

Por Thais Santi  
Especial para *O Papel*

# SEGURANÇA CIBERNÉTICA NA INDÚSTRIA 4.0

Com aumento dos ataques direcionados às indústrias, fornecedores de tecnologia atualizam softwares de automação com novos recursos que garantem maior segurança para o processo

**S**e por um lado a base da **Indústria 4.0** passa pela conectividade, buscando dados do nível zero de produção (chão de fábrica), interligando sistemas e soluções até os níveis corporativos, por meio de uma plataforma de automação de processos centralizada e integrada, por outro, a quantidade de informações expostas é muito maior, atraindo ataques direcionados às indústrias.

Conforme Pesquisa Anual de Riscos Globais de Segurança de Tecnologia da Informação de 2017, realizada pela B2B International e pela Kaspersky Lab, 28% das 962 indústrias pesquisadas sofreram tais ataques, entre a profusão de ameaças, nos últimos 12 meses. Isso representa 8 pontos percentuais a mais que no ano pas-

sado, quando apenas 20% das organizações industriais vivenciaram essa situação.

Com isso, a segurança cibernética tem se tornado um tema relevante para a Automação Integrada. “Desde a migração dos Sistemas de Automação para o uso de plataformas abertas de TI, como Servidores e Workstations baseadas em Windows, o risco de ataques cibernéticos vem sendo uma preocupação. No entanto, isso não deve ser encarado como uma barreira para que as empresas façam uso da tecnologia e, com isso, atinjam seus objetivos de otimização e redução de custos”, disse Marcos Hillal, gerente de Produto da divisão Industrial Automation da ABB Brasil.

O gerente lembra que qualquer comprometimento nesse sentido pode trazer resultados negativos. “Isso vale não apenas do ponto de vista financeiro para as empresas, mas também do ponto de vista de exposição da imagem no mercado e da segurança das pessoas e da comunidade na qual elas se integram”, alerta Hillal.

Para as empresas, ao realizarem o seu planejamento de segurança, o principal foco deve ser garantir que o Sistema de Backup de Dados, atualização de *patches* de segurança – espécie de programa criado para atualizar ou corrigir um *software* de forma a melhorar sua usabilidade ou performance – e versões de Sistemas Operacionais (como Windows, por exemplo) estejam sempre nas versões mais recentes. “Versões antigas de Sistemas Operacionais podem se tornar uma porta aberta para a entrada de *softwares* maliciosos e vírus que irão comprometer a segurança da operação e da informação”, apontou o profissional.

Quando se fala em um projeto de instalação de segurança cibernética, especialmente em uma grande planta, como nas indústrias de papel e celulose, por exemplo, pode-se dizer ainda que envolverá toda a Política

DIVULGAÇÃO ABB BRASIL



Hillal: “Versões antigas de Sistemas Operacionais podem se tornar uma porta aberta para a entrada de *softwares* maliciosos e vírus que irão comprometer a segurança da operação e da informação”

de Segurança de Tecnologia da Informação (TI) e a de Tecnologia de Automação (TA), como é o caso da Klabin. “Dentro disso, temos algumas etapas base, como a escolha dos equipamentos dessa segurança cibernética, como *firewalls*, *softwares* de antivírus, instalações customizadas e controle de transferência de dados; além da capacitação de profissionais”, explica Sinésio Barberini, gerente de Projetos da Klabin.

O foco nas pessoas também foi destacado como relevante pelo gerente de produto da ABB. “De nada adianta um sistema de segurança bem instalado se o time de manutenção e operação não for adequadamente treinado e conscientizado da relevância do tema da segurança cibernética e das políticas de segurança da informação da empresa”. Além disso, para garantir que os dados de produção estejam protegidos e que a rede é segura, Hillal conta que a ABB pensa o tema de forma sistêmica, através do olhar da tecnologia e das pessoas que irão implementar os projetos.

Do ponto de vista tecnológico, Hillal cita a plataforma de Digitalização, o *software* ABB Ability™ 800xA, que teve a segurança da informação como um tema-chave na sua concepção, fazendo uso de avançados mecanismos de proteção a ataques externos. O *software* é uma plataforma SDCD (Sistema Digital de Controle Distribuído) completa de Controle e Automação de Processos específica para indústrias de papel e celulose.

As últimas versões do ABB Ability™ 800xA contam com recursos, como uso do sistema operacional Microsoft mais recente; mecanismos de assinatura digital; mecanismos de Whitelisting, que permitem que apenas códigos pré-aprovados funcionem, automaticamente, negando a entrada de qualquer executável que não esteja cadastrado; e atualização constante de *patches* de segurança e arquivos de definições de vírus.

Tal *software*, o ABB Ability™ 800xA, foi recentemente implantado na Unidade Monte Alegre, da Klabin, em Telêmaco Borba-PR. Barberini conta que todas as unidades da Klabin possuem sistemas de segurança cibernética e tecnologias de automação. “No caso da Unidade Monte Alegre, visando também a avançar no uso de tecnologias da **Indústria 4.0**, os equipamentos da ABB instalados já englobam a segurança da informação necessária ao que são destinados, tendo sincronia e contribuindo com a segurança cibernética da fábrica em sua totalidade”, justificou.

Na prática, isso representa a disponibilidade de grande volume de dados para equipes de manutenção e gestores, acessíveis em tempo real por meio da in-



ternet. “Este fluxo precisa acontecer em um ambiente extremamente seguro para evitar quaisquer possibilidades de acessos não autorizados”, complementa o gerente de projetos da Klabin.

Sobre a intenção de ampliar a segurança para outras áreas da planta ou de outras unidades e da avaliação de risco de cada operação, Barberini aponta que na Klabin a segurança aplicada aos sistemas de controles industriais é um processo dinâmico, no qual as áreas de Tecnologia de Automação (TA) e Tecnologia da Informação (TI) avaliam rotineiramente os riscos e já indicam as melhorias. “Com a modernização planejada das plantas, novos controles são inseridos e/ou atualizados constantemente. Sistemas das décadas de 1990, 2000 ou anteriores, por exemplo, que em sua origem atuavam de forma isolada e praticamente imunes aos potenciais ataques cibernéticos, quando são modernizados, trazem embarcadas todas as funcionalidades da TI e TA, exigindo, dessa forma, que os projetos já contemplem todas as soluções de segurança cibernética.

“Com relação a avaliação de riscos, a Klabin efetua periodicamente análises envolvendo procedimentos de acesso, equipamentos e *softwares* de proteção”, destacou o profissional da companhia. Tais análises de risco também podem ser realizadas em parceria com a ABB, que desenvolveu o ABB Cyber Security Fingerprint. Trata-se de um serviço de consultoria que, por meio de uma ferramenta não invasiva, pode analisar qualquer sistema de controle e identificar os principais *gaps* de segurança. “A partir daí, recomendações e planos de ação são criados e implementados, conforme a demanda de cada caso”, concluiu Hillal. ■

**Barberini: “Com relação a avaliação de riscos, a Klabin efetua periodicamente análises envolvendo procedimentos de acesso, equipamentos e *softwares* de proteção”**