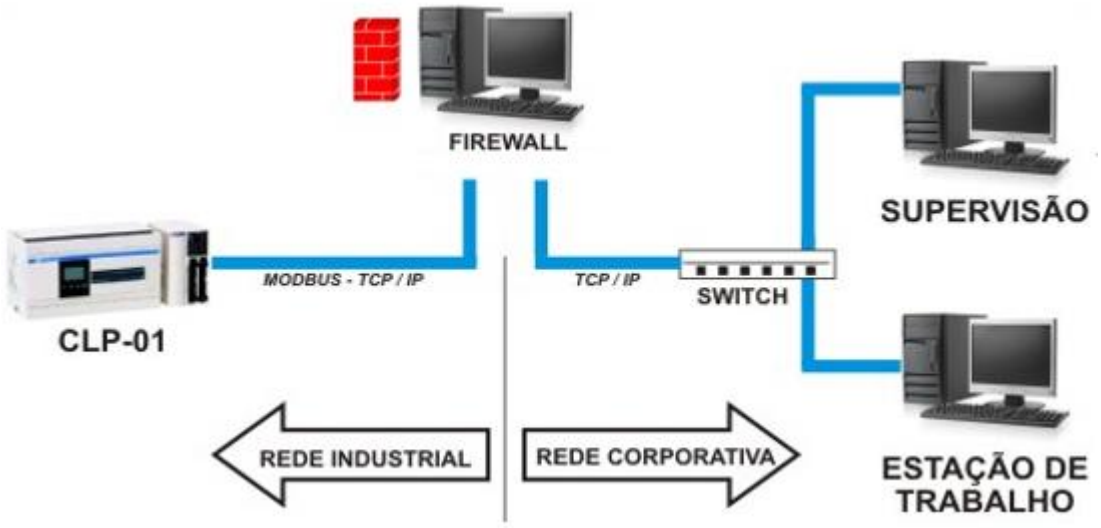
Engenharia de Controle e Automação – 9º Período
Disciplina: Aspectos de Segurança em Automação
Professor: José Maurício S. Pinheiro

AULA 4: Segurança em Automação

1. Interligação de Sistemas Corporativos e de Automação

O ambiente de automação industrial, antes isolado do ambiente corporativo das empresas, passa por uma grande e constante evolução tecnológica e atualmente é uma necessidade que esses dois ambientes sejam interligados e compartilhem informações, pois é necessário que sistemas inteligentes como sistemas de otimização de processo e gerenciamento de produção sejam alimentados com essas informações.
A interligação da rede de automação industrial com a rede corporativa é cada vez mais necessária do ponto de vista de recebimento de informações para gestão e planejamento estratégico das empresas, seja para obter informações dos indicadores de produção industrial ou para suportar o processo de cobrança para o consumidor final dos serviços prestados e produtos fornecidos, por exemplo.
O principal receio dos administradores de ambientes de automação industrial, cujas redes precisam ser interligadas, é a ameaça de indisponibilidade do seu parque industrial, com um potencial acesso indevido ou a proliferação de vírus. Porém, não se deve deixar de incluir como preocupação no ambiente de automação industrial, o acesso indevido proveniente de outras origens à rede de automação, como a Internet e demais redes de automação interligadas.



Atualmente é possível comunicar vários equipamentos da automação com uma rede corporativa, podendo comunicar um CLP com um sistema ERP ou com um sistema supervisor em um computador qualquer da rede. Isso pode ser feito de duas maneiras: todos os equipamentos da automação devem estar

interligados na mesma rede corporativa e comunicando-se através do protocolo TCP/IP, ou o CLP possuir dois módulos de comunicação distintos, em que num módulo o CLP se comunica com os equipamentos da automação em um protocolo e meio físico qualquer, e no outro módulo, o CLP se comunica com a rede corporativa através da Ethernet utilizando o protocolo TCP/IP.
Muitas empresas estão criando métodos e normas internas para tentar combater e prevenir a falta de segurança, porém, é muito importante que haja uma interação entre a equipe de TI (Tecnologia da Informação) com a equipe de TA (Tecnologia da Automação) para que a rede possa ser projetada da melhor forma possível, unindo velocidade e segurança.

2. Ataques aos Sistemas de Automação

Existem diversas formas de atacar um sistema de automação industrial, seja na degradação de serviços da rede, ou na exploração de falhas. Alguns itens merecem destaque, como: propagação de códigos maliciosos, negação de serviços, exploração de falhas no sistema operacional ou a má configuração dos serviços de rede. A segurança interna entre os equipamentos da própria rede também deve ser levada em consideração, pois um usuário dentro da empresa pode ter acessos privilegiados a informações que não deveria ter, facilitando a liberação de vírus e roubo de informações.

3. Vulnerabilidades

É necessário saber como são classificadas as ameaças que podem causar impactos nos sistemas, comprometendo os princípios de segurança. As vulnerabilidades podem estar expostas no hardware, software, meios de armazenamento ou comunicação.
Deve-se primeiramente rastrear e eliminar as vulnerabilidades do ambiente de tecnologia de informação, após isso, será possível dimensionar os riscos aos quais o ambiente está exposto e definir as medidas de segurança mais apropriadas para o ambiente. Dentre as vulnerabilidades temos:

- **Vulnerabilidade da infraestrutura**: Instalações inadequadas, ausência de recursos para combates a incêndio, disposição desorganizada de cabos de redes, energia;
- **Vulnerabilidade do hardware**: Defeitos de fabricação, configuração de equipamentos, ausência de proteção contra acesso não autorizado, conservação inadequada de equipamentos;
- **Vulnerabilidade de software**: Caracteriza-se normalmente por falhas de programação, que permitem acessos indevidos ao sistema, liberdade de uso do usuário;
- **Vulnerabilidade dos meios de armazenamento**: CD-ROM, fitas magnéticas e discos rígidos, se utilizados de forma inadequada, seu conteúdo poderá estar vulnerável a uma série de fatores, como confidencialidade de informações;
- **Vulnerabilidade de Comunicação**: Abrange todo o tráfego de informações. O sucesso no tráfego de dados é um aspecto fundamental para a implementação da segurança da informação, como está também

associada ao desempenho dos equipamentos envolvidos. Ausência de sistemas de criptografias, por exemplo;

- **Vulnerabilidade Humana**: Relaciona-se a danos que as pessoas podem causar às informações e ao ambiente tecnológico. A maior vulnerabilidade seria o desconhecimento das medidas de segurança adotadas que são adequadas para cada elemento do sistema.

3.1. Vulnerabilidades em Sistemas SCADA

Os sistemas SCADA (*Supervisory Control and Data Aquisition*) – Sistemas de Supervisão e Aquisição de Dados, que em algumas aplicações são referidos como sistemas supervisórios, são responsáveis por coletar os dados de processo disponibilizados pelos equipamentos de controle (CLP's, remotas industriais e outros) e os apresentar em tempo real. Vulnerável a vários tipos de ataques, os sistemas SCADA gerenciam grande parte das infraestruturas industriais no mundo, mas pouca atenção foi dada à segurança cibernética contra estes sistemas, uma vez que se acreditava que estas redes eram praticamente imunes a ataques pela Internet. A exposição dos sistemas SCADA às ameaças aumenta, à medida que estes são conectados a um número cada vez maior de redes e sistemas para compartilhar dados e fornecer serviços on-line.

4. Ataques

Os ataques são eventos que podem comprometer a segurança de um sistema ou de uma rede. Podem ou não ter sucesso, se tiver, caracteriza-se por uma invasão ou uma ação que pode ter um efeito negativo.
Há duas categorias de ataques: a primeira envolve conexões permitidas entre um cliente e um servidor, ataques de canal de comando, direcionados a dados, a terceiros e a falsa de autenticação de clientes. Já a segunda, envolve ataques que trabalham sem a necessidade de se fazer conexões, injeção e modificação de dados, negação de serviços etc.

5. Conceitos de Segurança da Informação

Na gestão empresarial moderna, a informação é tratada como um importante ativo da empresa. Essa informação pode ser impressa, manuscrita, gravada em meios magnéticos, ou simplesmente ser do conhecimento dos funcionários (falada). Essas informações (ou ativos), também podem ser classificadas de acordo com o eventual impacto negativo gerado decorrente de acesso, divulgação ou conhecimento não autorizado. Podem, por exemplo, ser classificadas como confidenciais ou restritas, internas ou públicas.
A divulgação ou o conhecimento não autorizado desses ativos pode gerar impactos dos mais variados, dentre os quais cita-se: problemas financeiros, queda na produtividade, riscos para o negócio, perda de credibilidade, desgaste da imagem, etc. A Segurança da Informação, mais que um problema de utilização de tecnologias, deve ser encarada como a gestão inteligente da informação em qualquer ambiente.

Para atender essas expectativas de uma corporação, um sistema de segurança da informação deve atender aos objetivos básicos destacados a seguir:

- **Confidencialidade ou privacidade** – proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia;
- **Integridade dos dados** – evitar que dados sejam apagados ou alterados sem a permissão do gestor da informação;
- **Disponibilidade** – garantir o funcionamento do serviço de informação e acesso aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos e sistemas e política de backup;
- **Consistência** – certificar-se de que o sistema atua de acordo com a expectativa dos usuários;
- **Isolamento ou uso legítimo** – controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema;
- **Auditoria** – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e logs, que registram o que foi executado no sistema, por quem e quando;
- **Confiabilidade** – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado;
- **Legalidade** – a informação deve estar em conformidade com os preceitos da legislação em vigor.

6. Políticas de Segurança da Informação

As políticas de segurança da informação devem fornecer meios para garantir que as informações de uso restrito não serão acessadas, copiadas ou codificadas por pessoas não autorizadas. Uma das maneiras de se evitar o acesso indevido a informações confidenciais é através da codificação ou cifragem da informação, conhecida como criptografia, fazendo com que apenas as pessoas às quais estas informações são destinadas, consigam compreendê-las.
A Figura 1, representa um fluxo de informações e quatro ameaças possíveis para a segurança de um sistema de informação:

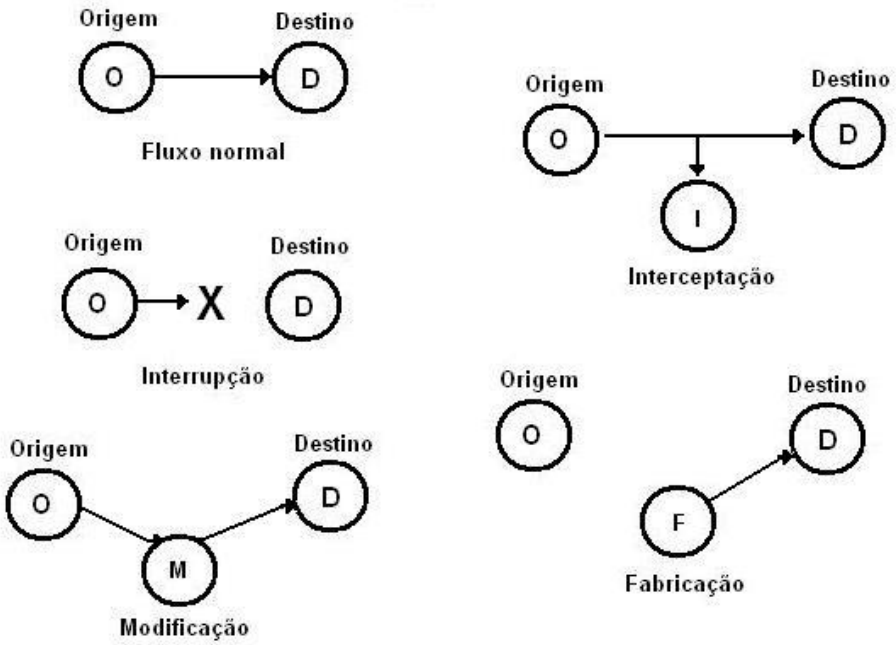


Figura 1 - Exemplos de ataques contra um sistema de informação

- **Interrupção:** Ataque na transmissão da mensagem, onde o fluxo de dados é interrompido. Um exemplo pode ser a danificação de componentes de hardware ou a queda do sistema de comunicação por sabotagem.
- **Interceptação:** Este é um ataque sobre a confidencialidade. Ocorre quando uma pessoa não autorizada tem acesso às informações confidenciais de outra. Um exemplo seria a captura de dados na rede, ou a cópia ilegal de um arquivo.
- **Modificação:** Este é um ataque à integridade da mensagem. Ocorre quando uma pessoa não autorizada, além de interceptar as mensagens, altera o conteúdo da mensagem e envia o conteúdo alterado para o destinatário.
- **Fabricação:** Este é um ataque sobre a autenticidade. Uma pessoa não autorizada insere mensagens no sistema assumindo o perfil de um usuário autorizado.

7. Critérios de classificação das informações

Os critérios de classificação definem qual o tratamento de segurança que uma informação receberá, ou seja, quanto será preciso investir em segurança para garantir a confidencialidade, integridade e disponibilidade dessa informação, objetivando sempre priorizar recursos. Para tanto, podemos classificar as informações quanto a:

- **Confidencialidade** – Classificar a informação levando em consideração a gravidade do impacto ou prejuízo que a revelação não autorizada da mesma trará para a organização. Podem-se definir três níveis de classificação quanto a confidencialidade:

  - Confidencial - é toda informação considerada de alto risco para a empresa, pois sua revelação não autorizada pode trazer graves prejuízos. Geralmente estas informações são acessadas pela alta administração da empresa (presidência, diretoria, superintendência);
  - Restrita – é toda informação considerada de médio e baixo risco para a empresa, pois sua revelação não autorizada pode trazer prejuízos a uma determinada área da empresa. Geralmente estas informações são acessadas pelas áreas envolvidas na geração e uso destas informações, pelos gestores da área e pela alta administração;
  - Pública – é toda informação considerada de nenhum risco para a empresa e sua revelação não autorizada não traz nenhum prejuízo. Estas informações são acessadas por todos os funcionários e pessoas externas à empresa.
- **Integridade** - Classificar a informação levando em consideração a gravidade do impacto ou dos prejuízos que a modificação não autorizada da informação trará. Podem-se definir dois níveis de classificação quanto à integridade:
  - Crítica – é toda informação de alto risco para a empresa. Esta informação não pode ser alterada sem prévia autorização;
  - Não Crítica – é toda informação que, se alterada sem prévia autorização, não representa nenhum risco para a empresa.
- **Disponibilidade** - Classificar as informações levando em consideração a gravidade do impacto ou dos prejuízos que a indisponibilidade da informação trará. Podem-se definir dois níveis de classificação quanto à disponibilidade:
  - Vital - é toda informação de alto risco para a empresa. Esta informação precisa estar sempre disponível;
  - Não Vital - é toda informação que em caso de indisponibilidade não representa nenhum risco para a empresa.
- **Classificação Padrão** - Todas as informações que não forem classificadas deverão entrar no nível padrão de classificação.

Por exemplo, numa rede de automação existem aspectos de segurança que devem ser observados com maior atenção: confidencialidade, integridade, autenticação, autorização, disponibilidade, auditoria. Todos os dados trafegados na rede têm uma origem e um destino, porém, esses dados podem ser interceptados, modificados e reenviados para seu destino, isso acontece em redes que não garantem a confidencialidade, integridade e autenticação de seus dados. Em outros casos, os dados são apenas interceptados e usados na espionagem e, assim, dados confidenciais podem ser obtidos facilmente. A autorização e disponibilidade garantem que cada tipo de usuário acesse somente os dados permitidos para sua função, ou seja, um usuário com senha para coletar dados do processo não poderá acessar a programação do CLP e modificá-la. A auditoria garante que todos os itens acima sejam cumpridos e checa o sistema para garantir sua integridade.

8. Diferenças entre Ambiente Industrial e Corporativo

A integração do ambiente industrial e o corporativo é um fato, porém, possuem características individuais. O ambiente industrial tem como prioridade a produção e a segurança humana, já o ambiente corporativo prioriza o desempenho e a integridade dos dados (Figura 2).

Figura 2 - Prioridades nos ambientes industrial e corporativo

O ambiente corporativo prioriza a confidencialidade dos dados, protegendo contra acessos não autorizados, também a integridade e a disponibilidade dos dados. Já o ambiente industrial tem como prioridade a disponibilidade, pois não pode tolerar pequenas interrupções, que podem causar grandes perdas, sejam elas de produção ou danos ao equipamento. Seguindo a ordem de prioridades vem a integridade e a confidencialidade, protegendo e garantindo que os dados não sejam danificados ou acessados por pessoas não autorizadas.

9. Programa de Segurança em Redes Industriais

Para aumentar o nível de segurança em redes de automação industrial é necessário implementar um programa abrangente e cíclico de ações e projetos que englobem todos os tipos de ativos (tecnologias, processos, ambientes físicos, pessoas) que suportam diretamente ou indiretamente tais ambientes.
A primeira atividade que deve ser executada está relacionada ao conhecimento detalhado do escopo do ambiente que se pretende proteger, cuja norma ISO 31000 (Gestão de Riscos) denominou de “Definição do Contexto”, que se dá pelo Inventário de Ativos (técnicos e não técnicos). Atrelada a esta atividade inicial há de se inventariar também as potenciais Ameaças (técnicas e não técnicas) relacionadas ao ambiente de automação industrial.
Conhecido todo o ambiente, chega o momento de se analisar detalhadamente os ativos que compõem a automação industrial, baseada em Melhores Práticas em um conjunto de normas legais (leis, normas, decretos etc.) para Conformidade do ambiente.
Uma das atividades de análise comumente praticada pelas empresas é o teste de invasão, projeto que simula um ataque externo (oriunda da Internet) ou interno (pela rede interna corporativa ou de automação da empresa) ao ambiente tecnológico da planta industrial evidencia, caso haja sucesso na

“invasão”, as fragilidades e vulnerabilidades do ambiente alvo do teste, recomendando medidas de segurança mitigatórias.

9.1. Avaliação e Tratamento de Riscos

Com a análise realizada, uma ação de Avaliação de Riscos precisa ser realizada a fim de priorizar o conjunto de projetos a serem desenvolvidos e implementados em um Plano de Tratamento dos Riscos, ou mesmo identificar quais os riscos serão aceitos e/ou transferidos. O Plano de Tratamento dos Riscos envolve vários projetos e ações mitigatórias classificadas como, por exemplo:

- Técnicas (implantação de ferramentas, customizações, correções no ambiente etc.);
- Mudança Comportamental (Treinamento técnico e para usuários, Campanhas de Divulgação etc.);
- Normativa (Elaboração de Diretrizes, Normas, Procedimentos Operacionais e Instruções de Trabalho);
- Continuidade de Negócio (Análise de impacto no negócio, Planos de Contingência e de Negócio etc.).

Independentemente do tamanho das unidades industriais é necessário monitorar constantemente (24 horas x 7 dias por semana) o ambiente, dando respostas rápidas aos alertas, eventos e incidentes que afetam a automação industrial que podem impactar o negócio, transformando em desastre ou catástrofe, se nada for realizado. Portanto, um Centro Integrado de Comando e Controle deve ser implementado com pessoas capacitadas, sistemas integrados de detecção e alertas, infraestrutura adequada com recursos visualização para tomada de decisão e controle.

10. Medidas para Reforçar a Segurança em Automação

Muitas medidas podem ser tomadas para reforçar a segurança em redes de automação, porém, é preciso analisar as vulnerabilidades do sistema para conhecer melhor as decisões a serem tomadas. Abaixo segue uma relação de algumas das principais iniciativas.

- Desenvolvimento e implementação de políticas de segurança baseadas nos sistemas de automação;
- Instalação em locais estratégicos de firewall e outros mecanismos contra softwares maliciosos;
- Controle dos serviços de acesso remoto, permitindo sessões criptografadas;
- Planejamento de atualizações de softwares como sistema operacional, antivírus, firewall e outros softwares específicos;
- Realização de treinamentos para que todos os usuários da rede possam saber de suas responsabilidades e deveres perante a rede corporativa;
- Manutenção do tempo de sincronismo dos equipamentos da rede;

- Criação de políticas de backup;
- Segmentação física e lógica da rede;
- Permitir somente os serviços necessários no equipamento, desabilitando outros serviços que podem servir de porta de entrada para vírus e acesso de pessoas não autorizadas;
- Utilização de tecnologias capazes de certificar os usuários da rede;
- Utilização de sistemas capazes de detectar a presença de usuários não autorizados na rede;
- Criação de uma equipe de análise e auditoria dos dados trafegados na rede que possam tornar o processo de segurança sempre atualizado.