Cibersegurança industrial: a chave para o desenvolvimento econômico

Os ambientes industriais deixaram de ser um espaço exclusivamente tangível e grande parte da atividade produtiva tornou-se uma infraestrutura digital. Protegê-la é fundamental para o sucesso das empresas e para o equilíbrio econômico global.

A interconexão de dispositivos e a automatização de processos em ambientes industriais geraram, sem dúvida, melhorias notáveis em eficiência e produtividade. No entanto, essa mesma conectividade expôs vulnerabilidades a ataques cibernéticos que podem ter consequências graves para as empresas produtoras, colaboradores – como, por exemplo, fornecedores ou cadeias logísticas –, e até mesmo clientes.

Os especialistas da área trabalham para melhorar os sistemas de prevenção e ação, conscientes de que os desafios do futuro serão cada vez mais complexos. Conversamos sobre isso com **Francisco Lázaro Anguis, professor associado da Escola Técnica Superior de Engenheiros** de Telecomunicações da Universidade Politécnica de Madri (UPM).

A transformação dos sistemas operacionais

“No setor industrial, encontramos os ativos conhecidos como **Sistemas OT (Operational Technology),** que são **as tecnologias de gestão de processos de produção”,** explica Lázaro Anguis. O termo OT abrange desde sistemas de automação e controle industrial (ou ICS, Industrial Control Systems) até processadores de dados e sistemas SCADA (Supervisor Control and Data Acquisition). Os sistemas caracterizam-se, como explica o especialista, por serem “equipamentos que interagem com processos físicos (sensores e atuadores), fornecem os sistemas de controle industrial e operam em condições extremas”.

Lázaro Anguis destaca como os sistemas OT, que até poucos anos atrás estavam isolados da rede pública de Internet e agora estão sendo integrados em redes mais abertas. Isto envolve o uso de sistemas operacionais comerciais padrão, como Windows ou Linux, e a adoção de redes Ethernet para comunicação. Além disso, estão sendo realizados trabalhos de manutenção remota, aproveitando a infraestrutura de TI existente.

Neste contexto, é fundamental **o controle que tais sistemas exercem sobre elementos físicos importantes, como tubulações, motores elétricos e ferrovias,** além da relevância estratégica e a migração para tecnologias mais comuns e, portanto, com vulnerabilidades conhecidas.

“As ameaças respondem a diferentes motivos e vão **desde o interesse econômico** (materializando-se com ataques de ransomware, por exemplo) **aos geopolíticos** (pela negação

de serviço ou destruição de informações, entre outros)", afirma o professor da UPM. Os objetivos em ambos os casos seriam ativos como os controles de abertura e fechamento de interruptores, o aumento da rotação de centrífugas, – como no ataque do Stuxnet a usinas nucleares –, os misturadores das estações de tratamento de água para alterar o abastecimento de água ou os sensores e atuadores de temperatura, que afetam tanto a produção quanto a extinção de incêndios.

Fortalecer a cibersegurança industrial

Algumas das vulnerabilidades mais comuns que afetam os ativos em ambientes industriais são causadas por equipamentos obsoletos ou inseguros por falta de atualização, sobre a falta de segmentação – como isolamento em redes específicas –, ou falta de proteção contra ataques intencionais. Um **roteiro básico para criar um espaço seguro** passaria, segundo o especialista, por algumas fases essenciais:

- **Treinamento em cibersegurança.** O pessoal que utiliza os sistemas deve ser treinado em questões relacionadas com esse tema. Além disso, é recomendável designar uma pessoa ou equipe responsável pela cibersegurança dentro da organização.
- **Identificar obrigações legais.** Conhecer e cumprir a regulamentação existente no âmbito industrial implica estabelecer um quadro normativo e processual adequado que oriente as ações dentro da organização.
- **Inventário de ativos completo e correto.** Consiste em ter um registro de todos os recursos existentes, incluindo equipamentos, dispositivos e softwares. Isso ajuda a ter melhor controle sobre eles e facilita a implementação de medidas de segurança adequadas.
- **Realizar análises de risco formais.** Envolve avaliações sistemáticas dos riscos cibernéticos enfrentados pelos sistemas industriais, como identificar possíveis ameaças ou avaliar sua probabilidade de ocorrência para, assim, estabelecer controles de segurança que mitiguem esses riscos.
- **Monitorar comunicações e sistemas.** O objetivo é detectar e enfrentar possíveis incidentes de segurança em tempo real. Isso implica monitorar as comunicações e o tráfego de rede, bem como fazer o monitoramento contínuo dos sistemas em busca de comportamentos anormais ou indicadores de comprometimento.

Uma das principais complexidades dessa integração é a dicotomia – ainda não resolvida, segundo o especialista –, de **duas abordagens de segurança:**

1. safety, proteção contra riscos acidentais,
2. e security, prevenção de danos intencionais.

No mundo industrial, um sistema certificado no dia X é seguro no dia X+1 se não tiver sido modificado – caso em que deve ser certificado novamente. **No mundo cibernético,** um produto que é seguro no dia X continuará sendo no dia X+1, desde que esteja atualizado. O ciclo de vida previsto dos sistemas OT (de muito longo prazo) no ambiente de TI (onde a transformação é contínua) é um **desafio** para a gestão de riscos.

Um futuro combinado com a tecnologia

Enfrentar esse desafio só é possível, segundo Lázaro Anguis, a partir **da integração das melhores práticas em cibersegurança com os processos de gestão de crise e continuidade do negócio,** projetando estratégias para enfrentar incidentes em infraestruturas essenciais. Isso garante uma resposta eficaz e uma rápida recuperação contra possíveis ameaças.

Os perigos que ameaçam os ambientes industriais serão cada vez mais complexos, ainda que em paralelo com os riscos estejam sendo desenvolvidos sistemas de previsão e prevenção mais eficazes e eficientes. A tecnologia avança muito rapidamente e as empresas absorvem novos contextos a serem protegidos, como Blockchain, Internet das Coisas ou estações Cloud. "**Se tivesse que escolher uma ameaça futura, a inteligência artificial seria** uma adversária, ou seja, o uso que os criminosos farão dela para facilitar seus ataques. Paradoxalmente, a principal contramedida como aliada da cibersegurança será a própria IA, ao permitir detectar e responder mais rapidamente aos ataques", conclui.

Colaborou neste artigo:

Francisco Lázaro Anguis, professor associado na ETSI de telecomunicações da Universidade Politécnica de Madri e em diversos cursos de Mestrado em Cibersegurança e Proteção de Dados.

Em sua extensa trajetória, destacam: atuação como membro do Fórum Nacional de Cibersegurança, qualificação pelo Ministério do Interior como Diretor de Segurança e os prêmios ASLAN, SIC e Huella, entre outros.