

Doze Dicas SEL para Melhoria da Segurança de Ativos da empresa:

A SEL sempre se importou com aspectos de segurança de seus produtos e desde os primeiros relés de proteção já haviam 2 níveis de acesso com senhas separadas e contatos de alarmes para casos de falhas de acessos.

Há muitos anos a SEL vem enfatizando a importância da segurança em Sistemas Integrados e tem publicado muitos artigos técnicos descrevendo as ameaças, cenários de ataque, etc. além de fornecer um curso sobre segurança cibernética.

Acreditamos que a responsabilidade pela segurança não deva ser somente do Departamento de Informática das empresas, pois fatores como a rápida mudança tecnológica e a forte característica de que o sistema elétrico de potência aplica em diversos tipos de equipamentos eletrônicos com diferentes meios de comunicação e de acesso, provocam que a responsabilidade deva ser repartida entre todos envolvidos (equipe de automação/ SCADA, engenheiros de proteção, equipe de manutenção, fornecedores, consumidores, Governo, etc.).

Felizmente, existem muitas medidas simples e de baixo custo que podem ser consideradas para reduzir as ameaças de acesso ao sistema elétrico de potência. Abaixo, estamos listando 12 atividades que devem ser seriamente consideradas.

1. Conheça todos caminhos para chegar aos ativos: Faça um mapa de acesso!

SCADA, EMS, acesso pela engenharia, acesso pela manutenção, linha telefônica, rede sem fio, internet, interconexões entre diferentes sistemas, etc.

2. Use senhas de alto nível:

Os equipamentos SEL facilitam esta implementação, pois é possível escolher entre todos caracteres ASCII:

exemplo de senha de baixo nível: 17106400

exemplo de senha de alto nível: M\$!4fp&r

3. Gerencie as senhas:

- Não use senhas default
- Mude-as periodicamente
- Mude-as quando pessoas saírem da empresa
- Controle-as
- Use diferentes senhas em diferentes regiões

4. Faça comunicação encriptografada

Cabos, fibra, rádio, SCADA, acesso engenharia, manutenção

5. Pratique necessidade de conhecer (Need to Know)

- Mantenha seus projetos seguros
- Limite acessos a detalhes do sistema somente para aqueles que realmente precisam conhecê-los para desempenharem suas atividades

6. Compartilhe conhecimento

7. Para acessos chaves, tenha mais de um (seguro) meio de comunicação seguro

- Minimize o impacto de uma eventual falha de acesso geradas por crimes ou ataques cibernéticos
- Envie alarmes de segurança através do segundo meio de comunicação

8. Tome iniciativa agora. Não espere uma legislação do governo ou um ataque acontecer.

9. Revise alarmes e atividades de acesso.

10. Não esqueça da segurança física.

11. Pratique segurança em maior profundidade

Física, cibernética, comunicação, treinamento, cultura, etc.

12. Guarde as ferramentas de acesso

Computadores, senhas, equipamentos e chaves de encriptografia, manuais de instrução e softwares

10 MITOS SOBRE SEGURANÇA:

Quando acontece um problema, como crime cibernético, a natureza humana frequentemente recusa a aceitar sua importância ou sua existência. Mitos como os abaixo são frequentes formas de se evitar um problema ou retardar ações:

1. Nós usamos o protocolo xxxx e nenhum “ Hacker” o conhece.

É verdade que ao utilizar um protocolo não muito comum se reduz a possibilidade de um hacker atacar sua empresa, porém analisadores de protocolos tem surpreendido pelo profundo conhecimento dos protocolos de comunicação. Portanto, os protocolos sejam velhos ou novos, abertos ou proprietários são conhecidos.

2. Rádios Spread-spectrum são inerentemente seguros.

O principal motivo de aplicá-los é de se evitar interferência com outros sinais e não para aumentar a segurança da comunicação. É necessário utilizar encriptografia mesmo com rádios.

3. A rede da empresa é privativa, portanto o risco é pequeno.

Hackers possuem acesso a redes privativas e também podem acessar circuitos, cabos, sinais, etc. que outros também tem acesso. As redes privadas, assim como as públicas, NÃO são seguras e EXISTE RISCO.

4. Seria muito difícil acessarem o SCADA da empresa através rádio ponto a ponto.

Os hackers podem sintonizar frequências usando o nome da empresa e licenças de rádio da ANATEL e mesmo através da observação dos tipos, tamanhos e direcionamento de antenas. Existem dados de placa em seus equipamentos? Isto pode levar um hacker até o website do fabricante e lá ele obter mais informações. Ele pode interceptar seus sinais com um scanner comprado na “Santa Efigênia”, pode registrar seus sinais pela placa de som de seu computador, comprar um transceiver e atacar sua empresa repetindo o que ele intercepta.

Evite o ataque eletrônico através da encriptografia.

5. Na empresa usamos WEP (Wired Equivalent Privacy) e isto é muito seguro.

WEP possui buracos. Embora seja possível confiar para aplicações residenciais e de escritórios, não se pode confiar para controle industrial ou de um COS. Deve-se adicionar uma segunda camada, como por exemplo encriptografia AES de 128 ou 256 bits.

6. É muito caro investir na segurança do sistema da empresa.

Os equipamentos que estão instalados em sua empresa provavelmente possuem muitas características de segurança que não estão sendo usadas, como senhas, contatos de alarme, etc. Além disto, um transceiver SEL para fornecer encriptografia custa menos de R\$ 2.000,00 e pode ser fundamental para a segurança de uma subestação ou de um religador numa rede de distribuição.

7. Não usamos rede sem fio porque não é segura.

Enquanto afirmamos que WEP não é seguro, existem transceivers para rede sem fio que adicionam uma segunda camada de segurança e são muito seguros. Não despreze a segurança e comodidade de operar equipamentos através uma rede sem fio (para controlar religadores, chaves e disjuntores).

8. O Departamento de Informática é o responsável por segurança cibernética. Isto não faz parte de meu trabalho.

Eles podem não estar cientes dos diversos meios de comunicação em usinas e subestações. As equipes responsáveis por comunicação, medição, relés, SCADA, esquemas de controle de emergência e também a equipe de informática da empresa precisam estar focadas em segurança, de forma individual e em conjunto.

9. Deveria haver uma norma para cobrir tudo isto.

Independentemente da importância de normas, é necessário que todos estejam cientes de ameaças. Além disto, as normas ficam e as ameaças estão sempre em constante mudanças. Medidas de segurança devem se tornar um hábito e não simplesmente para atender normas. Aquelas pessoas mais próximas dos ativos de uma empresa é que estão em melhor condição de visualizarem e apontarem as necessidades.

10. Isto não pode acontecer conosco.

Pode!