Na Mídia

19/04/2022 | Valor Econômico

Elétricas reforçam medidas de segurança cibernética

Resolução 964 da Aneel, que prevê novas normas de prevenção, entra em vigor em julho

Robson Rodrigues

Faltando menos de três meses para entrar em vigor a resolução 964 da Agência Nacional de Energia Elétrica (Aneel), que prevê que o setor de energia se adapte às novas normas de segurança cibernética, as empresas correm para atender as exigências e implantar sistemas cada vez mais robustos de proteção dos ativos.

Isso porque os ataques virtuais ao setor elétrico cresceram muito após o período da pandemia. As ofensivas dos hackers já fizeram vítimas como a EDP, Energisa, Light, Eletronuclear, entre outras.

Geralmente esses crimes causam a indisponibilidade do Sistema de Supervisão e Aquisição de Dados (Scada) e Dispositivos Eletrônicos Inteligentes (IEDs), podendo causar apagões e blecautes. No caso da Eletronuclear, o assunto gerou mais apreensão por estar relacionado a usinas nucleares.

Na época, a subsidiária da Eletrobras disse que nenhum problema operacional ou de segurança foi detectado. O superintendente de Tecnologia de Informação e Comunicação (TIC) da Eletronuclear, Rodrigo Costa dos Santos, ressalta os trabalhos da empresa, como a participação no Exercício Guardião Cibernético (EGC), considerado o maior treinamento de proteção cibernética do hemisfério sul.

“As redes operativas das usinas [de Angra 1 e 2] e a rede corporativa não possuem ligação. Somente a rede corporativa tem acesso à internet. Nos últimos anos fizemos diversos investimentos, destacam-se o reforço do nosso plano de continuidade de TIC, maior rigidez nas rotinas de atualização dos softwares e contratação de um Centro de Operações de Segurança para monitoramento dos ativos”.

A EDP é também já foi atacada e agora se mobiliza. O gerente de Gestão de Risco da Segurança da Informação da EDP no Brasil, Milton de Jesus Almeida, conta que desde então fortaleceu os trabalhos de gestão de riscos e fechou parceria com universidades e com as forças armadas. A empresa atua em geração, transmissão e distribuição de energia e tem ciência de que deixar o sistema vulnerável poderia ser catastrófico.

“Em função das necessidades regulatórias, começamos um programa interno (...). A gente se sente preparado para responder aos incidentes, mas passamos por uma fase de grandes transformações e a pandemia trouxe o risco cibernético para uma arena muito atípica.”

Almeida afirma que está cotidianamente “em guerra” e o atual contexto geopolítico trouxe uma série de ferramentas de ataques em massa, táticas e manuais de extração de informação.

“O eixo composto por Belarus, Rússia, China e outros países do leste europeu estão tentando criar uma desestabilização e eles vão tentar isso em infraestrutura crítica. E isso é mais crítico ainda no setor elétrico”, conta.

De acordo com relatório do Centro de Estudos Estratégicos e Internacionais (CSIS) e Trellix (encomendado pela Tenable), 9% dos operadores de infraestrutura crítica não têm uma estratégia de segurança cibernética e 85% acreditam que foram alvo de uma ameaça cibernética de um estado-nação.

Entre as grandes geradoras, a AES Brasil está investindo para proteger seus ativos. O custo anual para suportar todos os serviços de cibersegurança no Brasil é de R$ 1,7 milhão. No último ano, a companhia aportou US$ 4 milhões nos EUA e Europa. O gerente de cyber na América do Sul, Carlos Sussmann, conta que os cuidados com infraestruturas críticas nascem desde o início dos projetos. E com o aumento da digitalização, a maioria das unidades de geração e transmissão de energia no Brasil operam remotamente.

“Nenhum controle de segurança é 100% seguro, por isso usamos uma série de controles de segurança, que funcionam como barreiras para filtrar as possíveis ameaças, além do programa de capacitação de pessoas”.

No segmento de distribuição de energia, a Light investiu, em 2021, 170% a mais do que a média dos últimos quatro anos e está mantendo esse ritmo de investimento para 2022.

“A empresa está concluindo o Plano Estratégico de Segurança da Informação (PESI), que inclui as ações para atender as normas de segurança cibernética previstas na resolução 964, editada pela Aneel em 2021. Em 1º de julho, a Light estará adaptada às exigências normativas com, por exemplo, ações de Operation Technology (OT) ou Cyber Operation Technology - Cyber OT - relacionadas à segurança operacional dos recursos de engenharia da companhia”, diz o superintendente de Tecnologia da empresa, Alexandre Santos.

A empresa que não adequar os critérios de segurança digital pode ser punida. Rosi Costa Barros, sócia da área de Energia, e Tatiana Campello, sócia da área de Privacidade de Dados e Cibersegurança, ambas do escritório Demarest, chamam atenção para o fato de que todos os agentes do setor elétrico que terão de cumprir as novas regras da Aneel ainda não deram a devida atenção ao tema, nem aos seus impactos, como penalidades e custos.

As executivas alertam que quem não se adequar aos procedimentos exigidos pode ser autuado e receber as penalidades como preveem não só a legislação do setor elétrico, mas toda a legislação que envolve o assunto segurança cibernética - desde as normas de Lei Geral de Proteção de Dados (LGPD), Marco Civil da Internet e também do Código de Defesa do Consumidor.

“Quando se tem uma determinação do órgão e não se cumpre, os agentes estão sujeitos às penalidades”, diz Costa.

Campelo acrescenta que o movimento regulatório vem avançando no combate aos ataques, mas é preciso ter ainda mais atenção ao tema justamente pelos potenciais impactos em toda a cadeia de abastecimento do país.

“Esta é uma tendência dos setores regulados para criarem boas práticas e normas específicas de segurança cibernética”, finaliza Campelo, do Demarest.