Na Mídia

14/07/2023 | Canal Energia

Segurança cibernética: como o setor elétrico está se posicionando

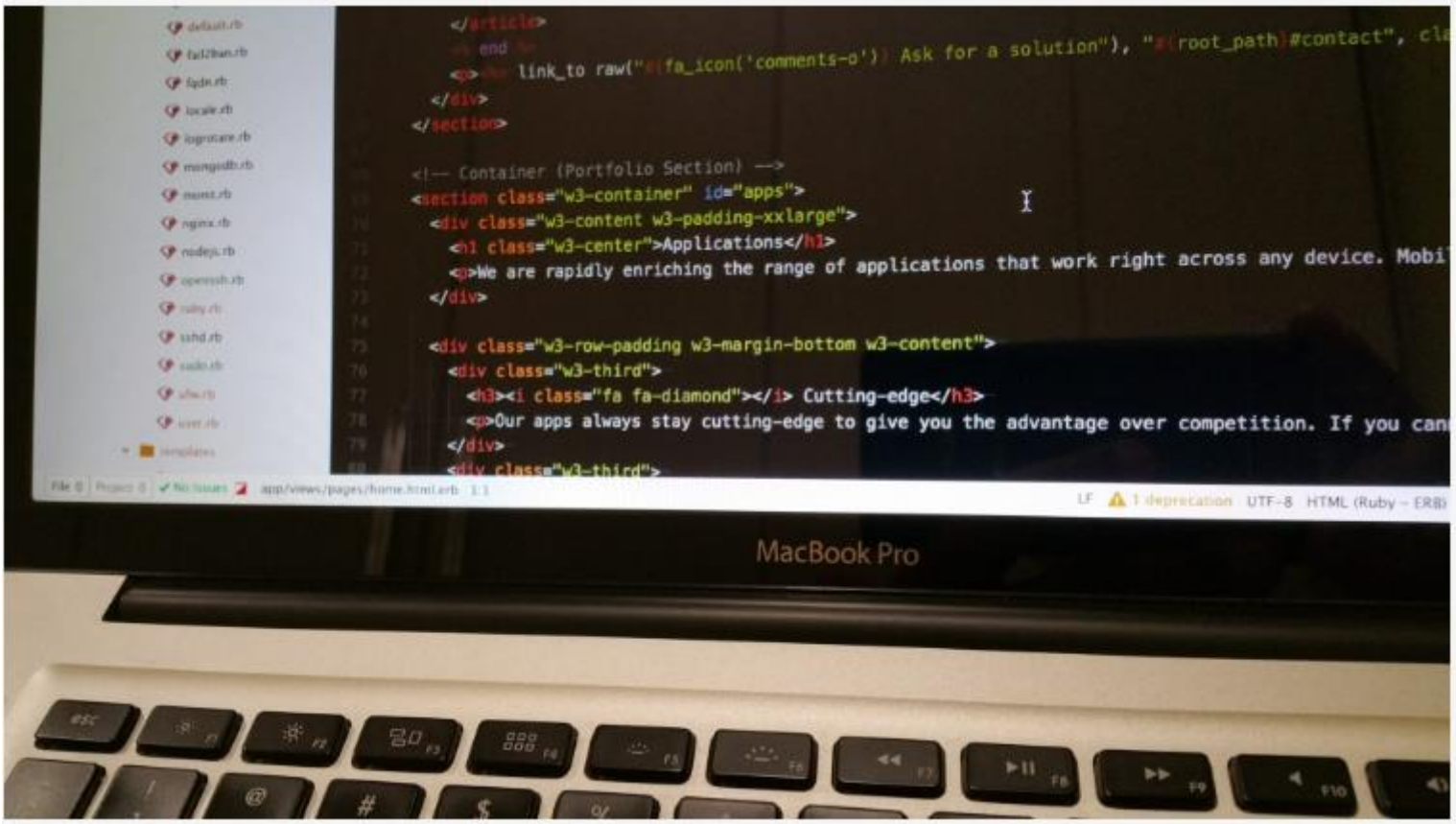
Ataques cibernéticos, principalmente na modalidade de ransoware (que visa roubar dados ou bloquear máquinas em troca de resgate geralmente em bitcoin) já atingiram ao menos cinco empresas do setor

Michele Rios

Nos últimos anos houve um crescimento de ciberataques no mundo e esse fato tem causado uma grande preocupação para as empresas de todos os setores da economia brasileira. Contudo, esse é um cenário bastante desafiador e que exigirá cada vez mais tempo, disciplina e recursos das organizações para ações de prevenção e resiliência.

Os ataques cibernéticos, principalmente na modalidade de ransomware (que visa roubar dados ou bloquear máquinas em troca de resgate geralmente em bitcoin) já atingiram ao menos cinco empresas do setor. As ações criminosas não chegaram a afetar a distribuição ou fornecimento de energia, mas vazaram dados e afetaram os sistemas administrativos das empresas, segundo dados da Aneel.

De acordo com a União Internacional de Telecomunicações (ITU, na sigla em inglês), órgão da Organização das Nações Unidas (ONU) e que coordena esforços na área de segurança cibernética, o Brasil ocupava a 71ª colocação no índice de segurança cibernética em 2018, divulgado em 2019. O país foi o 2° no mundo que mais sofreu perdas econômicas de ataques cibernéticos. Segundo os dados da ITU, os prejuízos com ataques cibernéticos no Brasil ultrapassaram US$ 20 bilhões, atingido ao menos 70 milhões de brasileiros. Contudo, com a melhora do ambiente legal e a entrada em vigor no país da LGPD, o Brasil passou para o 18° lugar no índice global de segurança cibernética em 2020, quando 193 países foram pesquisados. O que mostra como a criação de normas e regras contribui para aumentar a segurança.



Para o conselheiro da Câmara de Comercialização de Energia Elétrica (CCEE), Marco Delgado, o setor elétrico tem riscos de exposição assim como qualquer outro segmento da economia. Esse é um cenário que afeta desde o mercado financeiro até a gestão de equipamentos públicos e nenhuma organização está totalmente blindada contra tentativas de ataques. “É muito importante a prevenção, com infraestruturas modernas e robustas de proteção e o incentivo às boas práticas por parte dos colaboradores”, disse. Ele ainda destacou que é crucial ter um plano de recuperação de ambiente bem estruturado, efetivado com tecnologia de vanguarda para ágil isolamento de camadas de segurança eventualmente afetadas e, principalmente, para restabelecimento dos sistemas com celeridade.

"O tema é tão relevante para a Câmara que se tornou um dos pilares para o desenvolvimento dos sistemas que usaremos para a coleta de dados financeiros dos agentes para o monitoramento prudencial, previsto pela Consulta Pública ANEEL nº 011/2022", ressaltou. Delgado ainda afirmou à **Agência CanalEnergia**, que nas interações com os agentes para apresentar o modelo e as ferramentas tecnológicas agregadas, a preocupação com a segurança cibernética era sempre destacada. Nesse sentido, já no planejamento para a criação das plataformas, eles já definiram que utilizariam soluções criptografadas assimétricas em nuvem e com requisitos máximos de proteção para os dados.

Na CCEE, eles concentram um volume muito grande de informações sensíveis e, por isso, trabalham com o que há de mais robusto em tecnologias de segurança, além de desenvolvermos técnicas de treinamento e iniciativas de conscientização dos colaboradores. "Esse é um exemplo claro de como prezamos pelo tema e como a prevenção aos ciberataques já faz parte do dia a dia do setor elétrico", explicou.

Delgado afirmou que essa questão em relação a preocupação com ataques cibernéticos é constante. "Estar preparado para responder rapidamente e de modo assertivo aos ataques cibernéticos significa investir em sistemas e controles, ter uma equipe de gestão de riscos e colocar em prática ações de conscientização dos funcionários".

Ele acredita que esse tema é muito importante. "O setor elétrico, na sua essência, tem uma função pública imprescindível para o funcionamento da economia e para o cotidiano da população, além de movimentar bilhões de reais em valores financeiros todos os meses. Ataques que interfiram na operação de uma empresa ou, pior, no mercado como um todo, podem gerar prejuízos em todas as esferas da vida nacional. Vale mencionar também que os consumidores precisam ter a garantia de segurança das suas informações que circulam nos sistemas de empresas e entidades", ressaltou.

Transformação digital no setor

Já para o diretor sênior de serviços e soluções da Siemens Energy no Brasil, Armando Juliani, o setor de energia está passando por uma nova onda de transformação digital, alavancada pelo crescimento do uso de IA (Inteligência Artificial) e aplicações de IoT (Internet das Coisas). "A conectividade inteligente de infraestruturas no setor de energia vem acompanhada de uma legítima preocupação para as empresas de energia, pois uma maior quantidade de ativos conectados significa maior vulnerabilidade a ataques externos, que podem ser caracterizados por roubos e desvios de dados ou até mesmo perigosíssimas paralisações totais de geração e distribuição", disse.

Juliani destacou que progressivamente e em maior número, as empresas de energia reconhecem que a probabilidade de serem atacadas é de quase 100% e que devem fortalecer sua agilidade e resiliência para que possam responder quando – não se – forem atacadas. “Uma evidência desse contínuo e necessário estado de alerta no setor pode ser encontrada em uma pesquisa de 2019 da Siemens Energy com o Ponemon Institute, realizada com mais de 1.700 especialistas em cibersegurança de empresas de energia, e ainda válida para o atual momento. À época, 64% dos entrevistados afirmaram que os ataques cibernéticos são um dos principais desafios para a sua gestão, e 54% destes esperavam um ataque a uma de suas infraestruturas críticas de energia nos próximos 12 meses”, explicou.

Ele acredita que à medida que as tecnologias digitais se espalham e agregam valor à infraestrutura de energia, os ataques continuarão a aumentar em frequência e sofisticação. Segundo o executivo, não há dúvidas de que a digitalização do setor de energia deve considerar em seu escopo a cibersegurança como uma prioridade.

De modo geral, todas as empresas ficam mais expostas conforme se digitalizam, modernizam ou fazem a recapacitação de *assets* infraestrutura e energia, conectando-os a redes virtuais, sejam elas fechadas ou abertas. “Na Siemens Energy, temos observado, ao redor do mundo, que tanto o número de ataques quanto a sofisticação aumentaram exponencialmente nos últimos anos. E esses ataques, em sua maioria, ocorrem a partir da convergência entre os mundos físico e digital”, destacou Juliani.

Ele ainda acrescentou que também houve evolução na maturidade e na capacidade de hackers em explorar as vulnerabilidades e lacunas de segurança dos sistemas de tecnologia operacional. O aumento das ameaças cibernéticas às empresas de toda cadeia de valor da energia avança à medida que esses adversários mal-intencionados se tornam mais familiarizados com a tecnologia utilizada. “Antigamente, apenas os profissionais de cibersegurança que trabalhavam nessas empresas compreendiam os produtos e os protocolos vulneráveis a ataques. Contudo, estamos agora enfrentando um conjunto de ameaças executadas por adversários altamente talentosos, capazes de direcionar especificamente diferentes segmentos, como é o caso da geração e transmissão de energia elétrica”, explicou.

O executivo da Siemens Energy afirmou que outro aspecto importante é que por muito tempo a cibersegurança no setor de energia foi desenvolvida com o objetivo de melhorar a eficiência por meio do aumento da conectividade interna das organizações. Contudo, quanto mais as empresas passaram a adotar tecnologias digitais para aprimorar a eficiência e criar soluções sistêmicas de modo a equilibrar a rede elétrica, por exemplo, também abriram caminhos para novas ameaças cibernéticas, atrativas para a exploração de agentes maliciosos.

“Vivemos em um novo panorama de ameaças. Ele deve ser abordado com urgência por empresas privadas, serviços públicos, operadores e fabricantes originais de software e hardware. Acreditamos que resolver esse problema exigirá fomentos à inovação, regulação robusta e parcerias fortes tanto no desenvolvimento de tecnologia operacional (TO) quanto na segurança de sistemas de tecnologia da informação (TI) essenciais nos ambientes digitais de hoje”, disse. E ele ainda destacou que mais do que isso, a eficiência de qualquer solução passa também por mudanças culturais, incentivadas por meio de investimentos em treinamentos de segurança, promoção de *awareness* sobre riscos e avaliação de ameaças no setor de energia e nos demais atores que administram infraestruturas críticas.

Resolução Normativa da Aneel

A resolução normativa nº 964, de 14 de Dezembro de 2021 da ANEEL, que entrou em vigor em 01 de julho de 2022, prevê a implementação de políticas de segurança compatíveis com o porte da empresa, a obrigatoriedade de as companhias comunicarem situações de crise em segurança cibernética, assim como o compartilhamento entre os agentes e o órgão regulador de ocorrências relevantes.

Também prevê procedimentos relacionados à gestão da segurança, como a segmentação de redes de operação da rede de TI e da Internet, ações de resposta rápida para contenção de incidentes, avaliação e tratamento de riscos.

De acordo com a resolução da Aneel, as empresas são responsáveis pela segurança das instalações, a continuidade da prestação do serviço e pelo ônus da adaptação de seus sistemas. Os gastos necessários para implantação dessas medidas poderão ser avaliados pela agência, para um eventual reconhecimento de custos nas tarifas.

Para o sócio e diretor comercial da Avantia, Bruno Carvalho, a resolução é um marco muito importante para o desenvolvimento da cultura do armazenamento, gestão e proteção de dados. “A resolução da ANEEL deixa muito clara a importância da disseminação interna, entre os colaboradores, de se ter uma cultura de segurança cibernética, sobretudo, no que diz respeito a notificação no caso de um evento, adoção de normas e boas práticas, diagnósticos e recuperação dos incidentes, mitigação de riscos, análise da causa e impacto, tudo isso vem somar com a consolidação e aplicação de uma cultura preventiva no que tange a cibersegurança”, explicou.

Segundo o diretor, algumas empresas já se movimentaram, com soluções que estão em implantação de forma mais maduras e outras estão iniciando essa movimentação, importante nesse contexto é que, as empresas do setor elétrico estão começando a entender que cibersegurança precisa ser uma prioridade, não só pelo atendimento a legislação, pela continuidade dos bons serviços prestados, mas, também, pela continuidade e sustentabilidade do seu negócio, uma pesquisa da Ernest Young de 2023 em conselhos de grandes grupos empresariais, mostrou que segurança cibernética e privacidade de dados estão entre cinco maiores prioridades de investimento pra esse ano. “Isso mostra que, as empresas que ainda não se adequaram, se adequarão por uma exigência do próprio mercado”.

Ele acredita que um dos maiores desafios das empresas do setor elétrico é identificar as melhores soluções para se adequarem as legislações pertinentes ao tema e as resoluções da Aneel. A digitalização do setor, que recebe contribuições de movimentações do tipo indústria 4.0 (IoT, big data, machine learning), vem passando por essa transição, onde, a utilização de dados de forma inteligente é um desafio, mas que traz maior controle, gestão, planejamento e redução de custos operacionais. “Com a maturidade na adoção de medidas preventivas a tríade confidencialidade, integridade e disponibilidade, estará cada vez mais presente na operação das empresas do setor de energia”, explicou.

Para Thaís Araujo Rato Tarelho e Oscar Hatakeyama, ambos advogados da área de energia e recursos naturais do Demarest, a resolução da Aneel dá diretrizes para que as empresas do setor publiquem normas que permitirão a adequação de sua operação a um novo cenário mundial. “Acreditamos que a resolução esteja de acordo com as práticas necessárias para o tema. No entanto, tais normas não superam os desafios que são e serão enfrentados pelas empresas conforme exposto nas abordagens anteriores”, afirmaram.

O conselheiro da CCEE, Marco Delgado, acredita que a REN 964/2021 tem a função importante de padronizar as políticas de segurança cibernética a serem adotadas pelos agentes que participam do mercado brasileiro de energia. “Sua publicação estimula as empresas e organizações setoriais para que organizem esforços em prol da prevenção contra os ataques de hackers e demais incidentes de informação, bem como para que prezem pela transparência e pelo zelo pelos dados que concentram”, ressaltou.

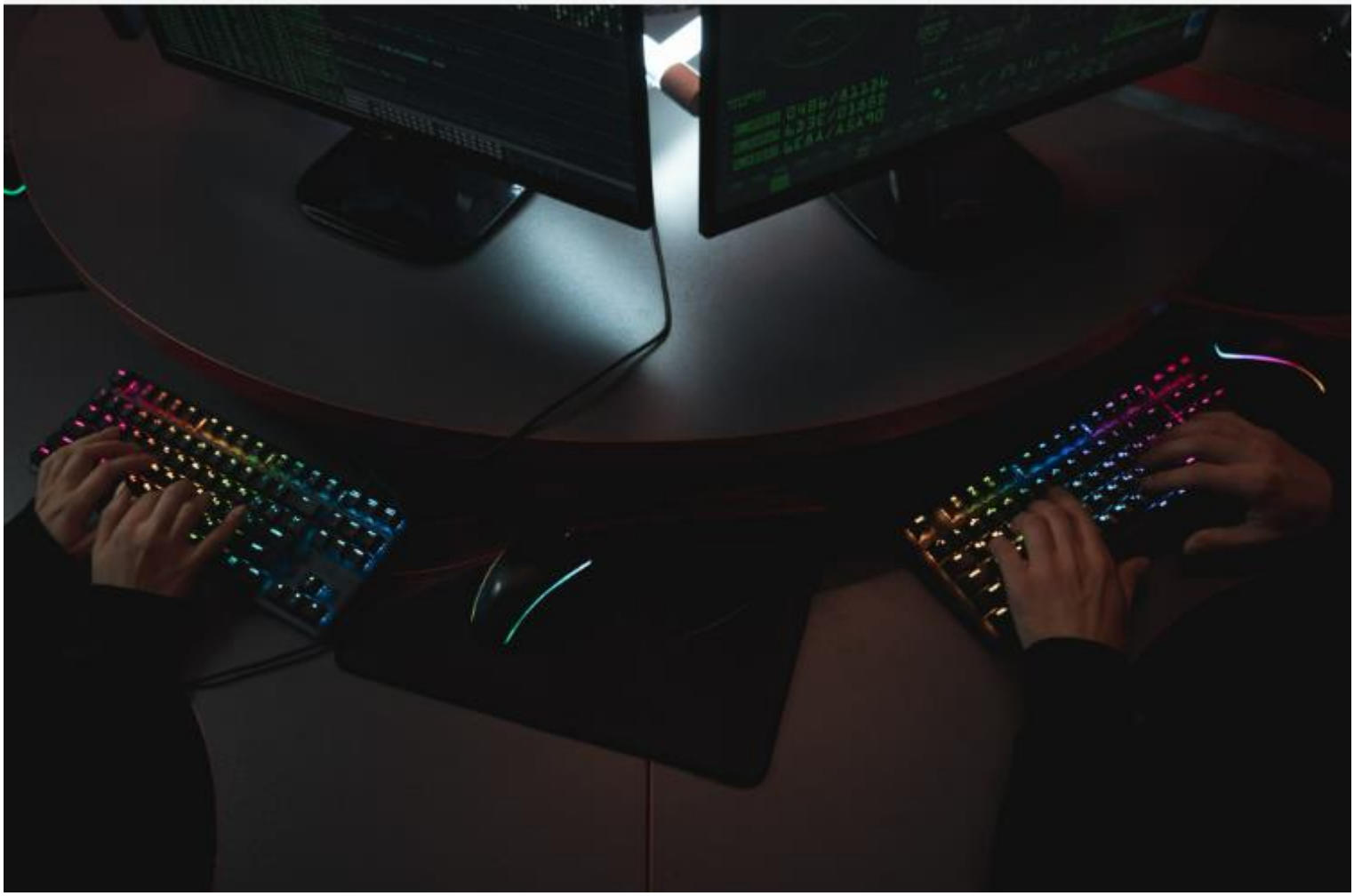
Como evitar ataques

Embora a questão da cibersegurança já venha sendo discutida há tempos no cenário empresarial, ainda pode ser considerada como uma preocupação recente. Nesse contexto, os setores regulados e o poder concedente vêm emitindo normas que regulam e exigem que as empresas adequem suas operações a políticas que previnam esses ataques.

Segundo Cecília Cunha, advogada das áreas de privacidade, tecnologia e cibersegurança e propriedade intelectual e inovação do Demarest Advogados, para as empresas do setor elétrico mitigarem o risco de sofrerem um ataque cibernético, elas deverão rever internamente quais são as medidas técnicas e administrativas de segurança da informação adotadas, como, por exemplo, planos de resposta a incidentes e remediação, para verificar se essas medidas já foram testadas internamente e se estão atualizadas.

"Ainda que não estejamos falando unicamente de dados pessoais, é importante também lembrar que uma obrigação prevista na LGPD aos agentes de tratamento é a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", ressaltou.

De acordo com os advogados Demarest, esse é um tema de importância mundial. O setor elétrico é estratégico para o país e qualquer ameaça que possa colocar em risco sua disponibilidade deve ser tratada com seriedade. Eles ainda destacaram que considerando esse contexto, a atuação da Aneel foi precisa no tema, havia a necessidade de regular a obrigação de manter políticas que previnam ataques nesse sentido. Contudo, mais que isso, é necessário medidas efetivas e concretas para a proteção desses ataques, o que é um desafio para as empresas porque demanda investimentos, muitas vezes, não dimensionados.



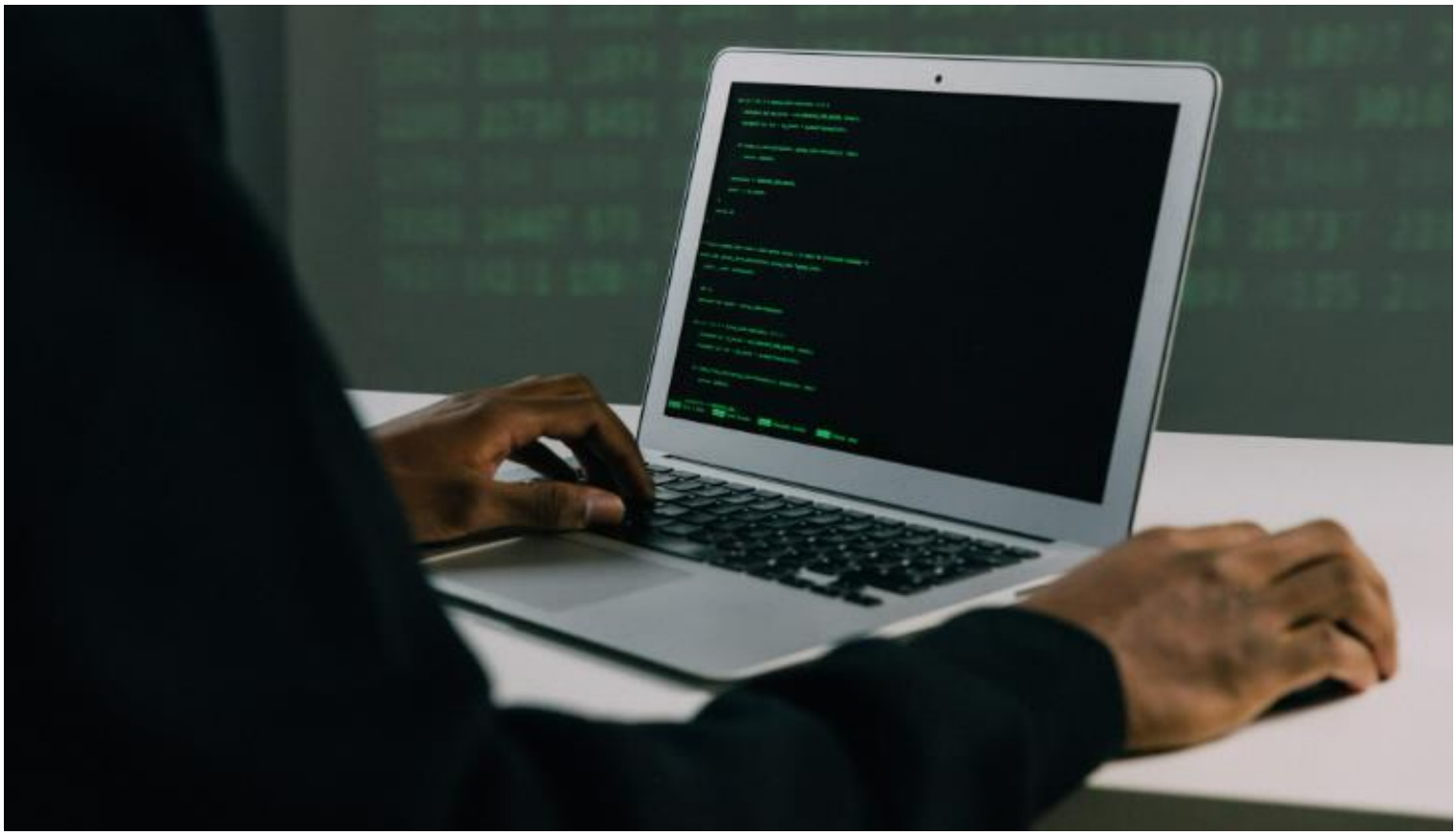
O CTO da TI Safe, Thiago Branquinho, destacou que para evitarem esse tipo de ataque as empresas precisam primeiro mudar a sua mentalidade. “Muitos gestores ainda não entenderam que suas empresas podem ficar fora do mercado e ver suas ações reduzidas a pó por conta de um ataque cibernético”. Ele destacou que a partir desse entendimento, podem ser estabelecidos controles “clássicos” para prevenir os incidentes, como: publicar políticas e procedimentos específicos para os ambientes de tecnologia operacional (TO); conscientizar dos colaboradores e fornecedores; proteger perímetros de rede com firewalls de próxima geração (Next Generation Firewalls – NGFW); detectar anomalias de rede com plataformas conhecidas como IDS industrial; adotar sistemas modernos de prevenção contra malware – incluindo ransomware – como EDR (Endpoint Detection and Response) homologado para as redes de automação; microssegmentar ambientes de rede e reforçar o controle de acesso de usuários (principalmente o remoto).

Ainda ressaltou que a segurança é como um “ser vivo” e requer cuidados permanentes. Para tal, é fundamental ter uma equipe especializada para atuar 24×7 na prevenção e no monitoramento contínuo. Em caso de incidentes, essa equipe atua na contenção e na erradicação do problema, bem como utiliza o evento para reforçar os controles.

Desafios do setor

O executivo da TI Safe acredita que esse tema ainda é um desafio para as empresas do setor. “As empresas vivem escassez de mão de obra especializada, falta de orçamento e até mesmo falta de entendimento sobre a real necessidade da segurança cibernética”, disse. Segundo Branquinho, a mão de obra necessária para realizar as atividades de segurança de forma assertiva é rara e não faz parte dos planos de carreira das empresas do setor. Assim, contratar pessoal ou formar esses profissionais, não pode ser considerada trivial. “Quanto ao orçamento, é raro ver as empresas com planejamento financeiro adequado para as necessidades de segurança. Os dois primeiros pontos são, muitas vezes, fruto da falta de entendimento sobre o que é a segurança. Multo além do compliance, as medidas para a proteção da tecnologia operacional maximizam a resiliência do ambiente, contribuindo diretamente para a continuidade dos negócios”, explicou.

Para Marco Delgado, o desafio para o setor elétrico é igual para os demais segmentos da economia. “O crime virtual se renova constantemente e a preocupação das empresas com o tema deve ser contínua. Algumas práticas, porém, não mudam. A engenharia social é um dos aspectos mais importantes da prevenção contra ciberataques e continuará sendo”, disse.



Delgado afirmou que as dicas importantes que já conhecemos, de não abrir links e mensagens com origem desconhecida, cuidar de senhas e informações de acesso, armazenar corretamente os documentos, tudo isso é essencial para uma boa prática de segurança da informação. “Uma vez que, como sabemos, a maioria dos incidentes é causado por falhas humanas e não de sistemas. Portanto, diria que, sim, é um desafio, mas a CCEE e o setor trabalham continuamente para que os agentes e os consumidores possam ficar despreocupados”, ressaltou.

Para finalizar, Armando Juliani, da Siemens Energy, destacou que devem ser realizados investimentos contínuos de cibersegurança em torno de ativos físicos de energia ao mesmo tempo em que se equilibra melhorias na eficiência operacional. “Inclusive, isso deve ser feito urgentemente, pois ao olharmos para o futuro, em direção a uma rede descentralizada, as medidas de defesa se tornarão mais complexas de serem implementadas conforme o setor de energia adota mais dispositivos e ativos conectados, desenvolve instalações de geração menores e cada vez mais residências passam a fazer parte do ecossistema de energia pela geração distribuída”, finalizou.