acordo com a arquitetura, tecnologia, política de senhas e treinamento coorporativo e podem ter pesos diferentes de acordo com o nível de segurança cibernético desejado.

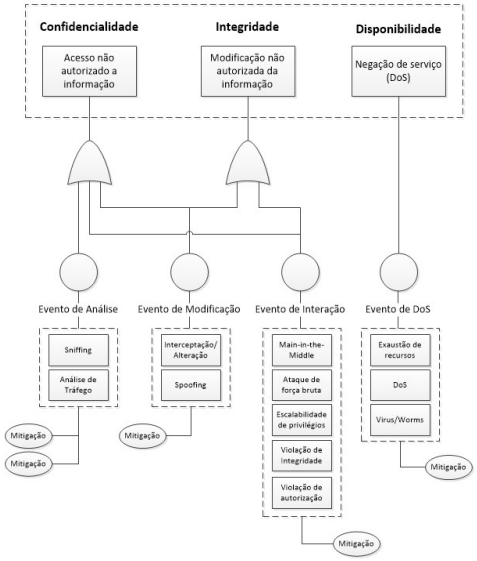


FIGURA 1 – Árvore de ataques cibernéticos.

2.0 - ARQUITETURAS DE REDES SEGURAS

2.1 Arquiteturas de redes de acesso direto e utilizando hosts de segurança

A integração da tecnologia Ethernet nas subestações de energia pode trazer diversos benefícios e facilidades na operação e coleta de informação dos IEDs de proteção. Através da rede Ethernet é possível coletar oscilografias, modificar ajustes e efetuar comandos remotos diretamente dos centros de engenharia. A conexão entre os centros de engenharia e as subestações é feita através de roteadores, que normalmente incorporam as funções de firewall para a permissão ou bloqueio de pacotes, como mostrado na Figura 2 (a). Porém, a utilização de roteadores e firewalls integrados em um único equipamento pode sofrer de várias insuficiências, sendo a primeira delas a inexistência de formas de autenticação e, portanto, sem registros de quem está tentando se conectar à rede. A performance do roteamento também é prejudicada pois o roteador é obrigado a abrir e inspecionar todos os pacotes, causando atrasos na entrega dos dados e prejudicando o desempenho da rede de tempo real.

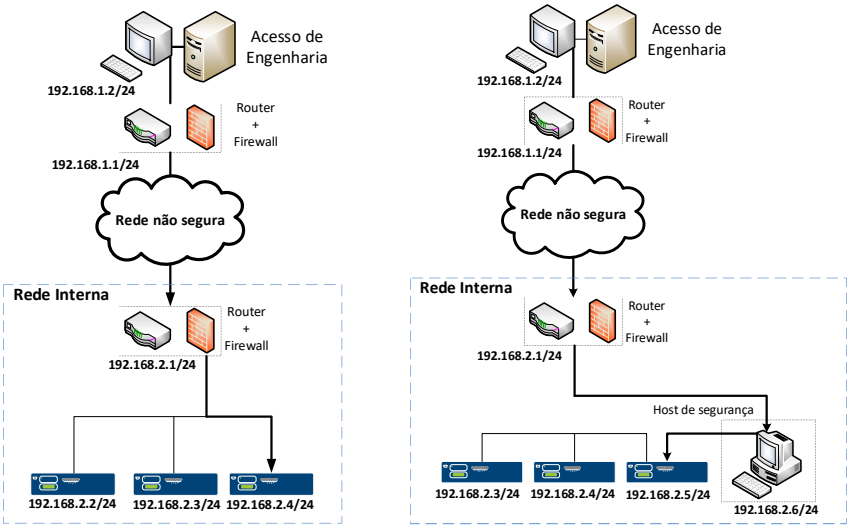


FIGURA 2 – (a) Método de Acesso direto, (b) Método de acesso indireto utilizando um host de segurança.

A arquitetura com a utilização de um host de segurança ou host de blindagem [4], como mostrado na Figura 2 (b), desacopla o mecanismo de inspeção de pacotes desempenhado pelo roteador através da inserção de um equipamento de segurança. A segurança primária ainda é fornecida pelo firewall do roteador, porém o host de segurança é capaz de organizar as informações em ambas as direções, concentrando assim o acesso dos clientes aos IEDs em um único ponto de conexão. O host de segurança é uma máquina segura e constantemente auditada conectada na mesma rede dos outros IEDs e possibilita a inspeção profunda de pacotes, inclusive das camadas de aplicação. Uma das grandes vantagens da utilização de hosts de segurança é com a segurança cibernética, a configuração dos firewalls se torna basicamente um descarte de todos os pacotes, exceto os pacotes referenciados ao host de segurança. Entretanto, a utilização de hosts de segurança não define um perímetro de rede seguro, pois os equipamentos (inclusive o host de segurança) são conectados diretamente à rede não segura fornecendo um meio de acesso à rede, que deveria ser isolada.

2.2 Arquiteturas de redes de acesso utilizando perímetros eletrônicos seguros (ESP)

Uma estratégia popular para separar as redes das subestações das redes não seguras, como a internet, é elevar a rede de roteamento, possibilitando que todo o tráfego de entrada e saída transite em uma região específica e isolada, como mostrado na Figura 3. A elevação da rede de roteamento possibilita a criação de perímetros de segurança seguros ou ESP. O ESP é uma região intermediária, entre zonas distintas que devem coexistir em proximidade. Ao criar um perímetro cibernético a partir de ESP, são intrinsecamente adicionadas múltiplas camadas de segurança à rede de informação [5]. A primeira delas traduz-se na existência de pelo menos dois roteadores envolvidos na proteção da rede interna. O primeiro roteador (roteador exterior) é situado entre o gateway e a rede não segura. O segundo roteador (roteador interior) entre o gateway e a rede interna. As disposições dos roteadores delimitam um perímetro de rede ou ESP. A rede perimetral, compartilhada entre os dois roteadores, não deve possuir nenhum outro dispositivo, a não ser os equipamentos de roteamento e os equipamentos de confiança, como os hosts de segurança, o que possibilita um ajuste fino da rede de acesso aos IEDs de proteção.

Através da ESP é possível controlar de forma multidirecional e precisa todo o tráfego de entrada e saída da rede interna. No exemplo da Figura 3 (a), é possível ajustar o firewall interior para bloquear todos os pacotes de saída da rede interna para o roteador exterior, e também bloquear todo tráfego de entrada advindo do roteador exterior. Isso possibilita que todo o fluxo de informação seja processado sempre em duas etapas. Dessa forma, os clientes externos a ESP sempre se comunicam com as máquinas de interface (host de segurança e roteadores) para efetuar a troca de informação com os servidores da ESP. Os clientes, internos a ESP, também se comunicam de forma indireta com os servidores da rede externa a ESP. A comunicação em etapas, realizada por equipamentos intermediários traz diversos benefícios para manutenção como: rastreabilidade e controle de acesso centralizado aos equipamentos.

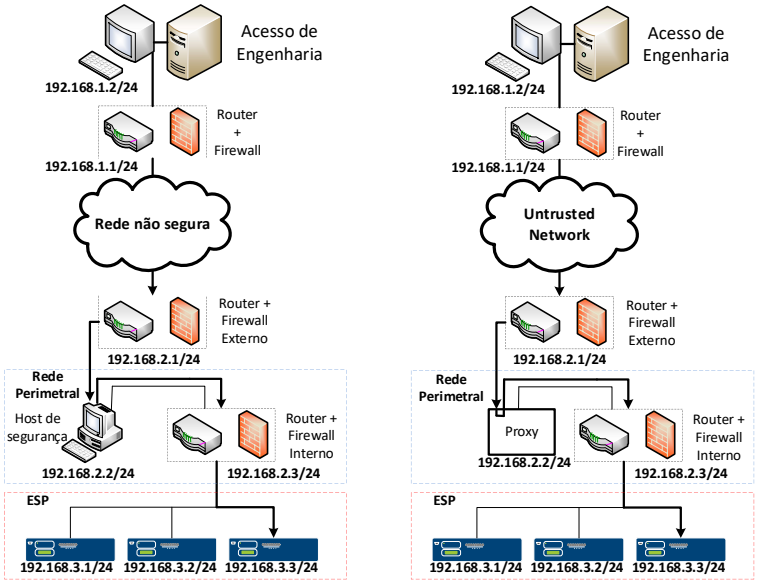


FIGURA 3 – (a) Segregação da rede de acesso utilizando ESP, (b) Método de acesso utilizando servidores proxies

2.3 Arquiteturas de redes de acesso utilizando servidores Proxies

Um servidor proxy é um host de segurança, porém um host de segurança não é necessariamente um proxy. Os servidores proxies possuem funções semelhantes aos hosts de segurança, e muitas vezes as funcionalidades de ambos se sobrepõem. O host de segurança é um computador seguro que atua como uma área de preparação para a informação que está em trânsito e normalmente é o ponto de entrega da informação. Os servidores proxies funcionam mais como um ponto de controle do que como um ponto de entrega. O proxy atua dentro da rede perimetral como um espelho da aplicação do servidor ou do cliente. Portanto, o envolvimento do proxy é transparente para os dispositivos finais. A Figura 3 (b) exemplifica a conexão entre um cliente e um servidor através de um proxy de acesso. O acesso é feito de forma transparente através do proxy que gerencia os serviços de acesso aos servidores.

3.0 - ANÁLISE DE VULNERABILIDADE CIBERNÉTICA PARA ACESSO AOS IEDS DE PROTEÇÃO

3.1 Índice de segurança cibernética condicional: β

O índice de segurança cibernética condicional é uma medida preliminar que avalia o grau de segurança cibernética de um sistema a partir de hipóteses determinadas e customizadas para cada sistema. Para o caso de acesso remoto aos IEDs o índice de segurança condicional é baseado em três hipóteses:

1. O sistema não possui nenhuma evidência cibernética de intrusão;
2. O sistema é auditado frequentemente;
3. Existência de pelo menos uma política de senhas adotada.

O índice β pode assumir os valores de 0, 5 e 10, onde o valor 0 representa sistema menos vulnerável e o valor 10 o sistema mais vulnerável. O índice β é determinado de acordo com as hipóteses mostradas na Tabela 1.

Tabela 1 – Avaliação do índice de segurança cibernética

Condições Satisfeitas	Valor de β	Descrição
(1) & (2) & (3)	0	Todas as hipóteses foram satisfeitas, existem implementações de contramedidas avançadas e uma boa política de senhas.
(1) & (2) ou (2) & (3) ou (1) & (3)	5	Pelo menos duas condições satisfeitas.
(1) ou (2) ou (3) ou (nenhuma)	10	Apenas uma condição satisfeita ou nenhuma condição.

3.2 Índice vulnerabilidade cibenética: α

O índice de vulnerabilidade é uma combinação métrica baseada no sistema de contagem CVSS (Common Vulnerability Scoring System) (6) e métricas operacionais relacionadas com o sistema em avaliação. Para o

estudo de acesso remoto aos IEDs de proteção este artigo avalia quatro tipos de eventos cibernéticos: análise, modificação, interação e DoS (negação de serviço). O índice α é calculado de acordo com a equação 1:

Equação 1 – Cálculo do índice α.

$$\alpha = \frac{\sum_{i=1}^{n} CVSS}{n} + \frac{\sum_{i=1}^{n} InterrupçãodeEnergia(horas)}{n} \quad (1)$$

A primeira parcela da equação representa o grau de severidade da vulnerabilidade explorada. A segunda parcela representa a métrica operacional, que é o resultado caso o ataque cibernético seja bem-sucedido. Neste artigo o impacto da segunda parcela é avaliado através da interrupção causada no fornecimento de energia, medida em horas. As tabelas 2, 3, 4 e 5 descrevem as vulnerabilidades para cada caso escolhido. Os valores de CVSS foram obtidos através da calculadora diponivel em (7). Os parametros básicos foram determinados de acordo com a complexidade da vulnerabilidade.

Tabela 2 – Avaliação do índice de vulnerabilidade cibernética para o evento de análise.

Evento de Análise	CVSS	Interrupção de Energia (horas)	Descrição
Sniffing Protocolos de acesso	7,5	0	Captura e análise de informações como senhas, medições e ajustes.
Sniffing Transferência de arquivos	5,9	0	Captura e análise de informações como ajustes e oscilografias.
Índice α total	6,7		O índice representa a severidade de um evento de análise para o acesso remoto aos IEDs.

Tabela 3 – Avaliação do índice de vulnerabilidade cibernética para o evento de modificação.

Evento de modificação	CVSS	Interrupção de Energia (horas)	Descrição
Spoofing de comandos	8,5	5	Falsificação de comandos através de injeção de trafégo na rede.
Índice α total	13,5		O índice representa a severidade de um evento de modificação para o acesso remoto aos IEDs.

Tabela 4 – Avaliação do índice de vulnerabilidade cibernética para o evento de interação.

Evento de modificação	CVSS	Interrupção de Energia (horas)	Descrição
Ataque de força bruta em senhas	8,1	0	Ação repetitiva através de tentativa e erro de combinações de usuários e senhas.
Escalabilidade de privilégios	7,3	0	Ganho de acesso a níveis de segurança elevados.
Índice α total	7,7		O índice representa a severidade de um evento de interação para o acesso remoto aos IEDs.

Tabela 5 – Avaliação do índice de vulnerabilidade cibernética para o evento de DoS.

Evento de DoS	CVSS	Interrupção de Energia (horas)	Descrição
Exaustão de recursos	8,2	0	Ataque de negação de serviço ou conectividade.
Virus / Worms	7,5	0	Código malicioso.
Índice α total	7,85		O índice representa a severidade de um evento de DoS para o acesso remoto aos IEDs.

3.3 Índice mitigação cibenética: Ω

O índice de mitigação cibernética é uma métrica composta através da resiliência do sistema a ataques cibernéticos e sua complexidade de implementação. Os índices são mensurados através de 3 níveis: baixo, médio e alto, vide tabela 6:

Tabela 6 – Valores dos níveis de mitigação cibernética

Nível	Valor
Baixo	0 – 3,3
Médio	3,3 – 6,6

Alto	6,6 – 10

O índice de mitigação é calculado através da equação 2:

Equação 2 – Cálculo do índice Ω.

$$\Omega = Resiliência - Complexidade \quad (2)$$

O valor Ω = 0 representa o sistema mais vulnerável e o valor Ω = 10, o sistema menos vulnerável. As seguintes contramedidas serão adotadas como possiveis soluções: política de senhas, autenticação, autorização, e rastreabilidade de usuários, ESP, VPN, e proteção contra malware. A resiliência é estimada através de fatores como dificuldade de quebra de sigilo e o historico de implementações. Como exemplo: a probabilidade de quebra de uma senha complexa de 12 caracteres por um ataque de força bruta é estimada em algumas centanas de anos, o que torna a medida consideravelmente segura, porém o nível de complexidade é grande devido ao esforço de manuntenção.

Tabela 7 – Avaliação do índice de mitigação cibernética para a política de senhas.

Política de senhas	Resiliência	Complexidade	Ω	Descrição
Ausência de senha	0	0	0	O sistema não possui senha.
Senha padrão	3	0	3	O sistema utiliza a senha padrão dos equipamentos.
Senha complexa	9	6,6	2,4	O sistema utiliza uma senha complexa de 12 caracteres.
Gerenciamento de senhas	10	3,3	6,7	O sistema possui um sistema automático de gerenciamento de senhas complexas.

Tabela 8 – Avaliação do índice de mitigação cibernética para a autenticação de usuários.

Autenticação de usuários	Resiliência	Complexidade	Ω	Descrição
Usuário padrão	0	0	0	O sistema de acesso utiliza usuário padrão.
Usuário não padrão	6,6	3,3	3,3	O sistema de acesso utiliza usuário não padrão.
Usuário autenticado	10	3,3	6,7	O sistema possui sistema de autenticação de usuários (ex: LDAP e RADIUS)

Tabela 9 – Avaliação do índice de mitigação cibernética para a autorização de usuários.

Autorização de usuários	Resiliência	Complexidade	Ω	Descrição
Nível de acesso padrão	0	0	0	O sistema possui nível de acesso padrão.
Gerenciamento de nível de acesso	6,6	3,3	3,3	O sistema possui políticas de níveis de acesso de acordo com a função e cargo.

Tabela 10 – Avaliação do índice de mitigação cibernética para a rastreabilidade de usuários.

Rastreabilidade	Resiliência	Complexidade	Ω	Descrição
Rastreabilidade descentralizada	3,3	0	3,3	Rastreabilidade descentralizada. Ex: utilização de sequencial de eventos a nível de IEDs.
Rastreabilidade centralizada	10	3,3	6,6	Rastreabilidade de usuário e datas de acesso utilizando uma plataforma centralizada.

Tabela 11 – Avaliação do índice de mitigação cibernética para a ESP.

ESP	Resiliência	Complexidade	Ω	Descrição

Perímetro cibernético externo	3.3	0	3,3	O ESP é definido por apenas um roteador/firewall de borda.
Perímetro cibernético externo e interno	8	3,3	4,7	O ESP possui um firewall externo e um interno, restringindo o acesso e criando uma camada extra de segurança.
Perímetro cibernético externo, interno e monitoramento	10	3,3	6,7	O ESP é ligado a uma central de segurança. Ex: SIEM.

Tabela 12 – Avaliação do índice de mitigação cibernética para VPN.

VPN	Resiliência	Complexidade	Ω	Descrição
Ausência de VPN	0	0	0	O sistema não possui VPN.
VPN utilizando chave simétrica	8	3,3	4,7	O sistema utiliza criptografia através de compartilhamento de chave simétrica
VPN utilizando chave assimétrica	10	3,3	6,7	O sistema utiliza criptografia através do compartilhamento de chave assimétrica.

Tabela 13 – Avaliação do índice de mitigação cibernética para proteção contra malware.

Proteção contra malware	Resiliência	Complexidade	Ω	Descrição
Ausência de proteção	0	0	0	Não possui proteção contra malware.
Proteção nos dispositivos finais	10	6,6	3,3	A proteção contra malware é realizada nos hosts.
Proteção nos dispositivos intermediários	10	3,3	6,6	A proteção é realizada nos dispositivos de acesso indireto como proxies, firewalls e roteadores.

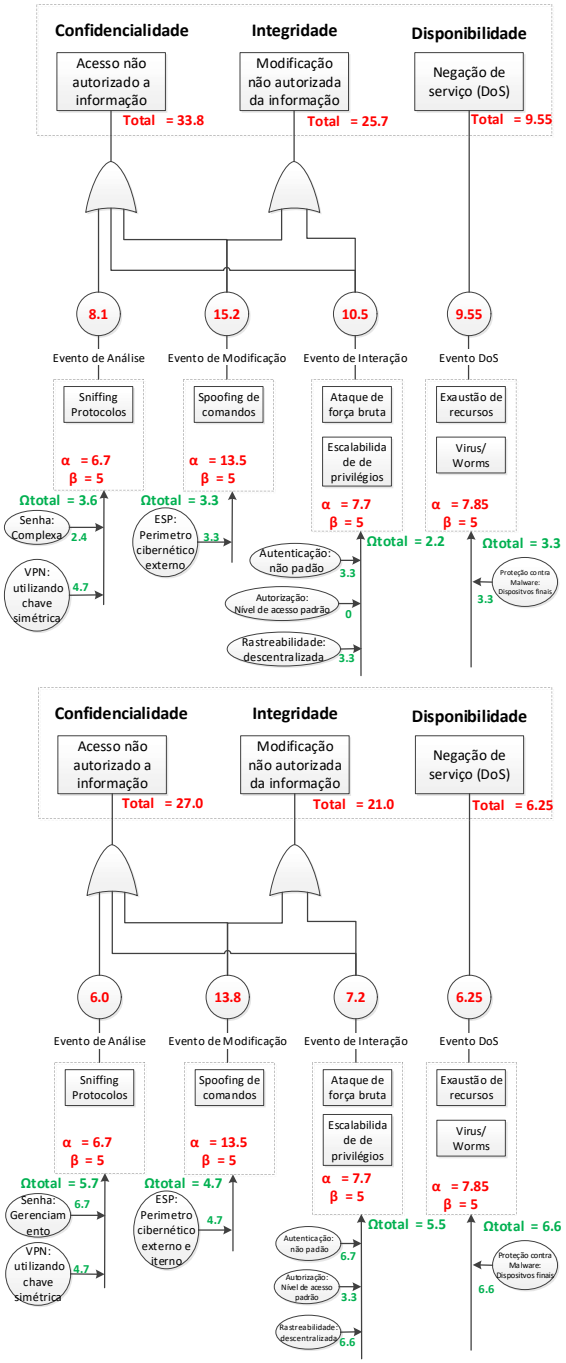
Após a escolha das contramedidas para cada tipo de evento cibernético o índice Ω total é calculado através da equação 3:

Equação 3 – Cálculo do índice Ω total.

(3)

4.0 - ANÁLISE DE VULNERABILIDADE COMPARATIVA: MÉTODO DE ACESSO DIRETO X ARQUITETURA DE ACESSO UTILIZANDO SERVIDOR PROXY

A árvore de ataques da figura 4 (a) é utilizada para avaliar o método de acesso direto e a árvore de ataques da figura 4 (b), o método de acesso utilizando um servidor proxy. Os índices de vulnerabilidades cibernéticas β e α possuem os mesmos pesos paras os dois sistemas. O índice de mitigação cibernética Ω foi considerado para cada sistema utilizando os recursos cibernéticos disponíveis para cada topologia e levando-se em conta a complexidade da instalação. As figuras 4 (a) e (b) descrevem os métodos de mitigação e os valores adotados para cada sistema em análise.



(a) (b)

FIGURA 4 (a) – Árvore de ataques para o método de acesso direto, (b) – Árvore de ataques para o método de acesso utilizando proxy.

A tabela 14 disponibiliza a análise comparativa entre os dois sistemas. Através da implementação do proxy e considerando a complexidade da implementação é possível observar uma redução na vulnerabilidade de 20% para o atributo de confidencialidade, 18% para a integridade do sistema e 34% para sua disponibilidade. A redução no nível de vulnerabilidade é observada devido à capacidade do sistema de restringir o acesso através de uma melhoria na política de senhas, gerenciamento de usuários e redução da superfície de conexões através da implementação de um acesso centralizado e indireto utilizando o servidor proxy.

Tabela 14 – Análise comparativa dos índices de vulnerabilidade entre o método de acesso direto e utilizando o proxy.

Método de Acesso	Confidencialidade	Integridade	Disponibilidade
Direto	33,8	25,7	9,55
Proxy	27,0	21,0	6,25
(Direto – Proxy / Direto) x 100	20%	18%	34%

5.0 - CONCLUSÃO

O artigo apresentou como construir e avaliar uma topologia de rede segura para o acesso indireto aos equipamentos de proteção e controle. Através da avaliação entre os métodos de acesso direto e utilizando o proxy, o artigo descreveu os pontos positivos e negativos de cada tipo de arquitetura de acesso. A análise comparativa através da árvore de ataques avaliou de forma quantitativa os ganhos e benefícios da utilização de um servidor proxy para o acesso à informação.

O método de acesso direto é o método com a maior facilidade de implementação, porém o mais vulnerável. O método que utiliza servidores de segurança insere uma camada extra de segurança, porém são difíceis de auditar e manter. O método utilizando proxies de acesso é o mais confiável e seguro, porém depende da escolha do equipamento com os corretos atributos. O proxy de acesso aos IEDs de proteção deve conter atributos capazes de mitigar as vulnerabilidades inseridas pelo meio externo e pelo acesso interno à informação. Funcionalidades como VPN, gerenciamento de senhas e rastreabilidade de usuários são essenciais para o correto funcionamento do sistema de acesso à informação.

O trabalho apresentou um novo método de análise comparativa entre dois métodos: acesso direto e o acesso utilizando servidores proxies. O método de análise utilizou uma árvore de ataques para mapear as vulnerabilidades e propor os métodos de mitigação. Através do cálculo dos índices de vulnerabilidade cibernéticas foi possível avaliar de forma numérica os ganhos de implementação do acesso indireto utilizando servidores proxies de acesso.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) S. Manso e D. Anderson, “Practical Cybersecurity for Protection and Control System Communications Networks,” 2017.

(2) N. Ferguson, B. Schneier e T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley , 2016.

(3) C. W. Ten, C. C. Liu e M. Govindarasu, “Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees”.

(4) C. Scott, P. Wolfe e M. Erwin, Virtual Private Networks, O'Reilly, 1999.

(5) R. Bryson, “Using Defense in Depth to Safely Present SCADA Data for Read-Only and Corporate Reporting,” 2017.

(6) https://www.first.org/cvss/user-guide, acessado em 15/03/2018

(7) https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, acessado em 11/04/2018

7.0 - DADOS BIOGRÁFICOS

Mauricio Silveira: formado em Engenharia Elétrica pela Universidade Estadual Paulista, atuou em projetos de P&D voltados para sistemas elétricos de potência antes de se juntar a equipe da SEL em 2014. Iniciou sua carreira na equipe de Engenharia e Serviços como Engenheiro de Proteção, em seguida assumiu os estudos avançados em tempo real utilizando o RTDS. Em 2016 se juntou a equipe de R&D na SEL-USA atuando no desenvolvimento de equipamentos voltados para aplicação da norma IEC 61850-9-2 (Sampled Values). Retornou ao Brasil fazendo parte da equipe de Engenharia de Aplicação da SEL, atuando nas áreas de Automação, Redes e Segurança Cibernética. Atualmente trabalha na sede da SEL em Pullman-WA no departamento de Pesquisa de Desenvolvimento como Engenheiro de Integração e Automação.

Eduardo Gonçalves é formado em Engenharia Elétrica pela Universidade Federal de Itajubá. Em 2014 ingressou na Schweitzer Engineering Laboratories, Inc. (SEL) como engenheiro de proteção para aplicações em campo. Posteriormente, atuou como engenheiro de estudos

realizando ensaios de simulações digitais em tempo real e estudos de coordenação e seletividade e energia incidente. Em 2016 trabalhou na matriz da empresa junto à divisão de Pesquisa e Desenvolvimento em tecnologias baseadas na aplicação das normas IEC 61850-9-2 (Sampled Values) e IEEE 1588 (Precision Time Protocol). Atualmente é engenheiro de aplicação e suporte técnico na SEL Brasil. Fornece suporte técnico a clientes em aplicações de controle e integração, ministrando treinamentos técnicos e participando de seminários do setor.