*Por Rodrigo Leal**

Capítulo VIII

Uma visão holística sobre segurança cibernética no setor elétrico brasileiro

Como abordado anteriormente neste fascículo, o setor elétrico tem passado por grandes mudanças e trazendo enormes desafios para as empresas e agências do setor. O avanço tecnológico e o processo de digitalização estão proporcionando novas soluções e, com isso, mudando todo um ecossistema e processos associados, proporcionado melhorias significativas.

O processo de digitalização no setor elétrico torna-se cada vez mais relevante e é uma tendência irreversível, uma vez que traz ganhos em qualidade e desempenho, contribuindo com a modicidade tarifária.

Esta é uma viagem sem volta, visto que a digitalização está mudando o mundo como o conhecemos e está alterando a forma como vivemos, trabalhamos e nos relacionamos e não poderia ser diferente quando falamos sobre o setor de energia, nas áreas de geração, transmissão e distribuição.

O mundo possui hoje mais de 10 bilhões de dispositivos conectados, aumentando a superfície de contato – ou o perímetro –, ocasionando um aumento da exposição diária a ataques cibernéticos maliciosos, colocando nossas vidas e a estabilidade da nossa sociedade em risco. Com esse novo cenário, observamos uma explosão de incidentes cibernéticos nas mais diversas verticais de negócios, impactando inclusive empresas do setor de energia.

Neste contexto, a segurança cibernética tornou-se um tema de extrema relevância na sociedade em geral e tem sido assunto frequente também no setor elétrico ao longo dos últimos anos.

No Brasil, o tema vem ganhando tanta relevância que faz parte dos fóruns dos diversos setores de missão crítica e no setor elétrico já faz parte da agenda regulatória da Agência Nacional de Energia Elétrica (Aneel) e do Operador Nacional do Sistema Elétrico (ONS), conforme comentamos ao longo desta série de artigos.

A existência de uma regulamentação nacional para o setor elétrico é base para que um país tenha infraestruturas críticas de energia menos expostas e vulneráveis, garantindo a segurança nacional e capacidade de reação em caso de incidentes.

A necessidade de uma visão holística

No setor elétrico, atualmente, o assunto segurança cibernética tem sido tratado, em algumas empresas, de forma mais orquestrada e com apoio da alta administração. No entanto, o maior número de empresas não possui uma visão holística do cenário, com poucos recursos sendo disponibilizados para atacar o real problema, provavelmente, porque os investimentos em segurança cibernética não estavam sendo priorizados em seus planos de negócio.

Os ataques mais próximos das empresas do governo federal e do setor elétrico fizeram com que a Aneel acelerasse a publicação da política de segurança cibernética para o setor elétrico, que é válida para todas as geradoras, distribuidoras e transmissoras de energia no país, considerando que a ausência de uma política poderia aumentar os casos de interrupção do fornecimento de energia elétrica.

Com as novas regulamentações entrando em vigor, as empresas do setor elétrico foram levadas a incorporar, de forma obrigatória, em seu

BRVAL ELECTRICAL

CABINES PRIMÁRIAS APROVADAS NAS PRINCIPAIS CONCESSIONÁRIAS DO PAÍS.

NEOENERGIA · energisa · CPFL ENERGIA · edp · enel · Light · CEMIG · equatorial ENERGIA · COPEL

BR 6

Conjunto de manobra de média tensão isolação Ar/SF6.

G2 SLIM

Conjunto de manobra em média tensão isolado a ar.

PROSET

Conjunto de manobra em baixa tensão.

TRANSFORMADOR

A Seco De Média Tensão.

Nova Unidade

Sorocaba-SP

Rua **Ribeirão Preto**, nº **46**, bairro: **Jardim Leocadia**
Sorocaba-SP | CEP: 18085-380

21 **97105-6853** 21 **3812-3100** **brvalelectrical**

vendas@**brval**.com.br www.**brval**.com.br

SAIBA MAIS:

planejamento ações e investimentos em segurança cibernética para estar em conformidade com o mercado.

Maturidade operativa

As empresas já possuíam ações de segurança cibernética no ambiente corporativo, mas, com as novas regulamentações, as exigências agora englobam também o ambiente operativo.

De um modo geral, as empresas de energia possuem em seus ambientes operativos procedimentos, dispositivos e aplicações que fazem algum tipo de proteção contra ataques cibernéticos, porém, é fundamental que as empresas façam uma avaliação para entender o seu nível atual de maturidade.

A partir desta fotografia, é fundamental elaborar um plano, seguindo as melhores práticas, visando desenhar a jornada completa de segurança cibernética necessária para alcançar o nível de maturidade adequado para o setor, minimizando a exposição aos riscos e atendendo às novas exigências regulatórias do ONS e da Aneel

Essa jornada passa por um detalhamento completo do aspecto tecnológico, de processos e de cultura. Após a avaliação de maturidade, constata-se que as médias e grandes empresas do setor elétrico possuem problemas e riscos similares sobre os aspectos de segurança cibernética e se observa que parte deles são oriundos de tópicos relacionados a seguir:

- Estrutura organizacional;
- Políticas e procedimentos;
- Capacitação e treinamento;
- Arquitetura de redes;
- Gerenciamento de vulnerabilidades;
- Visibilidade da rede;
- Centro de Operação de Segurança;
- Autenticação forte e segura.

No que diz respeito à estrutura, muitas vezes, não temos uma área de segurança cibernética para ambientes operativos, sendo, inclusive, tratada como "apêndice". Grandes empresas estão se estruturando com a figura do CISO, executivo de cibersegurança, de forma independente e com acesso direto ao board da empresa.

Atualmente, as empresas com maior nível de maturidade, tem a figura do BISO (Business Information Security Officer), um profissional que tem conhecimento do tema, mas que atua diretamente com as áreas de negócio, funcionando como um facilitador do processo ao combinar as duas culturas - corporativo e negócios.

No tocante a políticas e procedimentos, as empresas estão se ajustando visando cumprir as novas exigências regulatórias, mas é necessário avançar de forma ágil. Na parte de capacitação e treinamento, de um modo geral, falta investimento.

O investimento em conhecimento é de suma importância atrelado ao grande desafio da falta de profissionais. Estima-se que hoje faltam 4 milhões de profissionais de cibersegurança no mundo, 441 mil só no Brasil.

Os treinamentos internos de conscientização são de suma importância, pois é provável que os empregados simplesmente não entendam a gravidade de uma ameaça cibernética e como ela pode impactar gravemente a empresa.

Os pontos relacionados à área de tecnologia foram abordados nos artigos anteriores e podem ser consultados por meio da revista impressa ou digital (www.osetoreletrico.com.br) .

É importante observar que nem todas as empresas precisam ter os mesmos níveis de maturidade em segurança cibernética. Alguns fatores que podem influenciar as decisões de investimento incluem:

- Regulamentos;
- Legislações ;
- Estratégias de negócios;
- Apetite aos riscos;
- Receita associada.

As exposições advindas dos temas aqui relacionados aumentam os riscos e, consequentemente, diminuem o nível de maturidade da empresa. A jornada de segurança cibernética endossada pela alta administração da empresa é um fator chave de sucesso.

Preocupação com a cadeia produtiva

Para finalizar esta série de artigos, destaco que é fundamental também nos preocuparmos com toda nossa cadeia produtiva, realizando uma gestão de segurança cibernética de terceiros, fornecedores e clientes.

Nada adianta termos a melhor tecnologia e melhores processos se um terceirizado não estiver envolvido no tema como parte do ecossistema, por exemplo.

Assim, encerramos esta série de artigos do Fascículo de Segurança Cibernética no Setor Elétrico e reforço que não existe "bala de prata" para tratar este relevante tema e, por isso, a necessidade de uma abordagem holística e investimentos com o objetivo de proteger o perímetro das ameaças e mitigar a exposição ao risco.

**Rodrigo Leal é graduado e Mestre em Engenharia Elétrica com MBA em Gestão de Projetos e cursando MBA Executivo de Negócios do Setor Elétrico pela Fundação Getúlio Vargas. Desde 2006 é funcionário da Chesf, onde já exerceu cargos de Assessor e Gerente, na área de Telecomunicações, Proteção e Automação. Atualmente está como assessor do Diretor de Operação, coordenando vários processos da diretoria, incluindo os assuntos relativos à tecnologia operativa. Atualmente ocupa posição de Vice-Presidente do Conselho Diretor da UTC América Latina e Coordenador do Comitê de Tecnologia da Informação e Telecomunicações no CIGRE-Brasil.*