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

Ataques cibernéticos impõem nova realidade às empresas e aos profissionais do setor de energia elétrica, alerta Hitachi ABB (1)

Davi de Souza

A questão de cibersegurança está em evidência no país. O recente caso de vazamento de dados de milhões de brasileiros deixa claro que o Brasil deve se voltar ao tema, de forma a garantir a segurança das informações na rede. Essa mesma preocupação se replica em setores cruciais da economia, como o elétrico. Ataques às empresas brasileiras desse segmento no ano passado acenderam o sinal de alerta. A Agência Nacional de Energia Elétrica (Aneel) já elencou como prioritária a discussão sobre o tema em sua agenda regulatória de 2021-2022. Diante desse cenário, vamos abrir o noticiário desta semana conversando com o gerente de tecnologia da Hitachi ABB Power Grids, Júlio Oliveira. A empresa tem fornecido equipamentos cada vez mais digitais e tecnológicos para o setor elétrico e, por isso, a proteção contra ataques cibernéticos é uma das grandes preocupações da companhia.

O executivo alerta que um cracker poderia, entre diversas possibilidades, desligar um disjuntor que alimenta uma linha de transmissão ou um circuito de transformador ou mesmo alterar limites de monitoramento dessas máquinas. "Há riscos tanto de indisponibilidade da instalação, perda de capital e até de danos à imagem da concessionária responsável", lembrou. Oliveira também diz que esse ambiente de ciberataques vai exigir novas realidades aos profissionais que trabalham nesse mercado. "Hoje, o profissional moderno que vai atuar nesse segmento precisa atuar nessas três esferas unidas: eletrônica, elétrica e tecnologia da informação. Estamos falando de um novo profissional, de fato, com conhecimento nessas três áreas", analisou. Falando sobre negócios, a Hitachi ABB já entregou três subestações digitais no Brasil nos últimos anos e vê com otimismo as possibilidades de novos negócios no país daqui em diante: "As perspectivas são muito positivas. Mesmo com tudo isso que estamos vivendo, com a pandemia de Covid-19, existe muita coisa a se fazer no país. Há muitas obras de infraestrutura no setor de energia elétrica", concluiu.

Ao que o senhor atribui o aumento de ataques cibernéticos no setor elétrico nos últimos tempos?

Começamos a observar um comportamento um pouco mais agressivo em relação às infraestruturas de missão crítica desde 2014 até agora. Isso não significa que antes esses ataques já não estavam acontecendo. Mas se observamos os reportes internacionais de 2014 até os dias atuais, existe um aumento exponencial de ciberataques para esse tipo de infraestrutura.

Um dos pontos que observamos é que os crackers, os atacantes mais especializados, começaram a perceber que o nível de segurança dentro de missão crítica é muito menor se comparado com as aplicações do lado de TI, por exemplo. Ao atacar o sistema elétrico, esses crackers conseguem duas coisas que são muito importantes para este

perfil de atacante: dinheiro e fama. Há uma percepção de falhas básicas de segurança em aplicações desse segmento.

Quais são os maiores riscos de um eventual ataque contra um sistema elétrico?

O que eu vou falar tem um foco mais em energia elétrica, mas serve também para outras infraestruturas como água e óleo & gás também. Existe uma preocupação muito grande no design dos sistemas de automação em relação à disponibilidade. Há também preocupação com a performance nas funções executadas para ligar ou desligar os equipamentos e na tomada de decisões lógicas em um período de tempo muito curto. Esses sistemas são pensados para isso. No entanto, tradicionalmente, eles não são pensados para segurança e proteção de informações que estão circulando nesse tipo de sistema.

Um invasor externo pode comprometer uma rede para diminuir a performance de sistemas, caso não haja uma proteção para acesso a esses dados. Se o cracker tiver um conhecimento um pouco mais apurado do processo, não somente sobre a tecnologia de comunicação que está atacando, pode pontualmente desligar um disjuntor que alimenta uma linha de transmissão ou um circuito de transformador. Ele pode também alterar limites de monitoramento dessas máquinas, de tal maneira que o sistema responsável pelo monitoramento receba uma informação incorreta e, dessa forma, não tome uma ação para proteger esse ativo quando necessário. Então, há riscos tanto de indisponibilidade da instalação, perda de capital e até de danos à imagem da concessionária responsável.

Como o mercado elétrico brasileiro tem se posicionado frente a esse problema?

Esse é um tema que normalmente se discute muito em fóruns da área. É notório que em mercados como Estados Unidos ou Europa Ocidental existe um nível de maturidade maior, tanto em uso das técnicas de cibersegurança quanto na parte de regulação. O Brasil demorou um pouco para poder aderir a essa realidade. Aqui no país, existe uma preocupação muito forte em relação a como proceder para proteger a infraestrutura por parte das concessionárias, dos clientes, dos fabricantes, e dos reguladores (Aneel e ONS). Ou seja, como proteger os diferentes níveis da rede elétrica: desde a subestação até os centros de controle que se comunicam com o ONS.

Estamos vendo trabalhos muito interessantes do lado da Associação Brasileira de Distribuidores de Energia Elétrica (Abradee), da Associação Brasileira das Empresas de Transmissão de Energia Elétrica (Abrate), e da Associação Brasileira das Grandes Empresas Geradoras de Energia Elétrica (Abrage). O próprio ONS tem algumas iniciativas muito bacanas coordenadas com a Aneel. E os fabricantes estão se envolvendo também junto com os agentes. Agora, vemos um despertar muito forte. Há um grupo de trabalho muito interessante para resolver esse gap histórico.

Como essa questão de cibersegurança tem sido trabalhada e pensada dentro da Hitachi ABB? O que estão oferecendo ao mercado?

A Hitachi ABB Power Grids tem atuações tanto com o foco de produtos quanto na integração do sistema completo. Temos algumas políticas ou formas de trabalho que começam justamente no equipamento. Existe um tipo de ação que nós chamamos de hardening. Essa ação consiste em tomar ações para poder proteger um determinado dispositivo, independente do sistema ao qual ele será conectado.

Por exemplo: vamos supor que eu tenha um equipamento IED [intelligent electronic device], que faz a proteção e o controle de um circuito em uma subestação de energia. Esses equipamentos inteligentes têm capacidade de comunicação muito grande. A ação de hardening típica para isso é: se vou utilizar um determinado protocolo e uma porta de comunicação específica, as demais portas podem ser desligadas e, inclusive,

podemos desabilitar os protocolos usados para se comunicar com o mundo externo. Fazemos esse tipo de ação tanto no IED quanto no software. O hardening dá um passo adiante no design da arquitetura.

Existe uma série de discussões para fazer um tipo de design security by default, tomando cuidados para elencar as interfaces necessárias e evitando que haja vazamento de dados nesses sistemas ou subsistemas.

Uma coisa que precisamos mencionar sempre: não existe sistema 100% seguro. O que nós fazemos é mitigar os riscos para poder diminuir as possibilidades de um ataque se desenvolver. E que caso esse ataque tenha êxito, que as consequências sejam minimizadas. É isso que procuramos o tempo todo com nossos produtos e soluções.

Gostaria também que falasse sobre como deve ser a preparação dos profissionais do setor para lidar com essa nova realidade.

Essa pergunta é muito boa porque levanta um problema maior. Estamos falando muito de indústria 4.0. A revolução tecnológica pela qual estamos passando agora é comparável àquilo que aconteceu há 20 anos, quando deixamos as máquinas de escrever e os computadores começaram a se popularizar de fato. É uma quebra de paradigma muito grande em relação ao nível de automação aliada a TI.

É justamente em relação a TI que existe um ponto de atenção. Dentro desse ecossistema de automação de energia elétrica, é muito comum que os profissionais tenham conhecimentos profundos sobre eletrônica e elétrica. Mas a parte de TI é algo relativamente novo quando falamos de sistemas de condição crítica. Hoje, o profissional moderno que vai atuar nesse segmento precisa atuar nessas três esferas unidas: eletrônica, elétrica e tecnologia da informação. Estamos falando de um novo profissional, de fato, com conhecimento nessas três áreas.

As próprias universidades estão repensando a forma de como promover a engenharia elétrica, eletrônica ou mesmo as áreas de ciência de computação, para poder incluir pedaços dessas três áreas contidas nesses cursos. O que acontece muito também é que os fabricantes e próprios clientes estão formando profissionais com essas três características. Como a Hitachi ABB tem uma liderança de mercado em várias tecnologias, nossa contribuição é criar treinamentos para que consigamos, ao longo do tempo, formar profissionais com essas características.

Por falar em digitalização, a Hitachi ABB tem fornecido subestações digitais no Brasil. Quais são as vantagens dessas tecnologias?

No caso da energia elétrica, vou falar sobre as subestações digitais. Existe uma série de vantagens quando você usa fibras ópticas ao invés de cabos de cobre para fazer a conexão entre o pátio da subestação e a sala de controle.

A fibra óptica conectada aos equipamentos evita que você traga sinais de corrente e tensão elétrica para o painel da sala. Com isso, os profissionais de manutenção não lidam com essas grandezas elétricas diretamente. O risco de acidente acaba sendo bastante mitigado.

Outro ponto é que pelo fato dos cabos não serem necessários para trazer esses sinais para a sala de controle, a quantidade de material acaba sendo menor, com consequente redução de custo, redução de emissão de carbono e diminuição do tempo de instalação.

Há outro quesito bem interessante tem relação com o modelo de negócio existente no Brasil. É muito comum que tenhamos leilões de energia para criar novas subestações e ampliar empreendimentos. Com essa tecnologia digital, pelo fato da instalação ser mais simples, é possível reduzir o tempo de construção dos empreendimentos. Com

isso, as expansões são facilitadas em relação a custo, ao tempo da instalação e também para flexibilizar soluções com diferentes tipos de sistemas, lógicas ou de circuitos.

Quais são as perspectivas da companhia para o mercado brasileiro?

As perspectivas são muito positivas. Mesmo com tudo isso que estamos vivendo, com a pandemia de Covid-19, existe muita coisa a se fazer no país. Há muitas obras de infraestrutura no setor de energia elétrica. Temos observado uma escalada das energias renováveis no Nordeste do país. Temos uma base instalada de 15 GW a 17 GW, que deve crescer para 30 GW ou 40 GW nos próximos anos.

Além das energias renováveis, existe uma perspectiva de investimento muito forte em relação às subestações e linhas de transmissão. Nós prevemos um crescimento da economia quando essa questão da Covid-19 for debelada com a vacinação. A economia deve voltar aos eixos novamente e os investimentos devem voltar ainda com mais força. Os prognósticos são bem positivos.

(1) Artigo publicado no Brasil Energia. Disponível em: https://energiahoje.editorabrasilenergia.com.br/cinco-tendencias-de-eficiencia-energetica-para-alavancar-os-negocios/. Acesso em 19 de março de 2021.