Capítulo VI

Segurança em redes de computadores aplicadas a subestações de energia elétrica

Equipe de engenharia da Schweitzer Engineering Laboratories (SEL)

Até a década de 1990, os equipamentos de automação e proteção de subestações, que já tinham se tornado microprocessados, ainda estavam fora das redes de computadores e compunham soluções isoladas, sem conexão física com a rede mundial. As concepções de segurança estavam limitadas a isolar estes equipamentos em salas climatizadas, em que o acesso era restrito às pessoas autorizadas; preservação contra incêndios, etc. Contendo as invasões físicas, o sistema estava protegido e em condições adequadas de segurança.

Existem dois conceitos básicos de segurança que podemos nos servir da língua inglesa para melhor definí-los:

Safety – São os conceitos aplicados à segurança das pessoas. Iniciativas são tomadas para mitigar situações de risco que podem ferir o ser humano ou, de forma mais geral, o meio ambiente. Existem normas mundiais que disciplinam esta matéria, sendo que a IEC 61508 e a IEC 61511 são as mais conhecidas.

Security – São conceitos aplicados à segurança dos ativos de uma empresa. As instalações, os equipamentos, os negócios, os faturamentos e os lucros. Para este caso, podemos citar a norma IEC 62351.

A consequência de invasões em uma rede de computadores de uma empresa de energia elétrica está mais ligada ao conceito de "security". Apesar de a segurança das pessoas também estar exposta ao risco, este artigo está focado na segurança dos ativos das empresas e na continuidade de fornecimento de energia elétrica, preservando os requisitos de qualidade definidos pela Agência Nacional de Energia Elétrica (Aneel).

Com o crescimento exponencial da utilização da tecnologia TCP/IP e internet no mundo moderno, a automação de subestações não ficou imune. Hoje, os novos projetos adotam TCP/IP de forma ampla, total e irrestrita.

É evidente que os problemas de segurança em redes de computadores passaram a integrar as preocupações dos profissionais de tecnologia de automação, conhecida como TA. Neste contexto, foi adotada a terminologia "invasão ou ataque eletrônico" (no contexto de TI é conhecido como "invasão ou ataque cibernético").

As ameaças de invasão por meios eletrônicos estão aumentando por diversos fatores sociais, políticos e tecnológicos.

Nos dias atuais, existem vários fatores que contribuem para o aumento de nossas preocupações:

- De mainframes e protocolos proprietários, passamos para redes distribuídas e protocolos abertos. Interligação de redes originalmente isoladas por meio destes protocolos;
- Pressão na indústria pela automatização e corte de custos para manter margem de lucros;
- Legislação Nacional, Operador Nacional do Sistema (ONS) e Agência Nacional de Energia Elétrica (Aneel). O consumidor tem o direito de acessar dados das concessionárias de serviço públicos (servidores Web);
- Aumento da capacidade e complexidade do Sistema Interligado Nacional (SIN), de geração e transmissão de energia. Paradoxalmente, aumenta sua fragilidade;
- Aumento vertiginoso da interconectividade a sites remotos por meio de modems discados ou internet;
- Instabilidade no mercado de trabalho nas empresas de energia, causados pela competição e desregulamentação;
- Aumento de incidentes – China, Google e Intel;
- Rápido aumento da população com habilidades e conhecimentos consistentes em redes de computadores;
- Disseminação de literatura e ferramentas de hackers pela

internet;

• Aumento do número de países com iniciativas sustentadas pelo governo de "contramedidas" à invasão ou ataques eletrônicos.

Invasão ou ataque eletrônico

É o acesso à subestação via linhas telefônicas ou outros meios eletrônicos para manipular ou causar distúrbios nos Dispositivos Eletrônicos Inteligentes (IEDs). Estes IEDs incluem relés digitais, registradores de faltas, equipamentos de diagnósticos, oscilógrafos, equipamentos de automação, Unidades de Aquisição e Controle (UACs), Unidades Terminais Remotas (UTRs), computadores servidores da subestação, Controladores Lógicos Programáveis (CLPs) e interfaces de comunicação.

A extensão dos "ataques eletrônicos" ainda é desconhecida, pois poucas empresas possuem Intrusion *Detection System* (IDS). E aquelas que detectam têm pouca vontade de divulgar, pois seria uma publicidade negativa.

Ainda assim:

• 25% das empresas usam algum tipo de IDS;

• 17% destas reportaram tentativas de invasão eletrônica.

Os invasores sabem como abrir válvulas, apertar botões, abrir/fechar disjuntores, então é de se supor que, se eles invadirem o sistema, queiram fazer isso. É, portanto, necessário e inadiável um ato de responsabilidade para com a sociedade em geral e consumidores discutir as ameaças e estudar os métodos de mitigação dos riscos.

A segurança deve ser uma atitude empresarial. Uso de senhas, vários níveis de acesso e auditoria de logins devem ser utilizados de forma cuidadosa, apesar de aumentar os procedimentos burocráticos. Vamos relacionar abaixo alguns itens que devem ser cuidadosamente considerados no planejamento e na definição da política de segurança. Citamos termos importantes, ainda sem entrar nos detalhes de cada um deles:

- Tecnologia TCP/IP – Transmissão de pacotes

- *Sniffers – Ethereal – Wireshark.*
- Avaliação de riscos. O perigo vem de dentro.

- Firewalls. Software ou software + hardware

- Filtro de pacotes – Política "negar tudo" ou "permitir tudo" e fazer as exceções à regra.
- Filtro de aplicações – proxy.
  - *Event Logging – Syslog;*
  - *Intrusion Detection Systems (IDS);*
  - *Intrusion Prevention Systems (IPS);*
  - *Condições de alarmes.*

- Roteadores – proveem IDS, IPS, Event Logging, controle de acesso por IP, Port Number, gerenciamento de separação de tráfego, perímetro eletrônico de segurança e IEEE 1613.

- Controle de acesso, switches ou ponto de acesso wireless.
  - IEEE 802.1 X Remote Authentication Dial In User Service (Radius) – Passaporte para entrar na rede. MAC Address.
  - TACACS – Terminal Access Controler – Access Control Sys.

- Switches como alternativa de segurança. VLAN – IEEE 802.1Q, CoS -802.1P, RSTP – 802.1W.

- Virtual Private Network (VPN) – criptografia – autenticação.
  - Internet Protocol Security (IPsec) – RFC 4301, 4302, 4303.

- IEEE 1613 – Standard Environmental and Test Requirement for Communication Networking Devices in Electric Power Substations. Imunidade e compatibilidade eletromagnética – IEC61850-3.

A área de segurança de redes é uma ciência e vários órgãos internacionais propõem sugestões de comportamento ou medidas que as empresas devem observar. Uma delas é:

IEEE 1402-2000 – Guia para segurança física e eletrônica de subestações do sistema de potência.

Itens de alerta que fragilizam a rede:

- Erros grosseiros, confusão e omissão. *Resets* acidentais de relés de proteção, imperícia ou negligência na manutenção da rede;
- Fraudes, roubos, atividades criminais, *hacker*, *attacker* e *intruder*. Motivação econômica – prejuízos de US$ 123 milhões anuais;
- Empregados descontentes e inescrupulosos, retaliação e *insiders*;
- Curiosidade, ignorância, invasões por recreação ou maliciosa e *hackers*;
- Espionagem industrial. Em 1999, os prejuízos foram de US$ 60 milhões;
- Código malicioso: *malware*, vírus, *worms*, cavalos de tróia, bombas relógio, etc. que crescem exponencialmente;
- Abrir anexo e clicar em *links* de e-mails desconhecidos;
- Programas que prometem aumentar a velocidade de sua rede, mas estão roubando informações;
- Contramedidas a ataques eletrônicos financiados pelos governos de vários países.

A subestação como o ponto mais vulnerável de todo sistema elétrico

Avaliação de riscos

A subestação de energia elétrica é um ponto vulnerável, porque permitem acesso remoto e poucas possuem mecanismos de proteção, IDS, IPS ou firewalls, com o agravante que uma falha pode assumir proporções nacionais.

Linhas de comunicação entre subestações, centros de controle e computadores de rede corporativa são de conhecimento público.

Todos os IEDs são suscetíveis a ataques. Por meio de uma conexão telefônica, um profissional pode "resetar" o dispositivo, ou mudar o seu "ajuste". Um "intruso eletrônico" pode "discar" em uma porta desprotegida e colocar o "controlador de disjuntor" em um nível de tolerância alto a controles, permitindo telecomandos. Também pode colocar o equipamento em condições muito sensíveis, acima das operações normais, e que causam "*shutdown*" para autoproteção.

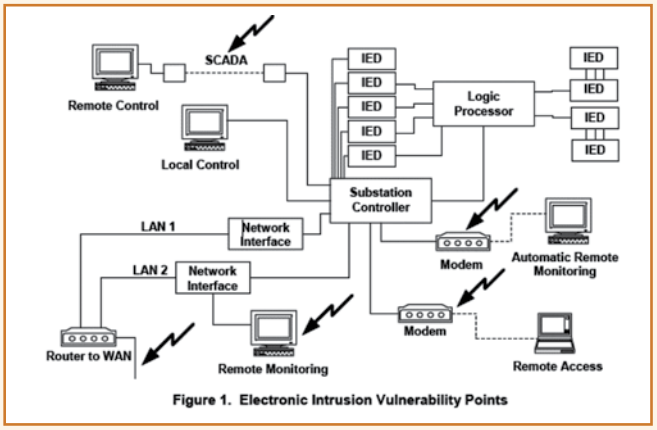

Figura 1 – Cenário de uma invasão.

Observamos na Figura 1 o cenário provável de uma invasão eletrônica. Usando um "programa discador", o intruso faz uma varredura nos números acima e abaixo do número telefônico da subestação, que é de conhecimento público, procurando por resposta de modems. Pode usar também um aplicativo de Ping, pesquisando milhares de IPs acima e abaixo do IP da concessionária, que é de conhecimento público.

Quando uma provável conexão é identificada, são emitidos múltiplos "enters", "pontos de interrogação", "help" and "hello", para conseguir informações do tipo da conexão. Quando é conseguido o diálogo de "login", o intruso usa "engenharia social" para determinar a senha. Ou lança um ataque com "dicionários" ou de "força bruta".

Quando a conexão for completada, o intruso está dentro de um IED, controlador ou Scada. Pode fazer shutdown, mudar ajustes, juntar informações para futuros ataques, "plantar" códigos maliciosos, etc. Este ataque clássico pode ser somado à engenharia social e a outros que exemplificamos na Figura 2.

Engenharia social é a ação de uma pessoa mal intencionada que se faz passar por uma ou mais pessoas, enganando os colaboradores de uma organização. Esta pessoa utiliza nomes de usuários e administrador coletadas previamente. Com isso, consegue obter informações privilegiadas, como senhas, ou induzir pessoas a executar ações que enfraqueçam a segurança, como executar um trojan.

O método mais simples, mais usado e mais eficiente que os engenheiros sociais utilizam para descobrir uma senha é perguntando. Se o colaborador da empresa estiver despreparado, há possibilidade de se obter com sucesso a resposta positiva à pergunta certa, assim, o engenheiro social irá ganhar acesso, controlar e conseguir mais acesso.

Muitos ataques de engenharia social são complicados, envolvem diversas etapas e planejamento elaborado, além de combinar o

conhecimento da manipulação e da tecnologia.

O início, na maioria das vezes, dá-se por meio de pesquisa na internet sobre a instituição ou o alvo de ataque. De posse de algumas informações, o ataque é preparado, podendo ser feito por telefone, ou se passando por um funcionário terceirizado que presta serviços à organização.

Contramedidas

A prevenção é a melhor política. Descrevemos resumidamente alguns métodos:

Autenticação – Dispositivos autorizados autenticam uns aos outros, trocando "chaves" – equivalente à senha. Gateway pode autenticar novos dispositivos que entram na rede.

- Smart cards – geram a senha em tempo real e ela é enviada na rede e pode ser interceptada;
- Verificação da integridade – equivalente ao checksum;
- Etiqueta de tempo evita ataques de "replays";
- Criptografia – algoritmos simétricos e assimétricos, chaves duplas;
- PKI – Public Key Encryption;
- IPsec – criptografa os pacotes TCP/IP;
- Algoritmos Diffie-Hellman – assimétricos.

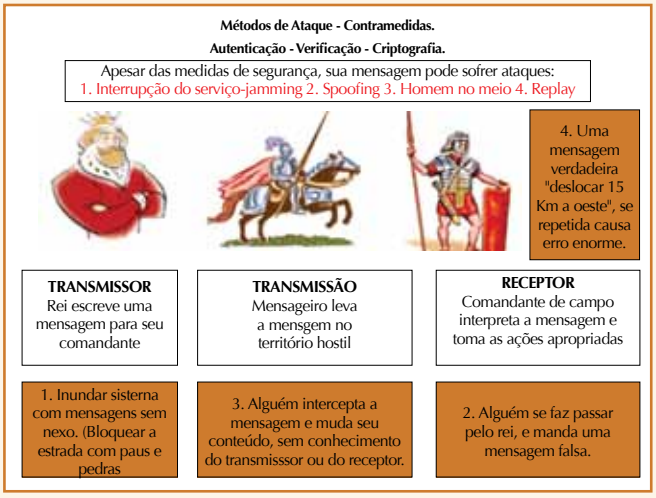

Figura 2 – Métodos de ataque.

Elaboração da política de segurança

Quais recursos serão protegidos? A quais ameaças estamos sujeitos? Quais as vulnerabilidades que podem concretizar as ameaças?

Considerar os itens a seguir:

- Quem tem autoridade para definir e fazer cumprir?
- Meios de divulgação da política;
- Política de senhas, requisitos de formação (número mínimo de caracteres alfanuméricos) e período de validade;
- Direitos e responsabilidades dos usuários;
- Direitos e responsabilidades do provedor de recursos;
- Ações previstas no caso de violação da política;
- Apoio da administração superior é fundamental;
- Periodicamente revisada;
- Não pode estar atrelada a softwares ou a hardwares específicos;
- Não pode haver exceção a indivíduos ou grupos.

Além das políticas, os investimentos são indispensáveis. É necessário equipar seu sistema com recursos de hardware e software.

Fazem parte do conjunto de dispositivos de segurança (hardware ou softwares) as lans virtuais, firewalls e criptografia (certificados digitais). Sobre as lans virtuais, já dedicamos um capítulo inteiro quando abordamos as arquiteturas de rede.

Firewalls

Responsável pela defesa do computador ou rede. Controla o acesso ao sistema por meio de regras e filtragem de dados. Filtragem de pacotes – redes pequenas ou médias que definem que endereços IPs podem transitar na rede. Por exemplo, serviços liberados (e-mail) ou bloqueados (ICQ).

- Windows – ZoneAlarm – www.zonealarm.com;
- Linux – IPTables – www.iptables.org;
- Trabalha nas camadas IP (endereços) e TCP (serviços);
- Controle de aplicações – (exemplos SMTP, FTP, HTTP) – instalados em servidores conhecidos como proxy. Mais seguro, não permite a comunicação direta do computador com a internet e tudo passa pelo proxy;
- Permite acompanhamento de tráfego de rede;
- Recursos de logs;
- Ferramentas de auditoria.

Exemplos e sugestões:

- As portas TCP que podem ser liberadas e continuar mantendo a segurança da sua rede são: porta de FTP, HTTP, HTTPS e serviço de e-mail, como o BlackBerry 3101. Bloqueie a porta 110 (POP3) caso o servidor de correio não a utilize. Esta porta permite que os usuários de sua rede possam baixar mensagens particulares utilizando algum software de correio eletrônico, sendo que a maioria dos servidores de e-mail trabalha apenas utilizando SMTP e IMAP.
- Evite regras excessivas e teste cada uma delas. As regras de externa para interna são muito importantes. Coloque uma para cada serviço de sua rede. Por exemplo: jamais libere a porta 23 ou 21 que não sejam redirecionados para o servidor correspondente. Também não faz sentido liberar o serviço HTTPS (443) de externa para interna se não possuir algum servidor que tenha SSL ativo.
- Muitas empresas possuem usuários que precisam enviar arquivos para Receita Federal. Neste caso, identificar a qual IP e porta que o programa da Receita Federal está tentando se conectar (netstat-aon) e liberar somente esse IP e porta específica.

Criptografia e certificados digitais

Symmetric Key Algorithms – a mesma chave secreta é usada pelo transmissor e receptor. Usado há milhares de anos, é a mesma chave para criptografar e descriptografar e usa menos recursos computacionais

que o Asymmetric. É necessário combinar a chave com antecedência. Exemplos: PGP e SSL.

Asymmetric Key Algorithms – Chaves diferentes para criptografar e descriptografar. É criado um par de chaves – uma pública e outra secreta. Mensagens criptografadas com a chave pública só podem ser descriptografadas pela chave secreta. As chaves são relacionadas matematicamente, mas é impossível derivar a chave secreta da chave pública. O algoritmo foi demonstrado na década de 1970 por Whitfield Diffie e Martin Hellman.

Problema central – Confiança que a chave pública é correta e que realmente pertence à pessoa ou entidade que afirma possuí-la e não foi modificada por intrusos maliciosos.

IPSec – combina diferentes tecnologias para prover maior segurança, como um mecanismo de troca de chaves de Diffie-Hellman; criptografia de chave pública para assinar as trocas de chave de Diffie-Hellman, garantindo, assim, a identidade das duas partes e evitando ataques do tipo man-in-the-middle (em que o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação); algoritmos de encriptação para grandes volumes de dados, como o DES (Data Encryption Standard); algoritmos para cálculo de hash (resto de uma divisão, de tamanho fixo) com utilização de chaves, com o HMAC combinado com os algoritmos de hash tradicionais, como o MD5 ou SHA autenticando os pacotes e certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

Como considerações finais, poderíamos relacionar os dispositivos (hardware e software) que nos auxiliariam na proteção de nossas redes. A lista de dispositivos é extensa.

Citamos os switches RuggedComm e GarretComm e Gateway SEL, que incluem toda tecnologia de segurança de criptografia e certificados digitais, IPSEC nas subestações.

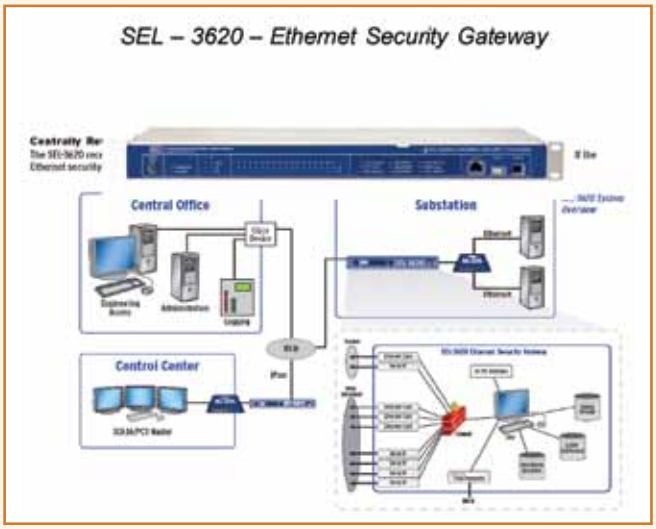

Figura 3 – Criptografia e certificados digitais em subestações de energia elétrica.

**Equipe de engenharia da Schweitzer Engineering Laboratories (SEL)*

CONTINUA NA PRÓXIMA EDIÇÃO
Confira todos os artigos deste fascículo em www.osetoreletrico.com.br
Dúvidas, sugestões e comentários podem ser encaminhados para o e-mail redacao@atitudeeditorial.com.br