Entrevista com Paul Schwyter (ABB): “Cibersegurança começa a entrar na pauta das empresas de energia do Brasil”

COUTO, Fábio. “Entrevista com Paul Schwyter (ABB): ‘Cibersegurança começa a entrar na pauta das empresas de energia do Brasil’”. Brasil Energia. Rio de Janeiro, 8 de maio de 2017.

Potencial de mercado para a cibersegurança – “A cybersecurity não é uma questão específica do Brasil, é um tópico ainda crescente pelo mundo. O desafio é descobrir o que de fato motiva a adoção do cybersecurity, o que está acontecendo no mercado. Eu acho que um dos motivos é que no passado, no mercado de utilities, nós tínhamos as comunicações tradicionais com a SDH e a PDH que eram menos vulneráveis a ataques. Elas tinham menos recursos, mas eram menos vulneráveis. Agora, as utilities estão se movendo, algumas mais rápidas, outras mais lentas, para a comutação de pacotes, como a Ethernet.

Algumas mais rápidas, outras mais lentas, mas todas estão se movendo para essas redes baseadas em comutação de pacotes, que é a tecnologia Ethernet. O MPLS é uma tecnologia que também roda sob a Ethernet e quando aumenta essa gama de aplicação usando a Ethernet, as vulnerabilidades começam a vir; tem mais poder, mas também tem mais vulnerabilidade.

Política de segurança da informação e uso de redes – Se não for estabelecida uma a política para que as pessoas sejam treinadas nas empresas sobre como lidar com informações sensíveis, não importa que tipo de curso técnico e produto você vai usar, se alguém simplesmente infringe uma lei e deixa alguma informação vazar, não importa a tecnologia. Por isso é super importante o fator pessoal. Na Europa, a política de tratamento do cybersec já está tão adiantada que os gerentes das empresas podem ser punidos caso não implementem uma política de cybersec e a empresa venha a perder dinheiro ou ter sua reputação prejudicada, em caso de ataque. É um nível maior de maturidade que se admite no continente europeu.

Tratamento regulatório na Europa x Brasil – A regulação existe, mas não tem como a utilityrecuperar o investimento. Mesmo assim, toda essa digitalização traz mais eficiência, reduz a manutenção, existe um ganho desse lado. Em contrapartida, você precisa garantir que todo o sistema esteja seguro usando essas técnicas de cybersecurity. Então você ganha pela eficiência, mas é preciso um investimento. Eu não sei exatamente como anda a situação do Brasil. Não sei em que ponto as utilities estão em termos de cybersecurity nem se as leis brasileiras se responsabilizam por isso.

Seria recomendável que essas utilities fizessem uma espécie de avaliação para ver como está a situação delas. Com base no conhecimento que a ABB tem mundialmente, nós fazemos para os nossos clientes o chamado assessment de segurança. Observamos, fazemos perguntas, realizamos testes. As utilities no Brasil estão partindo para [o modelo de] cada uma criar a sua própria política. Como a

Aneel ainda não tem nada por escrito e não existe o procedimento de rede também do ONS, o que estamos observando é que algumas utilities estão ficando muito preocupadas e começaram a pensar uma política por conta própria.

Importância dos departamentos de TI e Telecom nas empresas de energia – O que nós vemos é que as utilities são muito diferentes entre si. Em algumas, o departamento de TI tem mais poder, já em outras o departamento operacional é muito forte, pode dizer exatamente que precisa de tal desempenho e infraestrutura para, por exemplo, a proteção de uma linha de transmissão de 400.000 volts. Muitas vezes o departamento de TI não entende e não liga para isso, mas se houver um problema em uma linha dessas por causa de um cyberataque, regiões inteiras podem ficar sem energia. Frequentemente existe uma disputa entre o departamento de operações e o de TI, já que, normalmente, os conceitos e as finalidades dos dois grupos são diferentes.

A ideia não é deixar a TI dominar as operações, mas os gestores dessas áreas terem um tipo de trabalho para esses grupos interagirem, para entender lá na frente uma questão que vai envolver virtualização de sistemas com o IoT. Para pavimentar o cenário até lá é preciso ter construído algo antes, inclusive a política combinada com as duas equipes. Uma não vai ganhar domínio sobre o outro, e esse é o grande desafio. A ABB usa uma política para estabelecer o critério de cybersec chamada “protection dev”, ela parte da filosofia da cebola, de existirem várias camadas para fazer a proteção do seu ativo, que é o mais precioso.

Vai desde garantir o acesso ou não ao perímetro da subestação da utility - caso haja um ataque hacker, ele vai encontrar uma rede que está protegida por firewall, por política de segurança e de autenticação, com níveis de usuário e com o papel que cada um pode fazer – a ideia é justamente dificultar esse caminho, porque sabemos que não existe sistema 100% seguro. Só que a partir do momento que se faz essa proteção em camadas diferentes, você dificulta a invasão. É uma dificuldade a cada passo para melhorar a proteção.

Procura de empresas do Brasil por soluções – Na Europa, estamos com uma gama muito grande de clientes pedindo principalmente avaliações. Cada vez mais clientes têm vindo a ABB perguntar sobre as soluções, e a parte da ABB é fazer o assessment, como eu tinha dito antes, fazer perguntas básicas até ir aos níveis mais profundos para verificar as vulnerabilidades e depois ofertar a solução.

Há cinco anos não tinha praticamente nenhum requisito e especificação técnica perguntando sobre o cybersec e agora isso está acontecendo com bastante freqüência lá. No Brasil, para ser preciso, logo após o Carnaval, uma importante utility no mercado brasileiro nos procurou para perguntar exatamente qual a posição da ABB para fazer o hardening, a proteção dos ativos. A gente deve começar no modelo que a Europa está fazendo com o assessment, o nosso grupo junto a uma pessoa de fora para fazer esse assessment com o cliente.