INTERATIVIDADE CRESCENTE ENTRE **SISTEMAS OPERACIONAIS** E DE **TECNOLOGIA** REQUER **PLANEJAMENTO** DE **CIBERSEGURANÇA**

A realidade atual reflete ambientes fabris cada vez mais conectados à internet e aos sistemas de tecnologia e de conectividade das empresas, fator que demanda incrementos dos níveis de segurança cibernética ao ambiente de produção, a fim de minimizar os riscos de ataques aos sistemas ciberfísicos.

A estratégia de segurança cibernética para um ambiente de produção, também conhecido como OT (Operational Technology), começa pela convergência com a área de IT (Information Technology), conforme explica Fernando Lobo, vice-presidente de Tecnologias Avançadas e Tecnologia Operacional da Fortinet para América Latina e Canadá, empresa americana líder em segurança cibernética que desenvolve e comercializa soluções de cibersegurança empresarial, incluindo *firewalls*, segurança de rede, segurança em nuvem, operações de segurança, além de serviços avançados de segurança cibernética. "De maneira geral, a Indústria 4.0 foi e é o que está levando à necessidade de implementação de cibersegurança nos ambientes industriais. Até então, tínhamos o chamado *air gap*: a produção era separada do ambiente corporativo, pois não havia necessidade de troca de informação em tempo real. Quando essa realidade mudou, o mundo de cibersegurança, antes focado em IT, começou a olhar mais atentamente para o mundo de OT."

Dados do relatório global sobre o Estado da Tecnologia Operacional e Cibersegurança de 2025 da Fortinet mostram que os ataques cibernéticos que comprometem os sistemas de OT estão em ascensão: 47% dos entrevistados sofreram pelo menos uma violação de segurança cibernética no último anos, enquanto 29% relataram três ou mais violações. Os dados da pesquisa também mostram um aumento, ano a ano, nas invasões que afetaram tanto os sistemas de TI como de OT, subindo de 49% para 60%.

Na entrevista a seguir, Lobo e Leonardo Moreira (gerente de Engenharia para Desenvolvimento de Negócios em OT da Fortinet para América Latina e Canadá), abordam as formas de estruturar estratégias de implementação de segurança cibernética para os ambientes fabris, passam pelos principais desafios enfrentados atualmente e indicam as melhores práticas para superá-los.

POR CAROLINE MARTIN
Especial para *O Papel*

DIVULGAÇÃO FORTINET

Fernando Lobo: “Neste momento da Indústria 4.0, as necessidades de cibersegurança de um ambiente industrial são básicas, a começar pela segmentação, uma vez que é comum vermos todas as equipes conectadas em uma mesma rede”

DIVULGAÇÃO FORTINET

Leonardo Moreira: “É preciso enfatizar o quanto as condutas corretas são capazes de reduzir riscos e até mesmo promover melhorias de produtividade industrial e demais indicadores”

***O Papel* – Inserida no contexto evolutivo da Indústria 4.0, o setor de celulose e papel tem adotado uma série de tecnologias de automação, seja com finalidade preditiva seja com outros propósitos de análise de dados do processo. As medidas de proteção e segurança cibernética também avançaram nos últimos anos?**

Fernando Lobo, vice-presidente de Tecnologias Avançadas e Tecnologia Operacional da Fortinet para América Latina e Canadá – Há uma grande diferença entre segurança de IT e a segurança voltada às tecnologias operacionais. Se uma folha de pagamento falhar, não botamos em risco nenhum ser humano, ao passo que, se um *pipe* que está processando celulose falhar, além de haver risco para a vida humana, a fábrica pode sofrer uma parada e apresentar um tempo de recuperação de meses. O impasse entre as áreas ocorre pelo fato de o mundo de IT estar preocupado em disponibilidade de recurso e dinamismo, enquanto o mundo de OT, muito mais focado em risco e conformidade. Na prática, portanto, os conceitos de segurança têm de passar a ser adaptados para o mundo industrial. Neste momento da Indústria 4.0, as necessidades de cibersegurança de um ambiente industrial são básicas, a começar pela segmentação, uma vez que é comum vermos todas as equipes conectadas em uma mesma rede.

Leonardo Moreira, gerente de Engenharia para Desenvolvimento de Negócios em OT da Fortinet – Cerca de 80% dos clientes atendidos, considerando Canadá, Brasil e outros países da América Latina, não fazem nenhum tipo de segmentação. Costumo brincar que o computador de um profissional de recrutamento, por exemplo, pode modificar a configuração da PLC (Controlador Lógico Programável, dispositivo eletrônico digital usado para automatizar e controlar processos industriais) sem nenhuma dificuldade.

Lobo – O primeiro aspecto, quando iniciamos um trabalho de cibersegurança, é a conscientização sobre essa necessidade de segmentação. O segundo aspecto diz respeito à quantidade de terceiros que se conectam para fazer uma eventual manutenção da planta ou uma atualização de um processo. É necessário ter um controle de acesso que determine quem está se conectando. O contexto atual está mudando bastante, é preciso considerar que as tecnologias devem ser adaptadas às necessidades de cada operação. Partimos de uma mesma plataforma tecnológica, mas adaptada ou instalada de maneira coerente com o ambiente de cada operação.

***O Papel* – Falando especificamente das alternativas de segurança direcionadas à indústria de celulose e papel, qual é o arsenal tecnológico que se encontra disponível atualmente?**

Lobo – A Fortinet dispõe de um espectro gigante. Para incorporá-lo no dia a dia operacional de cada empresa, montamos um processo que chamamos de Cyber Security Maturity Assessment.

Moreira – Em uma visita agendada entre o cliente e os nossos engenheiros, mapeamos o nível de maturidade em que as unidades se encontram e traçamos uma jornada de longo prazo. A partir de dez perguntas estabelecidas para os cinco domínios que avaliamos, conseguimos entender quais são os sistemas e tecnologias adotados pela planta, e identificamos as necessidades relacionadas ao trabalho de segmentação, controle de acesso, revisão de *logs*, gestão de riscos, entre outros. O mapeamento é útil para posicionarmos o cliente sobre o nível de cibersegurança em que ele se encontra e para oferecer meios e ferramentas para elevar tal maturidade. A média de maturidade do setor industrial brasileiro como um todo, hoje, é de 0,87, numa escala de zero e cinco. Ao montar uma jornada baseada em boas práticas de cibersegurança para cada cliente, é possível avaliar as oportunidades de melhoria, acompanhar o crescimento em cada aspecto e mensurar a geração de valor do processo.

***O Papel* – Considerando um cenário ideal, de uma empresa que atenta às práticas de segurança cibernética, ainda assim existem áreas mais vulneráveis a ataques cibernéticos? Quais são os principais riscos mapeados hoje?**

Lobo – Antes de tudo, é importante comentar que há um aspecto primordial no trabalho de implementação de cibersegurança, que é a conscientização de todas as pessoas envolvidas. Se não partirmos daí, não adianta implementar nenhuma tecnologia, considerando que alguém vai eventualmente deixar a porta aberta. Partimos, portanto, da conscientização de que a porta deve ser mantida fechada.

Moreira – Em linhas gerais, não existe um sistema mais ou menos vulnerável, mas os sistemas que fazem algum tipo de interação com a parte de IT das empresas, precisam ser protegidos. Quanto mais interação esses sistemas têm com as redes de IT, mais chance de um atacante conseguir fazer esse salto do mundo de IT para o de OT. Outro tema muito importante são os sistemas legados. É comum encontrarmos equipamentos que estão rodando nas plantas há mais de 20 anos, por exemplo, e funcionam bem. Contudo, isso acaba gerando um risco adicional, uma vez que tais equipamentos muitas vezes não têm as contramedidas de cibersegurança que devem ser implementadas atualmente. Quanto mais antigo o equipamento, mais vulnerável ele está, uma vez que é pouco provável que uma empresa pare uma linha de produção para atualizar esses dispositivos. Do ponto de vista de cibersegurança, existem maneiras de blindar esses ambientes. Então, avaliamos quais tipos de vulnerabilidade temos na planta e identificamos quais controles compensatórios podemos acrescentar, minimizando os riscos e

chegando a um nível aceitável pela corporação. Eu diria, portanto, que não há áreas ou sistemas específicos mais vulneráveis, mas sim, que a interseção com o mundo exterior é extremamente crítica, exigindo a adoção de tecnologias e monitoramento constantes.

***O Papel* – Quais são as condutas tanto por parte dos *players* da indústria de celulose e papel quanto de seus fornecedores de equipamentos que contribuem para a minimização destes riscos?**

Lobo – É bastante comum os fornecedores de equipamentos industriais terem uma equipe de cibersegurança. O nosso time tem uma interface muito grande com esses fornecedores, considerando que eles almejam entregar plantas fabris intrinsecamente seguras. O time Fortinet atua também na certificação dessas soluções. Atualmente, a indústria de cibersegurança e a indústria de equipamentos tecnológicos voltados à indústria trocam informações o tempo todo.

> **ATUALMENTE, A INDÚSTRIA DE CIBERSEGURANÇA E A INDÚSTRIA DE EQUIPAMENTOS TECNOLÓGICOS VOLTADOS À INDÚSTRIA TROCAM INFORMAÇÕES O TEMPO TODO**

***O Papel* – Como vocês avaliam o posicionamento da indústria brasileira sob o viés da segurança cibernética? É possível posicionar o setor de celulose e papel nesse contexto da indústria nacional ou até mesmo em relação às práticas internacionais?**

Lobo – O Brasil não é um *early adopter*, assim como os demais países da América Latina. Ou seja, primeiro, não são países que adotam as melhores práticas. Contudo, considero isso um aspecto positivo, sob o ponto de vista da minha trajetória de 40 anos na indústria de IT. Muita tecnologia é usada precocemente e acaba sendo deixada de lado com o tempo. Quando um país não toma essa dianteira, adota tecnologias mais sólidas, já consolidadas.

Moreira – Concordo e adiciono que existe um nivelamento, avaliando o viés da cibersegurança da nossa indústria com as de outros países. É claro que a possibilidade de aportar mais investimentos traz mais oportunidades de adoção de tecnologias, mas muitas empresas da região, com atuação global, incluindo do setor de celulose e papel, têm dedicado atenção às medidas de cibersegurança e destinado investimentos massivos à área.

***O Papel* – Quais tendências vocês vislumbram para os próximos anos e de que forma a indústria nacional deve se preparar para acompanhar tais tendências de forma competitiva?**

Lobo – Essa é uma pergunta interessante e não tem como respondê-la sem falar sobre os desdobramentos trazidos pela Inteligência Artificial (IA). A Agentic AI aponta para uma tendência da IA passar a tomar decisões sozinha, aspecto que tende a influenciar a indústria como um todo. Será possível, por exemplo, contar com IA para criar um produto endereçado à solução de um problema que afeta a indústria. Logo, a concretização das práticas de IA vai mudar a indústria e consequentemente a cibersegurança, já que será necessário proteger as informações de IA que estão correndo dentro da indústria e que impactam diretamente a linha de produção. A evolução, em linhas gerais, é adotar a IA tanto na indústria como na cibersegurança. Outra tendência a ser considerada é a falta expressiva de profissionais especializados em cibersegurança. Temos hoje um dos mais completos e maiores programas de treinamento em cibersegurança do mundo, que é o Fortinet Training Institute, além de termos a meta de o treinar 1 milhão de pessoas em segurança cibernética até 2026. Já passamos de 63%. No entanto, mesmo ao atingirmos essa meta, não devemos cobrir o gargalo visto hoje e que, ainda, possui perspectiva de crescimento. Esse desafio só será resolvido quando a cibersegurança fizer parte de qualquer tarefa e projeto tecnológico nascendo com eles.

Moreira – Eu vim do mundo de cibersegurança de IT e migrei para o mundo de cibersegurança de OT. Porém, existe um outro perfil de profissional que faz outro caminho: vem do mundo de OT, normalmente com formação em Engenharia de Produção, Mecânica, Eletromecânica, e migra para o mundo de cibersegurança. Muitas dessas formações pregressas sequer abordavam os temas relacionados a cibersegurança, tendo em vista que é uma pauta mais atual. Convencer um engenheiro que está no mercado de trabalho há três ou quatro décadas de que as questões de cibersegurança são indispensáveis para o negócio e para o funcionamento da empresa como um todo, pode ser bastante desafiador. De qualquer forma, é preciso enfatizar o quanto as condutas corretas são capazes de reduzir riscos e até mesmo promover melhorias de produtividade industrial e demais indicadores. ■