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

O cerco dos hacker às companhias de energia(1)

Irany Tereza

Esta semana, no espaço de apenas dois dias, duas empresas do setor elétrico comunicaram ao mercado terem sofrido ataques cibernéticos. Na segunda, a Copel, distribuidora do Paraná, fez o alerta. Na quarta, enquanto a empresa ainda lutava para restabelecer plenamente a segurança de seus sistemas de tecnologia da informação e de telefonia, foi a vez de a Eletrobras informar ao mercado que sua subsidiária Eletronuclear estava sob "um ataque por software nocivo *(ransomware)* que alcançou parte dos servidores da rede administrativa".

Não se trata de uma simples coincidência de datas. Os dois episódios vêm se juntar a outros quatro também reportados à Agência Nacional de Energia Elétrica (Aneel) há pouco mais de oito meses: Energisa e Enel, em abril do ano passado; EDP e Light, em junho. Juntas, as empresas hackeadas atendem a uma base em torno de 37,4 milhões de usuários e seus serviços são oferecidos em 14 Estados do País.

"Esses ataques já são uma realidade e têm um potencial danoso muito grande", disse à Coluna o presidente da Aneel, André Pepitone. O tema está na agenda prioritária da agência para este ano e ainda neste semestre será efetivada consulta pública para formular medidas capazes de inibir a ação de hackers.

O ataque à Copel está sendo investigado pela Polícia Civil do Paraná e corre sob sigilo de Justiça. Há rumores, não confirmados, sobre um pedido de resgate. Casos de sequestro de dados por ataques cibernéticos com pedido de resgate não são incomuns no mundo. Na época da invasão ao sistema do grupo Energisa, circularam notícias sobre pedido de resgate equivalente a R$ 5 milhões em bitcoins, que o grupo não confirmou.

Um artigo do Grupo de Estudos do Setor Elétrico (Gesel), da UFRJ, de janeiro, menciona o caso, sem citar o nome da empresa, mas com um valor diferente. "No Brasil, em abril de 2020, um grande grupo de distribuição de eletricidade foi atingido por um ciberataque, que deixou diversos serviços indisponíveis por vários dias. No mesmo mês, outro grupo do SEB *(sistema elétrico brasileiro)* foi alvo de *ransomware* por hackers, que exigiram um resgate de € 14 milhões", diz o artigo.

A Lei Geral de Proteção de Dados (LGPD), entrou em vigor em setembro do ano passado, mas a data prevista para as sanções que a Autoridade Nacional de Proteção de Dados poderá aplicar a empresas e pessoas, foi adiada de 1° de janeiro, para agosto deste ano. À Coluna, a Enel do Brasil informou que reforçou medidas de segurança de sistemas e treinamento de funcionários, seguindo o que determina a lei. A concessionária lembrou outro caso, ocorrido em novembro do ano passado. "Ao tomar

conhecimento do incidente pontual envolvendo dados de clientes da distribuidora Enel São Paulo, a empresa cumpriu todos os procedimentos previstos na LGPD e prestou os esclarecimentos necessários às autoridades competentes. O incidente envolveu dados de consumidores da região de Osasco, representando cerca de 4% da base de clientes da companhia. Os clientes foram contatados direta e individualmente por e-mail ou carta, seguindo o compromisso de transparência da empresa."

Não houve, no País, nenhum caso registrado de interrupção no sistema de fornecimento de energia. Até agora o que se tem conhecimento é de invasão de sistemas com captura de dados administrativos. Mauricio Moszkowicz, pesquisador do Gesel, explica que, para reduzir riscos, as companhias têm atuado na segregação dos segmentos, mantendo a parte de informática e internet separada da operação para preservar ao máximo a parte relativa aos sistemas técnicos.

"Não temos evidências de que algo aconteceu na rede operativa, o que é muito mais complexo. É muito mais fácil capturar um banco de dados de uma empresa do que capturar um equipamento que está numa subestação, numa usina ou num centro de operações", diz Moszkowicz. Mas ele alerta que a questão é urgente, principalmente por afetar uma rede de infraestrutura crítica. A geração, transmissão e distribuição de energia elétrica, que no Brasil é feita por meio de um sistema integrado, tem a capacidade de afetar todos os demais setores.

A Aneel acompanha a questão desde 2015 quando uma missão técnica da agência participou de evento sobre o tema nos Estados Unidos, a convite do governo americano. Em dezembro daquele ano foi registrado, na Ucrânia, o primeiro ataque cibernético bem-sucedido a uma rede elétrica. Hackers invadiram os terminais dos operadores da distribuidora Kyivoblenergo e destruíram a possibilidade de restauração remota do sistema deixando 80 mil consumidores ficaram sem energia por três horas. "No Brasil, o que posso dizer é que os ataques prejudicaram as empresas, cada uma em medida diferente, mas não teve nenhum ataque mais severo que inviabilizasse serviços, prejudicasse sistemas ou atingisse faturamento. Pelo menos, não foi reportado para a agência", diz o presidente da Aneel.

O Gesel vai publicar, a partir do mês que bem, um informativo mensal sobre o tema, diz a também pesquisadora da entidade, Lorrane Câmara. Ela chama a atenção para outro problema crítico, que é a dificuldade de formação de mão de obra qualificada. A especialização é uma ferramenta fundamental para combater um tipo de crime que vem avançando tecnologicamente a grande velocidade. E tudo isso num mercado que também está em franca transformação digital.

A resposta aos ciberataques tende a evoluir para uma forma coordenada entre as empresas e o órgão regulador. Mas, enquanto os criminosos estão cada vez mais sofisticados, medidas regulatórias são normalmente demoradas e têm de seguir todo um caminho burocrático. A consulta que será feita pela Aneel irá apresentar quatro alternativas: 1 - Não regular, não fazer nada; 2 - Orientar e divulgar as melhores práticas de segurança cibernética; 3 - Regulamentar os itens da política de segurança cibernética; 4 - Regulamentar requisitos mais prescritivos de segurança cibernética.

Visto assim, de fora, parece bem clara a alternativa mais adequada. Nem precisava de lista.

"Equilibrar este jogo é algo que depende muito de vontade política, de regulamentaão, de redes de cooperação, normas, entidades que possam certificar, auditar, Enfim, ter planos para que a resposta aos incidentes não seja improvisada", diz Maurício Moszkowicz.

(1) Artigo publicado no Broadcast Energia. Disponível em: https://energia.aebroadcast.com.br/tabs/news/747/36632833. Acesso em 05 de fevereiro de 2021.