lfe
GESEL UFRJ
http://gesel.ie.ufrj.br/ gesel@gesel.ie.ufrj.br

Uma regulamentação para a segurança cibernética do sistema elétrico brasileiro

SCHUH, Marta. "Uma regulamentação para a segurança cibernética do sistema elétrico brasileiro". O Estado de São Paulo. São Paulo, 18 de junho de 2020.

O setor de energia está passando por uma transformação com a digitalização da indústria e adoção de tecnologias sofisticadas, incluindo inteligência artificial (IA), sistemas de controle e monitoramento. Inovações que permitem o gerenciamento de ativos de maneira mais eficiente.

O desenvolvimento e a transformação de cadeias de suprimento de energia estão no centro de prioridades do governo e das empresas, contudo o risco de incidentes cibernéticos é uma das incertezas mais altas em termos de impacto para empresários do setor. A interconectividade e a complexidade criam vulnerabilidades que podem causar impactos que vão além do setor de energia e impactar a economia do país. Com o aumento da frequência e gravidade de incidentes cibernéticos no setor de energia, o World Energy Council estima que há 155 grupos de hackers que tem como foco empresas do segmento.

Empresas em diversos países já foram vítimas. Na Europa, hackers já acessaram sistemas críticos de controle de companhias, o que poderia desligar a operação de geração e distribuição de energia. Em Israel, outra empresa de energia impactada por incidente de phishing que resultou na entrada de um malware e deixou parte da operação inativa por 2 dias. Nos EUA, a pequena barragem de Bowman hackers tiveram acesso não autorizado ao sistema SCADA, e conseguiram abrir a comporta. Segundo a agência de inteligência americana, se tratava de um teste de hackers iranianos em retaliação pela suposta atuação americana no ataque Stuxnet ao programa nuclear iraniano.

No Brasil não tem sido diferente. No último 29 de abril, a empresa Energisa, que controla distribuidoras de eletricidade em 11 estados do país, foi impactada por um ramsonware, o que deixou parte de seus sistemas inoperantes por 120 horas, segundo informações divulgadas.

Diante do aumento dos incidentes e severidades a Aneel lançou no dia 18 de maio a abertura de Tomada de Subsídios para coletar contribuições para avaliar a necessidade de intervenção regulatória para a segurança cibernética do Sistema Elétrico Brasileiro. De acordo com a Nota Técnica (nº 50/2020-SRT-SGI-SRD-SRG/Aneel), sobre a abordagem e abrangência da regulamentação, a segurança cibernética é uma prática mais madura em jurisdições como Estados Unidos, Austrália e Europa, enquanto é incipiente em outras, como na América Latina. No Brasil, existe um arcabouço legal para a segurança cibernética, porém apenas expresso em leis e decretos, como os já mencionados. Nos Estados Unidos, para o setor elétrico, existem os padrões CIP/Nerc, que têm caráter bem prescritivo e que são seguidos por diversos outros países.

Nos EUA, o Departamento de Energia e a Comissão Federal de Regulamentação de Energia já possuem regras e inclui a necessidade de que sejam reportados ataques

cibernéticos aos reguladores, na EU o parlamento europeu implementou diretrizes similares.

Com uma dependência digital cada vez maior, empresas de energia precisam garantir que suas práticas de gerenciamento de riscos e resposta evoluam para serem adequadas para um ambiente controlado digitalmente, oposto ao ambiente controlado fisicamente. Atualmente, em diversas empresas os processos e mecanismos de resposta e recuperação da infraestrutura de energia digital são menos estruturados e testado do que respostas a eventos de origem física.

A adoção de um planejamento estratégico que inclui práticas de avaliação da resiliência cibernética, além de processos de frameworks de cibersegurança, sistemas e condução de testes de simulação de incidentes são essenciais para traçar caminhos de recuperação de sistemas e desafios impostos por incidentes.

Adicionalmente, é importante considerar neste arcabouço de proteção contratos de seguros muito bem estruturados para minimizar os custos de recuperação de um incidente. Seja uma apólice de lucros cessantes por interrupção sistêmica; custos de resposta a incidentes; investigação Forense de TI; substituição de hardware danificado; custos de restauração de ativos; custos de resgate cibernético e extorsão assim como custos com ações regulatórias e penalizações. O seguro deve ser visto como um componente importante no fortalecimento de uma resiliência dinâmica e estruturada do risco cibernético.

Marta Schuh é especialista em riscos cibernéticos da corretora e consultoria de risco Marsh Brasil