IFE Informativos Eletrônicos do Setor Elétrico
ISSN 1678-6130
GESEL Grupo de Estudos do Setor Elétrico UFRJ

Fortalecendo a rede: a importância da cibersegurança no Setor Energético[1]

Leonardo Dib [2]
Luiz Carlos Gomes [3]

A crescente digitalização do setor de energia está transformando a forma como as empresas operam, trazendo benefícios significativos e garantindo sua relevância no mercado. No entanto, essa evolução também expõe as organizações a riscos até então pouco conhecidos. A implementação de soluções mais inteligentes e interconectadas, sem uma devida atenção à segurança cibernética, pode criar vulnerabilidades que comprometem não apenas a operação, mas também a infraestrutura essencial do setor.

Segundo o relatório 2024 X-Force Threat – IBM Security, o setor de energia ocupa a segunda posição entre os mais visados, concentrando 19% de todos os ataques virtuais monitorados no Brasil. Neste contexto, contar com uma governança digital robusta é um passo estratégico para evitar ataques e garantir a continuidade das operações.

Um dos principais riscos cibernéticos enfrentados no cenário corporativo é o ataque de ransomware (sequestro de dados). Esse tipo de ataque bloqueia o acesso da empresa ao seu próprio banco de dados, tornando-o inacessível até que um resgate seja pago. De acordo com relatório anual de ameaças publicado pela Kaspersky, entre jun/23 e jul/24, as tentativas de ataque de ransomware na América Latina a sistemas monitorados pela empresa alcançaram mais de 1.1 milhão (3.247 tentativas por dia). O Brasil segue como principal alvo, com quase 50% do número total de ataques e uma média de 1.334 tentativas diárias.

Além disso, o caráter estratégico do setor de energia expõe o mercado a ataques de negação de serviço (DDoS), que geralmente exploram dispositivos da rede com menor grau de sofisticação ou proteção, como equipamentos IoT. Este tipo de ataque tem por objetivo sobrecarregar sistemas e redes, e poderia causar, por exemplo, interrupções no fornecimento de energia e afetar a confiabilidade do sistema. Com raros casos de cobrança de resgate, os ataques são geralmente atribuídos a grupos ativistas ou a nações adversárias, podendo até ser atos de concorrência desleal.

---

[1] Artigo publicado no CanalEnergia. Disponível em: https://www.canalenergia.com.br/artigos/53295554/fortalecendo-a-rede-a-importancia-da-ciberseguranca-no-setor-energetico Acessado em 19.11.2024

[2] Leonardo Dib Freire, sócio do RMMG Advogados e especialista no setor de Energia;

[3] Luiz Carlos Gomes Filho, sócio do RMMG Advogados e head de Direito Digital.

Por isso, um importante ponto de atenção é a governança de supply-chain. Ataques cibernéticos miram no elo mais fraco da corrente e, não raro, este elo está ligado a fornecedores ou prestadores de serviços que podem não contar com a mesma sofisticação em sistemas de segurança, levando a brechas que podem afetar toda a rede de operação. Isso deve ser levado em conta durante a seleção e renovação de contratos com parceiros, sempre que possível, recorrendo a diretrizes claras e reconhecidas para acordar sobre os requisitos mínimos de segurança, como Normas ISO, por exemplo. Esta medida facilita um alinhamento entre as partes na busca por práticas robustas de segurança.

Internamente, uma boa estratégia de cibersegurança deve estar pautada pela continuidade operacional. A conscientização de colaboradores é fundamental, tendo em vista que muitos ataques exploram a vulnerabilidade humana, e o usuário final continua sendo um elo crucial na cadeia de ataques. Sob esse aspecto, treinamentos que enfatizem a identificação de phishing e incentivem a proteção de informações sensíveis podem reduzir significativamente a probabilidade de incidentes cibernéticos.

Para posições com acesso a informações críticas da organização, a proteção de identidade e o uso de mecanismos de segurança como autenticação multifatorial (MFA) confere ainda mais robustez e rastreabilidade aos acessos. Mas a verdade é que não há uma fórmula infalível, e, sim, a necessidade de combinar ferramentas de tecnologia, controles de governança e cultura de cibersegurança para uma estratégia que mantenha a defesa sólida.