

GRUPO GTL
GRUPO DE ESTUDO DE PROTEÇÃO, MEDIÇÃO E CONTROLE EM SISTEMAS DE POTÊNCIA – GTL15

Vantagens de uso de Criptografia em Redes Não Seguras
Mecanismos de Defesa para Redes Não Seguras

**WELLINGTON OLIVEIRA (1); ROMULO FABRICIO CORNA (1);
SEL(1)**

RESUMO

O acesso remoto a dispositivos eletrônicos se tornou trivial e podem ser feitos através de sistemas de telecomunicação proprietários ou terceirizados. Os dados são trafegados usando protocolos permitindo o acesso direto aos dispositivos. O uso de protocolos não seguros, abrem uma forte possibilidade de captura de credenciais. Até pouco tempo empresas que administram sistemas de automação de energia elétrica não possuíam grandes preocupações com ameaças cibernéticas, somado a isso alguns poucos países, como os Estados Unidos, possuem regulamentação estatal com diretrizes específicas de segurança cibernética, sobre políticas e procedimentos para aplicações computacionais em meio industrial. De acordo com a literatura técnica existem diversas ações preventivas contra a interceptação de informações em um canal de comunicação, o artigo irá propor a adoção de medidas preventivas, com o objetivo de tornar as instalações elétricas mais seguras.

PALAVRAS-CHAVE

Segurança cibernética, criptografia, rede.

1.0 - INTRODUÇÃO

A evolução de dispositivos eletrônicos inteligentes (IEDs - *Intelligent Electronic Devices*) possibilitou a incorporação da rede *Ethernet* para o ambiente crítico de instalações de energia elétrica. Muitos foram os benefícios aportados ao ambiente de subestações, dentre os quais podemos destacar a possibilidade de transmitir e receber múltiplos protocolos em uma mesma porta física, o ganho atrelado está na facilidade de um acesso remoto ao equipamento, sem que ele deixe de comunicar com o sistema supervisório. Dessa forma através de uma porta lógica ele comunica com o supervisório e com a outra porta lógica ele comunica com um *software* de engenharia, ocasionando em uma elevada redução de custos na implementação e manutenção, pois dessa forma, equipes passaram ter a opção de não se deslocarem até subestação para modificar ajustes ou coletar dados para uma análise de ocorrência.

Com o avanço das aplicações, o acesso remoto aos IEDs por *softwares* de engenharia tornou-se corrente, sendo que vários desses *softwares* utilizam protocolos como o Telnet e FTP (*File Transfer Protocol*), além das vantagens atreladas há também alguns riscos, sendo que no ponto de vista da segurança cibernética esses protocolos não são seguros, por permitirem a captura de credenciais com o uso de ferramentas de fácil acesso como softwares de análise de tráfego de rede *Ethernet*, como por exemplo o *Capsa Packet Sniffer*, *Microsoft Network Monitor* ou o *Wireshark*, podemos nomear uma intrusão como essa de um ataques do tipo “*Man-in-the-middle*”.

Até o começo deste século empresas do setor elétrico que administram sistemas de proteção e automação não possuíam grandes preocupações com este tipo de ameaça, entretanto após o caos provocado pelo *Ransomware Blackenergy*, companhias do mundo inteiro iniciaram buscas por estratégias, táticas e ferramentas para proteger seus patrimônios de ataques cibernéticos. Alguns poucos países, como os Estados Unidos, já possuem regulamentação estatal com diretrizes específicas de segurança cibernética a serem cumpridas por empresas de infraestruturas críticas como o setor elétrico, gás, água e transporte.

O principal padrão adotado é o NERC-CIP (*North American Reliability Corporation – Critical Infrastructure Protection*) com estabelecimento de regras para o projeto e características técnicas mandatórias aos equipamentos a serem instalados nas subestações. Adicionalmente, ainda nos Estados Unidos, também existe recomendações do NIST (*National Institute of Standards and Technology*) sobre políticas e procedimentos para segurança de

aplicações computacionais em meio industrial. No Brasil, não existem regulamentações ou normas com recomendações técnicas sobre políticas de segurança cibernética em ambientes críticos, essa ausência torna o trabalho de técnicos e engenheiros de automação no Brasil complexo e desafiador.

De acordo com a literatura técnica existem diversas ações preventivas contra a interceptação de informações em um canal de comunicação, dentre os quais podemos destacar a criptografia de dados. Este trabalho compara o nível de segurança em subestações que usam o acesso remoto a IEDs no modo tradicional com o modelo utilizando criptografia. Adicionalmente o trabalho irá propor a adoção de outras medidas preventivas nos projetos de subestação modernas como gerenciamento de senhas de IEDs de proteção e acesso indireto aos relés de proteção.

2.0 - FUNDAMENTAÇÃO TEÓRICA

O termo segurança cibernética de acordo com a UIT/ITU (União Internacional das Comunicações) é:

A coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e propriedades de usuários(as). A organização e as propriedades incluem dispositivos de computação conectados, funcionários(as) e colaboradores(as), infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade de informação transmitida e/ou armazenada no ambiente cibernético. A segurança cibernética busca garantir a obtenção e a manutenção das propriedades de segurança da organização e das propriedades do(as) usuários(as) contra riscos de segurança relevantes no ambiente cibernético (5)

Os ataques cibernéticos são muito atrativos pela facilidade do invasor poder agir anonimamente e remotamente, com rastreamento relativamente lento e descoordenado a empresa ficará somente com os danos. Ao escutar a expressão “ameaça cibernética” muitas pessoas associam o possível invasor à figura de um *hacker*, um jovem usuário com capacidades e conhecimento computacionais muito acima da média que invade sistemas apenas por diversão, entretanto isso não é a realidade de nosso mundo contemporâneo (3).

Invasões da atualidade podem ser arquitetadas por organizações criminosas, que agem ou por uma questão econômica, motivadas pelo uso de criptomoedas ou organização ligadas a governos que coordenam ataques por motivos políticos. Como esses temas envolvem governos, instituições militares já utilizam o termo Guerra Cibernética (6). Tecnicamente qualquer usuário é vulnerável, todavia em sistemas industriais ou ICS (*Industrial Control System*) as consequências atingem o coletivo, causando danos em áreas essenciais como: saneamento, telecomunicações, mobilidade urbana, mercado financeiro, hospitais e o setor elétrico.

2.1 Histórico de Ataques

Até o final da década de 90 os sistemas de automação de energia elétrica não possuíam preocupações com esta ameaça, isso em função do cenário técnico da época. As subestações, em sua maioria, eram totalmente isoladas por conta das comunicações seriais (3). O cenário começou a se alterar após o aprimoramento dos protocolos de automação, como DNP3, IEC104 e Modbus suportarem o padrão *Ethernet*, como já foi mencionado, possibilitando acesso remoto de engenharia na mesma porta *Ethernet*. Nesse ínterim, a aplicação dos protocolos da norma IEC 61850 facilitaram uma interligação ainda maior com os IEDs, proporcionando descomplicado acesso as informação dos dispositivos.

A preocupação se as redes de comunicação estão realmente seguras, encontra fundamento em muitas estatísticas, uma delas é o crescimento no número de ataques registrados pelo CERT (Centro de Estudos, Resposta e Tratamento) no Brasil, que contabilizou 833.775 incidentes no ano de 2017 contra 5.997 incidentes no ano 2000, o crescimento ao longo dos anos pode ser observado na Figura 1.

10 a 13 de novembro de 2019
Belo Horizonte - MG

Estatísticas dos Incidentes Reportados ao CERT.br

| 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999 |

Valores acumulados: 1999 a 2017

Total de Incidentes Reportados ao CERT.br por Ano

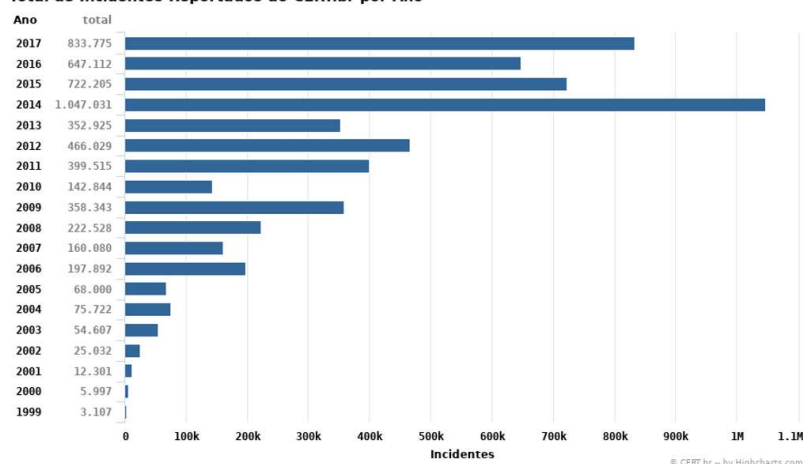


Figura 1 - Crescimento no registro de ataques cibernéticos. Fonte: CERT.

Adicionalmente à essas estatísticas empresas de ICS encontram fundamento para esta preocupação desde o ano de 2010 quando o vírus STUNET explorou vulnerabilidades em uma planta de enriquecimento de urânio no Irã. Após os ataques à Ucrânia em 2015 e em 2017 provocados pelos *Malwares* (*software* Malicioso) *Blackenergy 3* e *Crashoverride*, respectivamente, o que era preocupação, tornou-se uma necessidade de se proteger. A empresa Dragos afirma em seu relatório de análise que o dia 23 de dezembro de 2015 ficou marcado como um evento revolucionário para o setor elétrico. Pela primeira vez um caso registrado de um ataque cibernético interrompeu operações de uma rede elétrica (6).

O ataque provocado pelo *Malware Blackenergy 3* afetou 3 empresas do setor elétrico da Ucrânia e deixou 225.000 consumidores sem energia por um período de 6 horas, normalizados após operações manuais. O *Malware* ainda foi capaz de corromper o disco rígido de diversos equipamentos impedindo a comunicação dos dispositivos das subestações com o centro de controle por meses.

2.2 Tipos de Ameaças

Para defender o sistema de comunicação de uma ameaça é necessário saber quais são as ameaças e quais pontos comuns existem entre elas. As ameaças cibernéticas e os termos utilizados são:

- **Malware:** *Software* malicioso, desempenha um papel na maioria dos incidentes de intrusão e segurança do computador. Qualquer *software* que possa causar danos a um usuário, computador ou rede pode ser considerado *malware*, incluindo vírus, cavalos de Tróia, *worms*, *rootkits*, *scareware* e *spyware* (7).
- **Vírus:** *software* malicioso desenvolvido tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros *hosts*;
- **Phishing:** é uma tentativa de adquirir informações confidenciais, como nomes de usuário, senhas e detalhes do cartão de crédito, muitas vezes por razões maliciosas, mascarando-se como entidade confiável em uma comunicação eletrônica (9);
- **Worms:** não precisam se alojar em um arquivo para infectar, replicar e propagar. Depois que o *worm* encontra passagem pelo sistema, pode ser por conexão de rede ou arquivo baixado, ele se autocopia quantas vezes quiser e se propaga pela rede infectando *hosts* sem proteção;
- **Cavalo de troia:** *Malware* disfarçado de *software* legítimo. Podem ser empregados por criminosos virtuais para obtenção de acesso a sistemas dos usuários. Neste ataque, os usuários são induzidos por alguma forma de engenharia social a carregar e executar cavalos de troia em seus sistemas. Uma vez ativados os cavalos de troia, eles habilitam acesso de criminosos com o intuito de roubar informações;

- *Denial of Service (DoS)*: Ataques de negação de serviço, impedem que informações legítimas cheguem ao destinatário pretendido;
- Ataques distribuídos: Nesta ameaça um de hosts são infectados e controlados por um servidor de comando;
- *Rootkits*: *Software* que infecta uma máquina e deixa uma porta de comunicação aberta para uso posterior;
- *Ransomwares*: Tipo de *malware* que criptografa dados do usuário e solicita um 'resgate' para liberação dos dados. O prefixo do nome faz referência a palavra resgate em inglês. Criminosos costumam usar em conjunto com a ameaça *Phishing* e solicitar o 'resgate' através de pagamento via criptomoedas;
- *Man-in-the-middle*: Ameaça na qual a comunicação entre dois *hosts* é interceptada por alguém não autorizado. Os dados podem ser utilizados para roubo de informações ou alterados sem que as partes percebam.

2.3 Regulamentações

O que as ameaças possuem em comum são três passos para realizar um ataque: reconhecimento, análise de vulnerabilidades e por fim exploração. Usuários que buscam garantir a idoneidade da rede precisam de ações contínuas para evitar ataques e planos de contingência (1). Alguns países possuem regras bem estabelecidas de segurança cibernética em ambientes críticos. Na Figura 2 **Erro! Fonte de referência não encontrada.** pode ser visto a pirâmide das organizações americanas, sendo que dessas podemos destacar a NERC ¹(*North American Electric Reliability Corporation*) e a NIST ²(*National Institute of Standard and Technology*).

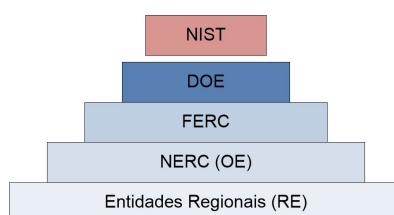


Figura 2 - Organizações americanas de segurança cibernética para ambientes críticos

As normas do NERC/CIP estabelecem requisitos mínimos para a implementação de um programa de segurança cibernética a fim de proteger o patrimônio institucional da empresa e manter a operação confiável (8). A abordagem da norma NERC/CIP é bastante abrangente e envolve desde os requisitos físicos da instalação até as ações necessárias para um plano de contingência. Infelizmente, no Brasil não existem normas de regulação ou orientação de segurança cibernética para ambientes críticos. Essas diretrizes estão divididas em:

- CIP-001: Sabotage Reporting;
- CIP-002: Asset Identification;
- CIP-004: Personnel Management;
- CIP-005: Electronic Security Perimeter;
- CIP-006: Physical Security;
- CIP-007: System Security;
- CIP-008: Incident Response;
- CIP-009: Recovery Plans;
- CIP-010: Configuration Management;
- CIP-011: Information Protection;
- CIP-014: Physical Security.

2.4 Criptografia

1 NERC: Organização sem fins lucrativos que possui como objetivo a regulamentação de requisitos de segurança formalizadas atrás das normas CIP (Critical Infrastructure Protection Standards);

2 NIST: Agencia governamental não regulatória que coordena desenvolvimento de normas para SmartGrid.

A necessidade de criação de mecanismos de segurança pode ser feito através de criptografia, assinatura digital ou controle de acesso, mas exige os requisitos listados a seguir.

- Confidencialidade: informações disponíveis somente a quem está devidamente autorizado a obter acesso a elas;
- Integridade: refere-se à informação estar intacta, sem alterações não autorizadas;
- Autenticidade: transmissor e receptor devem confirmar a identidade da outra parte envolvida;
- Irretratabilidade: este critério impede que o remetente ou destinatário negue uma mensagem transmitida
- Disponibilidade: informação deve estar disponível para o usuário que utiliza no momento em que necessita.

A etimologia do termo Criptografia tem sua origem na Grécia e é a junção de duas palavras: escondida e escrita. Sendo que sua aplicação está no objetivo de codificar uma mensagem através da utilização de símbolos e regras que só são conhecidas pelo transmissor e pelo receptor da mensagem. Essa regra de codificação possui duas classificações: chave simétrica e chave assimétrica (2).

2.4.1 Criptografia Simétrica

No modelo de criptografia simétrica a encriptação e a descriptação são realizadas usando a mesma chave, conforme ilustrado na Figura 3. Este modelo também é conhecido como criptografia convencional ou de chave única e proporciona velocidade e relativo baixo custo de implementação. O esquema de criptografia simétrica possui 5 fatores (2):

- Texto claro: Dado original;
- Algoritmo de criptografia: Código com as alterações e substituições do texto claro;
- Chave secreta: Valor alfanumérico utilizado para criptografar o texto claro;
- Texto cifrado: Mensagem criptografada que é transmitida;
- Algoritmo de descriptografia: Algoritmo que executa um processo inverso do algoritmo de criptografia e que recupera o texto claro a partir do texto cifrado.

Este princípio no qual o segredo deve residir exclusivamente na chave e não no algoritmo é chamado de Princípio de Kerckhoff, ou seja, os algoritmos são públicos e apenas as chaves são secretas. As chaves criptográficas são medidas em número de bits: 40bits, 56bits, 128 bit. Uma chave com 20 bits possui 2^{40} chaves possíveis e à medida que se acrescenta um bit no tamanho da chave será necessário o dobro de tempo para uma eventual quebra por tentativa ou ataque de força bruta.

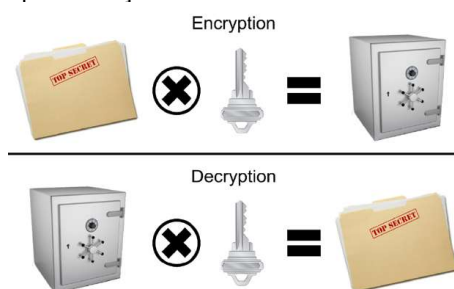


Figura 3 - Modelo de criptografia Simétrica

O padrão mais comum de chave simétrica é AES (*Advanced Encryption Standard*), também conhecida como Rijndael. A AES foi anunciada pelo NIST como o padrão americano de criptografia em novembro de 2001 após um concurso com outros 15 concorrentes. Vencedora, foi adotada pelo governo americano publicado como *Federal Information Processing Standard* (FIPS 197) e amplamente usado no mundo inteiro. Esta proposta estabelece que o tamanho do bloco do texto claro e o tamanho da chave podem ser especificados de forma independente em 128, 192 ou 256 bits.

2.4.2 Criptografia Assimétrica

10 a 13 de novembro de 2019
Belo Horizonte - MG

No modelo de criptografia assimétrica a encriptação e a desencriptação são realizadas usando chaves distintas, conforme ilustrado na Figura 4, entretanto matematicamente correlacionadas, uma chamada chave pública e outra chamada chave privada. Este método de criptografia é considerado mais robusto, entretanto em função da complexidade do algoritmo necessitam de mais poder de processamento e consequentemente são mais lentos.

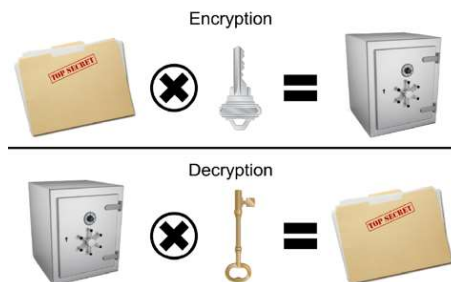


Figura 4 - Modelo de criptografia Assimétrica

3.0 - MECANISMOS DE DEFESA

3.1 Acesso de Engenharia

Os canais de comunicação de uma subestação podem conter enlaces com clientes externo, permitindo a entrada e a saída de dados da subestação. A infraestrutura de telecomunicações pode ser de propriedade da concessionária ou ainda de provedora de serviços de telecomunicações, expondo fisicamente os meios de comunicação a diversos ataques (5). Em alguns casos estes enlaces possuem algum tipo de conexão com a Internet o que aumenta a exposição a um ataque. Ataques do tipo *Man-In-The-Middle* ou DoS podem ocorrer. Uma ferramenta básica para observar mensagens trocadas através dos protocolos em execução é denominado analisador de pacotes (*packet sniffer*). Como o nome sugere, um analisador de pacotes cópia, ou fareja, passivamente mensagens enviadas e recebidas por um *host*, também exibe o conteúdo de vários campos das mensagens (7). Para exemplificar a ferramenta, a melhor escolha é o protocolo FTP, amplamente utilizado em *software* de acesso de engenharia, ilustrado na Figura 5, temos a tela do analisador de pacotes *Wireshark*, no qual é possível observar a senha digitada pelo usuário.

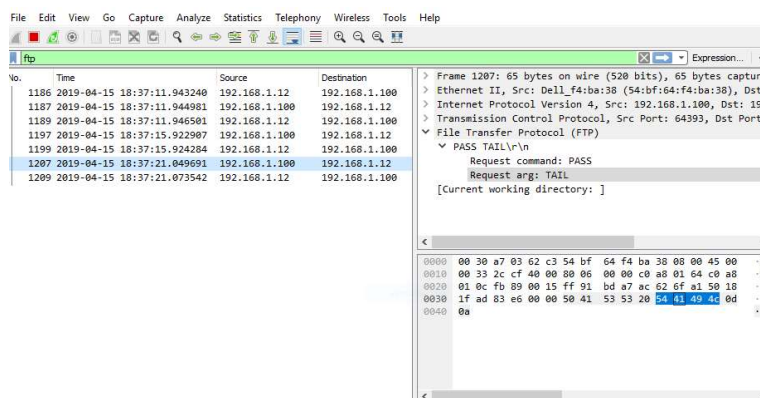


Figura 5 - Software Wireshark

Diante das ameaças de ataques, a utilização de criptografia para acesso remoto de engenharia é recomendada pela NER/CIP no item CIP-005. A utilização de criptografia dificulta a coleta de credenciais dos usuário por um invasor. No mesmo exemplo é realizado uma captura pelo *software* de análise, porém agora utilizando um protocolo também de transferência de dados, porém criptografado, conforme Figura 6, é possível observar que os pacotes agora necessitam de uma chave de descriptação para termos acesso a senha. A utilização de criptografia, portanto torna-se importante para utilização em canais de comunicação inseguros, canais externos à subestação.

10 a 13 de novembro de 2019
Belo Horizonte - MG

```

# SSH Version 2 (encryption:blowfish-cbc mac:hmac-sha1 compression:none)
Packet Length (encrypted): 6761a501
Encrypted Packet: 6404dfbce335354d3bcb02229b72716b8213237a
MAC: 93a12188853ec15e78e58861d93c0c1f8fa2503d

```

Figura 6 - Pacote capturado usando protocolo criptografado

3.2 Utilização de Gerenciamento de Senhas e Controle de Acesso

Além da utilização de criptografia a norma CIP-007-6 recomenda que o usuário de ambientes críticos utilize senhas complexas (senhas com pelo menos 8 caracteres contendo letras maiúsculas, minúsculas, números e caracteres especiais) nos dispositivos. Inicialmente o objetivo é evitar a utilização de senhas de fábrica nos dispositivos, entretanto mesmo que os usuários alterem as senhas dos dispositivos é recomendado que as senhas sejam alteradas periodicamente. Esta tarefa pode feita manualmente entretanto torna-se inviável, pela quantidade de equipamentos na rede. A opção que torna a tarefa viável é a utilização de um gerenciador de senha automático para realizar essas alterações periodicamente respeitando-se os critérios de senha estabelecidos na norma CIP-007-6. A norma NERC também estabelece através do item CIP-010-2 que o gerenciador de senhas deve manter um relatório de todos os usuários e suas senhas e quais alterações foram feitas. Este relatório deve ser enviado ao administrador da rede, um exemplo de relatório é ilustrado na Figura 7. Adicionalmente é importante que o gerenciador de senha também seja capaz de resetar as senhas para valores de fábrica em caso de alguma emergência.

Managed Device Passwords

Device	Account	Current Password	Proposed Password	Next Change
SEL751A	CAL	!E069NSMg8<p		
SEL751A	ACC	aRQdn2H ^de		
SEL751A	2AC	t<ipL>Ku2}QH		

Figura 7 - Exemplo de um relatório de um gerenciador de senhas.

A utilização de um gerenciador de senhas combinado com controle de acesso de usuários também é recomendada. Isso em função de que após gerenciar as senhas dos dispositivos os funcionários de uma empresa não saberão as senhas que estão nos IEDs. Dessa forma para eles acessarem os IEDs deverão utilizar credenciais da rede corporativa usando protocolos como o LDAP (*Lightweight Directory Access Protocol*) ou RADIUS (*Remote Authentication Dial-In User Service*), trazendo mais segurança para a aplicação e registro histórico das atividades. A Figura 8 ilustra um exemplo no qual um usuário chamado Bob tenta acesso a um IED, neste exemplo Bob usa as credenciais da rede corporativa da empresa para acessar o IED que só é liberado após verificação do gerenciador de acesso consultar um servidor. Importante ressaltar que em caso de desligamento do funcionário o acesso deve ser revogado em um período de 24 horas, conforme estabelecido pela CIP-004-6.

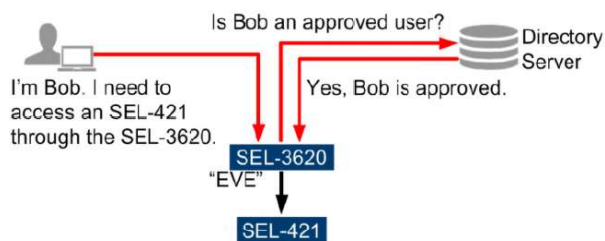


Figura 8 - Controle de acesso baseado em LDAP ou RADIUS

3.3 Proteção em Camadas

O conceito de segurança em subestações nos remete a uma imagem de proteção com cercas, cadeados e vigias. Esta compreensão tem origem na antiguidade, quando comparado aos sistemas de proteção de castelos medievais, no qual um invasor teria que passar por diversas etapas (fosso, muro alto, soldados, portões, etc.) até finalmente chegar ao trono do rei. Este conceito também pode ser empregado em segurança cibernética através do termo "Defesa em Profundidade" (5). Este princípio está previsto na norma CIP-005 e o objetivo é proteger a camada mais interna que seria os IEDs e os equipamentos primários, conforme observa-se na 10.

10 a 13 de novembro de 2019
Belo Horizonte - MG

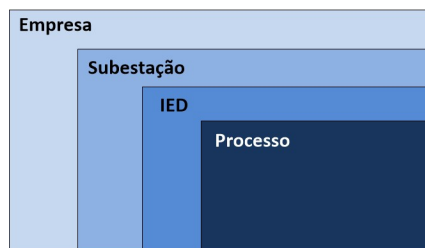


Figura 9 - Exemplo de segurança em camadas

Na camada da Empresa, é aconselhado a utilização de políticas corporativas de segurança baseadas em *firewall*, antivírus e controle de acesso centralizado. Na camada de Subestação também é recomendado o uso de *firewall* para controle de acesso interno e externo à rede da subestação e acesso indireto à camada de IED utilizando-se protocolos criptografados, conforme discutido nos itens anteriores, Figura 9. Por fim, deve ser utilizado senhas complexas para acessar a camada que pertence o IED, somados as alterações cíclicas nas senhas de acesso.

3.4 Utilização de Firewall

A utilização de *firewall* em ambientes industriais é a mais comum contra invasões de rede na borda da subestação. Firewall tem a função de isolar uma rede privada de rede externa, aceitando que somente alguns pacotes passem, sendo que os demais são desartados. Fisicamente é um roteador que possui filtros baseados em endereço IP (Internet Protocol) de origem e destino, tipos de protocolos e portas de origem e destino. Por ser alocado em uma zona de fronteira, deve ser um equipamento projetado adequadamente para que não ofereça uma falsa sensação de segurança (7).



Figura 10 - Camadas de Segurança

3.5 Sistema de Detecção de Intrusão

Como visto anteriormente, o *firewall* faz uma busca pelos endereços IP, portas, ou seja, ele analisa o cabeçalho das informações que pretendem passar pelo *firewall*. Porém ele não faz uma inspeção profunda de pacote, verificando o que a mensagem está transportando, logo há a oportunidade para mais uma proteção na rede, que seria justamente um IDS (*Intrusion Detection System*) (7).

Esse *software* quando identifica uma mensagem suspeita ele tem a capacidade de interromper o seu acesso à rede, ou se ele não consegue concluir ele enviar um alerta, ao gestor da rede, com os dados da mensagem suspeita. O IDS pode ser usado para detectar muitos tipos de ataques, como ataques Dos, ataques de inundação de largura de banda, *worms* e vírus. Há inúmeros sistemas IDS, um que é de domínio público é o Snort IDS, ele utiliza uma interface libpcap de análise gráfica, que também é empregado no *Wireshark*, e em muitas outras ferramentas de análise de pacotes (7).

3.6 Memórias USB

10 a 13 de novembro de 2019
Belo Horizonte - MG

Subestações de energia que possuem um computador local, que geralmente possui um supervisor, além de guardarem um *backup* para configurações dos IEDs, sempre são acessados localmente por uma memória USB, sendo que esse pequeno dispositivo é conveniente de usar pela sua flexibilidade. Através dele é possível verificar as atualizações de software, descarregar configurações ou *firmware* novos nos IEDs, carregar arquivos de análise de oscilografia e descarregar manuais de operação.

Porém por essa flexibilidade eles são um dos dispositivos de acesso de rede mais perigosos para sistemas operacionais que não executam verificações de segurança, infectando o sistema. A facilidade que esses dispositivos oferecem aos usuários, também é uma oportunidade aos invasores, pelo seu potencial de disseminar e infiltrar malwares em redes privadas. Como medidas paliativas podemos desativar recursos de execução automática, em todos computadores que acessam a rede com os equipamentos, outra medida seria estabeleça políticas restritas para o uso de memórias USB em todas as redes do sistema. (4).

4.0 - CONCLUSÃO

As preocupações com segurança cibernética não são mais exclusivas a profissionais de TI, esta realidade já atinge o ambiente de automação de subestações de energia e podem trazer consequências catastróficas. Regulamentações existentes nos EUA enfatizam a adoção de medidas preventivas nos projetos das subestações.

No Brasil ainda não existem regulamentações do governo federal ou da agência regulatória, entretanto isso não justifica a não adoção de técnicas de segurança cibernética nas subestações. A adoção de técnicas, como a criptografia contribuem na preservação da confidencialidade dos dados de usuário e evitam que dados capturados de forma não autorizada seja interpretadas ou manipulada. Especialmente para o caso de acesso de engenharia remoto a adoção de protocolos seguros (criptografados) sob redes não confiáveis deve ser uma premissa básica para o acesso remoto das subestações.

5.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) Gomes, M.G.F.M., Cordeiro S.S e Pinheiro, W.A. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle. Disponível em: http://rmct.ime.eb.br/arquivos/RMCT_3_tri_2016_web/RMCT_275.pdf
- (2) Aquino, Guilherme. Curso de segurança cibernética, Inatel, disciplina AS301.
- (3) Oliveira C., Abboud R. Desafios da Segurança Cibernética nas Subestações de Energia Elétrica, revista O Setor Elétrico, Ago 2013.
- (4) Industrial Control System: Focused Malware, Advisory (ICSA-14-178-01), Junho, 2014. Disponível: https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01#footnotea_rwoc26s
- (5) ITU, CIBERSEG, 2008.
- (6) Relatório Dragos. Disponível em: file:///C:/Diretorio%20Wellington/Cybersecurity/CrashOverride-01___Relatorio%20da%20DRAGOS.pdf. Acesso em 28 de março de 2019.
- (7) K. Jim, Ross, K. Redes de Computadores e a Internet: uma abordagem top-down. Editora Pearson, 6ª edição, 2013.
- (8) Heinisch A., Leite L., Spyer B., Rabello M. Segurança Cibernética para Processos Operativos em Sistemas de Energia Elétrica. Disponível em: <file:///C:/Diretorio%20Wellington/Cybersecurity/Seguranca%20Cibernetica%20para%20Processos%20Operativos%20em%20Sistemas%20de%20Energia%20Elétrica%20.pdf>
- (9) S. Michael, H. Andrew. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. Editora No Starch Press, 1ª Edição, 2012.

6.0 - DADOS BIOGRÁFICOS

Wellington Oliveira nascido em Salvador-BA em 1982 possui graduação em Engenharia Elétrica e Especialização em Automação de sistemas Elétricos de potência e conta com 19 anos de experiência na área de automação de SEP. O histórico profissional conta passagens por Cia de eletricidade e fabricante de equipamentos de proteção e automação. Colaborador da Schweitzer Engineering Laboratories desde 2012 e possui interesse nas áreas de automação, protocolos de comunicação, segurança cibernética e logicas IEC 61131-3.

Rômulo Fabricio Corna. Nascido em Curitiba-PR, em 1985. Possui graduação em Engenharia Elétrica pela UTFPR (2010), especialização em Teleinformática e Redes de Computadores pela



XXV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA

10 a 13 de novembro de 2019
Belo Horizonte - MG

3904
GTL/28

UTFPR (2015) e mestrando em Desenvolvimento de Tecnologia pelo LACTEC (2019). Tem interesse nas áreas de automação, engenharia elétrica, rede de computadores, segurança cibernética. Empresa: Schweitzer Engineering Laboratories, desde 2014.