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

# A segurança cibernética e o setor elétrico (1)

Nivalde de Castro
Lorrane Câmara
Maurício Moszkowicz

A segurança cibernética ganha cada vez mais importância estratégica em função de estar diretamente associada ao rápido e irreversível processo de digitalização, um dos três vetores da transição energética mundial. A digitalização avança à medida que a prioridade na descarbonização aumenta com a difusão de sistemas descentralizados de geração de energia elétrica renovável, de redes inteligentes, da mobilidade elétrica, do armazenamento distribuído e da tecnologia 5G, entre outros tantos exemplos.

A contrapartida da massiva introdução de processos automatizados e digitalizados em todos os segmentos do setor elétrico é o aumento potencial e real de ataques cibernéticos cada vez mais recorrentes e sofisticados a agentes privados e públicos do setor. Esta tendência de maior risco de ataques está associada à crescente interdependência e interação entre o ciberespaço e a infraestrutura física, cada vez mais dinâmica e intrínseca ao setor elétrico, em decorrência da capilaridade das unidades produtivas de geração, transmissão, distribuição e comercialização.

A intensificação e difusão da digitalização mundial determina um aumento muito expressivo do número de dispositivos conectados. Estima-se que, em 2019, havia cerca de 21 bilhões de dispositivos de IoT (Internet of Things), como medidores inteligentes, geração distribuída, redes inteligentes, etc., conectados em todo o mundo, número que deverá mais do que dobrar até 2025. Assim, hackers profissionais estão se aproveitando desta crescente superfície digital para realizar ataques, que podem comprometer todo o ambiente da rede digital de uma organização, o que aumenta a vulnerabilidade e o risco do setor elétrico.

Observa-se que sistemas digitais desatualizados ou atualizados de modo irregular são um ponto de entrada comum para ataques cibernéticos sofisticados. Ameaças cibernéticas também podem ser introduzidas por unidades USB, conexões remotas não seguras, redes wireless e HMIs (Human-machine Interfaces) não supervisionados. A pandemia, ao impor o home office, que tende a se perpetuar como um novo paradigma das relações de trabalho, ampliou, ainda mais, a superfície de ataque.

Como resultante deste processo de digitalização, a incidência de ataques cibernéticos vem crescendo de forma exponencial. Segundo o relatório "Cybersecurity - Fighting Invisible Threats", publicado pelo banco suíço Julius Baer, em 2021, os crimes cibernéticos devem custar US$ 6 trilhões à economia global, estimando-se que, diariamente, são registrados 8 trilhões de ataques, das mais diversas ordens e formas, ao redor do mundo. Mesmo sendo números estimados, a sua magnitude indica a gravidade do problema.

Dentre os ataques cibernéticos mais recorrentes figuram os ransomware, que restringem o acesso ao sistema infectado, criptografando dados e mantendo o sistema refém. O acesso ao sistema só é restabelecido mediante o pagamento de resgate em

criptomoedas. Este tipo de ataque é considerado dos mais graves, devido à rapidez com que fragiliza a infraestrutura digital e física de empresas, as quais, muitas vezes, têm as operações interrompidas durante dias.

O relatório do Julius Baer indica que, cada vez mais, os ataques cibernéticos estão sendo direcionados para infraestruturas críticas, como o setor elétrico, consideradas cruciais para o suprimento de serviços essenciais, com elevados riscos à segurança da sociedade. Em 2020, ataques cibernéticos a infraestruturas críticas foram classificados pelo Fórum Econômico Mundial (WEF) como o quinto maior risco de colapsos globais. Ademais, uma pesquisa realizada pela Accenture, baseada em entrevistas com 100 executivos de empresas de concessão de diferentes setores de mais de 20 países, indicou que interrupções no fornecimento de energia elétrica decorrentes de ataques cibernéticos foram indicadas como a principal preocupação de 57% dos entrevistados.

O primeiro ataque cibernético bem-sucedido a uma rede elétrica foi registrado na Ucrânia, em dezembro de 2015, quando os terminais dos operadores da distribuidora de energia elétrica Kyivoblenergo foram invadidos e a possibilidade de restauração remota do sistema destruída. Na ocasião, 80 mil consumidores ficaram sem eletricidade por três horas. Nos Estados Unidos, em 2017, hackers tentaram invadir geradoras, incluindo uma usina nuclear, e distribuidoras de energia.

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 Setor Elétrico Brasileiro (SEB) foi alvo de ransomware por hackers, que exigiram um resgate de € 14 milhões de euros. Outros Além disso, outros ataques cibernéticos a empresas foram registrados ao longo do ano.

Um estudo desenvolvido pelo Centro de Pesquisa e Desenvolvimento em Telecomunicações CPqD, através de um exercício teórico, estimou que cada minuto de interrupção no fornecimento de energia elétrica no Brasil teria um custo de R$ 5 milhões, de modo que um dia inteiro sem eletricidade implicaria em perdas na ordem de R$ 7,3 bilhões. Às perdas financeiras diretas somam-se outros efeitos indiretos de difícil quantificação, como relacionados à saúde, o que reforça e reafirma a segurança cibernética como uma área crítica.

De modo geral, os objetivos fundamentais da segurança cibernética são garantir a confidencialidade, a integridade e a disponibilidade de acesso e funcionamento dos ativos cibernéticos.

Neste contexto complexo de risco, é imperativo que as empresas criem protocolos de proteção cibernética contra este tipo de ameaça. Mas, por outro lado, é imprescindível que seja firmado um enquadramento regulatório direcionado ao tratamento da segurança cibernética no SEB, podendo-se tomar como referência o observado na União Europeia.

Em 2016, o Parlamento Europeu publicou a Diretiva (UE) nº 1.148/2016, que tem como prerrogativa garantir a segurança cibernética e a proteção de dados nos setores de serviços essenciais, estabelecendo regras transversais e o modelo de funcionamento do sistema de segurança cibernética europeu. A Diretiva foi complementada, em 2019, pela Clean Energy for all Europeans, que trata, de modo geral, da cibersegurança no setor energético e inclui quatro atos legislativos centrados especificamente no setor elétrico.

Neste sentido e direção, foi aprovada, em fevereiro de 2020, a Estratégia Nacional de Segurança Cibernética do Brasil, estabelecendo a necessidade de elevar o nível de proteção e resiliência dos setores de infraestruturas críticas. A partir desta importante iniciativa, é fundamental estabelecer um marco regulatório específico, em função da importância que este bem - energia elétrica - detém na sociedade, como exemplificado

pelos problemas econômicos, sociais e políticos vinculados ao apagão do estado do Amapá.

Em relação ao enquadramento regulatório, a Agência Nacional de Energia Elétrica (Aneel) identificou a segurança cibernética como um tema prioritário na atual agenda regulatória, estando prevista a abertura de uma consulta pública no primeiro semestre de 2021. O objetivo central será o estabelecimento de requisitos mínimos de segurança cibernética nos procedimentos de rede, ou seja, na interação digital das infraestruturas físicas. Em virtude desta pertinente iniciativa da Aneel, será possível definir e firmar elementos de transversalidade para ajudar na consolidação de uma política de segurança cibernética envolvendo outras áreas do governo.

Em suma, o problema é crítico e sensível. As empresas e instituições do SEB, especialmente o Operador Nacional do Sistema Elétrico (ONS), responsável direto por garantir o suprimento de energia elétrica em tempo real, não podem ficar sob o risco de ataques cibernéticos, um perigo real e concreto.

**Nivalde de Castro é professor do Instituto de Economia da UFRJ e coordenador do Grupo de Estudos do Setor Elétrico (Gesel).**
**Lorrane Câmara e Mauricio Moszkowicz são pesquisadores plenos do GESEL-UFRJ.**

(1) Artigo publicado no Broadcast Energia. Disponível em: https://energia.aebroadcast.com.br/tabs/news/746/36467198. Acessado em 22 de janeiro de 2021.