*Por Marcelo Branquinho e Rodrigo Leal**

Capítulo VII

Ambiente regulatório de segurança cibernética para empresas de energia no Brasil

Risco sistêmico: setor elétrico na berlinda

A explosão de um transformador deixou o estado do Amapá sem energia em novembro de 2020 e expôs fragilidades. Um dos maiores blecautes do país deixou quase 800 mil pessoas sem energia por 22 dias, dos quais quatro deles na escuridão total.

Um incidente como este poderia ser causado por um ataque cibernético? Sim.

Os ataques cibernéticos podem interromper a geração de usinas de energia, causar danos a equipamentos do sistema de transmissão e distribuição, operar sistemas por meio de acesso aos centros de operação, podendo criar desequilíbrio no sistema elétrico e numa maior gravidade causar blecaute de grandes proporções.

Para tentar diminuir este risco sistêmico, a Agência Nacional de Energia Elétrica (Aneel), juntamente com o Operador Nacional do Sistema Elétrico (ONS), está trabalhando há alguns anos em procedimentos que blindem as estruturas elétricas contra riscos cibernéticos. Em 2021 foi publicada a RO-CB.BR.01, pelo ONS, e emitida Resolução Normativa Aneel Nº 964, de 14 de dezembro de 2021 que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

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.

Política de segurança cibernética da Aneel

Os ataques hackers ao Ministério da Saúde, que derrubou o ConectSus, e contra a Polícia Rodoviária Federal, entre outros órgãos, foram sinais de alerta para os setores de missão crítica no Brasil. Prova disto é que a Aneel acelerou a publicação da política de segurança cibernética para o setor elétrico, válida para todas as geradoras, distribuidoras e transmissoras de energia no país.

O Conselho Nacional de Energia Elétrica (CNPE) já tinha aprovado as diretrizes para a política de segurança cibernética, mas essas normas ainda dependiam de uma regulamentação da Aneel para entrar em vigor. A nova resolução traz as diretrizes e os parâmetros mínimos a serem adotados, assim como orientações sobre as melhores práticas para o setor.

Segundo documento publicado no site da Aneel, cada agente e entidade deverá descrever em sua política a gestão, a avaliação e o tratamento dos riscos de segurança cibernética, incluindo procedimentos de resposta rápida para contenção de incidentes. Além disso, deve ser promovida junto aos funcionários uma conscientização acerca dos riscos cibernéticos por meio de exercícios cibernéticos. Entre os requisitos estabelecidos, estão:

- Obrigatoriedade de informar à Aneel casos de crise em segurança cibernética;
- Obrigatoriedade de compartilhamento de incidentes cibernéticos relevantes entre os agentes e entre os agentes e a

Aneel;

- Obrigatoriedade de a empresa escolher e aplicar periodicamente uma metodologia de avaliação de maturidade regulatória;
- Segmentação de redes de operação (TO) da TI e da Internet;
- Procedimentos de resposta rápida para contenção de incidentes;
- Implementação de processos de gestão, avaliação e tratamento dos riscos de segurança cibernética.

Segundo a Aneel, a ausência de uma política poderia aumentar os casos de interrupção do fornecimento de energia elétrica e abrir brecha para incidentes de segurança envolvendo dados. A conclusão dos trabalhos foi antecipada em seis meses diante da importância do tema.

Rotina operacional RO.CB.BR.01 do ONS

O setor elétrico brasileiro dispõe de um sistema interligado com mais de 145 mil km de linhas de transmissão em alta tensão, que conecta 170 GW de usinas geradoras de energia dispersas pelo território nacional aos centros de consumo. Ataques cibernéticos podem provocar "apagões" e impor o caos em extensas regiões do país. Trata-se, portanto de uma questão de segurança nacional que agora integra a Rotina Operacional sobre Segurança Cibernética (RO.CB.BR.01), publicada pelo Operador Nacional do Sistema Elétrico (ONS) no dia 9 de julho de 2021.

Pelo ONS, antes da publicação da RO-CB.BR.01, existia apenas um item nos Procedimentos de Rede que tratava do assunto, mas de forma abrangente. Os possíveis impactos da R.O. têm chamado a atenção dos agentes de geração, transmissão e distribuição elétrica e o assunto ganhou repercussão na mídia nacional e especializada.

Existe um risco sistêmico no Sistema Interligado Nacional (SIN), devido ao fato de as redes das empresas de energia estarem conectadas à rede do ONS. Isso significa que se uma delas for infectada por ransomware, por exemplo, pode haver propagação para todos os agentes do sistema. O objetivo da nova rotina operacional é justamente proteger contra esse risco.

O processo de aprimoramento da segurança cibernética já vinha sendo discutido pelo setor elétrico há algum tempo, em especial pelo ONS, pela Aneel e pelo Ministério de Minas e Energia (MME), mas ganhou relevância a partir do ano passado, em decorrência do aumento exponencial dos ataques às empresas de energia elétrica.

O ONS determinou que todas as empresas conectadas a ele implementem um conjunto de procedimentos e sistemas de segurança cibernética no prazo de até 27 meses, a contar da data da publicação.

A nova rotina operacional RO-CB.BR.01 deve ser implementada por todas as empresas de energia que compõem o ARCiber, incluindo os centros de operação dos agentes, equipamentos que participem da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes e o ambiente operativo do ONS.

Composta por 24 itens referentes a contramedidas de segurança cibernética globais, a rotina operacional é, na prática, um desafio de implementação para as empresas de energia dada sua complexidade e o grande número de soluções envolvidas, como mostra a tabela 1.

Tabela 1 – Correlação entre requisitos da rotina operacional do ONS e soluções tecnológicas

Item	Descrição	Capacitação	Planejamento	Políticas	NGFW	EDR	IDS Industrial	Acesso Seguro	Gestão de senhas	Logs	IDS-SOC
4.1.1.	As redes devem ser segregadas em zonas de segurança, de acordo com a sua função.		•		•						•
4.1.2.	O ARCiber não deve ser diretamente acessível através da internet mesmo que protegido por um ou mais firewalls, bem como seus ativos.				•						•
4.1.3.	O acesso ao ARCiber a partir de redes externas à organização (como, por exemplo, a internet) somente deve ser permitido para o desempenho de atividades autorizadas.							•			•
4.1.4.	Soluções Antimalware devem ser implementadas no ARCiber e mantidas atualizadas.					•					•
4.2.1.	Deve ser nomeado pelo menos um gestor responsável pela segurança cibernética do ARCiber e atuar como ponto de contato externo.	•		•							
4.2.2.	Deve ser estabelecida política que defina papéis e responsabilidades em relação à segurança cibernética do ARCiber.			•							
4.3.1.	Todos os ativos, softwares e hardwares, conectados ao ARCiber devem ser inventariados minimamente a cada 24 meses.						•				•
4.3.2.	O inventário dos ativos deve ser armazenado de forma segura, com acesso restrito às pessoas que necessitem das informações para o exercício de suas funções.			•							
4.3.3.	Padrões de configuração segura (hardening) devem ser criados conforme política de segurança do agente.			•							
4.4.1.	Devem ser implementadas rotinas de atualização de pacotes de correção de segurança (patches) para todas as tecnologias conectadas ao ARCiber.			•			•				•
4.4.2.	Novos ativos somente deverão ser conectados ao ARCiber após a aplicação de todos os pacotes de correção de segurança disponíveis.			•							•
4.5.1.	Deve existir uma política de gestão de acessos e identidades.			•							
4.5.1.1.	Credenciais de acesso devem ser individuais e aprovadas pela alçada competente.			•					•		•
4.5.1.2.	Deve existir uma política de senhas que contemple: tamanho mínimo, complexidade, máximo de tentativas de acesso e prazo máximo para troca da senha.			•					•		•
4.5.1.3.	Na construção dos perfis de acesso deve-se seguir o princípio de minimização (somente deve-se conceder o acesso mínimo necessário).			•					•		•
4.5.1.4.	Deve existir um prazo máximo para cancelamento/remoção de credenciais de usuários desligados.			•					•		•
4.5.1.5.	Credenciais de acesso privilegiadas devem estar sujeitas a controles específicos.			•				•	•	•	•
4.5.1.6.	As características especiais das credenciais de acesso padrão embarcadas (locais) nos sistemas operacionais e softwares devem ser consideradas em política.			•					•		•
4.6.1.	Os ativos do ARCiber devem estar configurados para gerar logs de segurança apropriados para suportar investigações e a reconstrução de possíveis incidentes de segurança.			•						•	
4.6.2.	Os dispositivos de segurança como Firewalls, IDS/IPS, Antimalware e subsistemas de autenticação devem estar configurados para gerar alertas caso identifiquem atividades suspeitas.			•						•	•
4.6.3.	Devem ser estabelecidos mecanismos para identificação e resposta a incidentes cibernéticos tempestivamente.			•							•
4.6.4.	Deve ser implementado um plano de resposta a incidentes cibernéticos.		•	•							•
4.6.5.	Testes de ativação dos planos de resposta a incidentes cibernéticos devem ser realizados periodicamente.			•							•
4.6.6.	Incidentes cibernéticos que afetem ativos do ARCiber devem ser informados ao ONS, conforme Rotina Operacional específica.			•							•
5.2.b	Cabe a cada organização adotar controles de segurança cibernética, conforme suas próprias políticas, diretrizes e avaliações de riscos.	•	•								

Remuneração dos investimentos

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 a capacidade de reação em caso de incidentes.

E para que as empresas de energia consigam realizar os investimentos necessários para garantir o atendimento às novas regulamentações é fundamental que também sejam remunerados de forma adequada visando a integração destas melhorias ao sistema em operação.

Um ponto importante e necessário é a revisão do Manual de Controle Patrimonial do Setor Elétrico (MCPSE) considerando estas novas necessidades de forma mais clara e objetiva, e principalmente, realizando ajuste no tempo de vida útil dos equipamentos de tecnologia operacional, pois estes equipamentos possuem ciclo de vida menor que o atualmente proposto no manual.

Bibliografia

www.ons.org.br
www.aneel.gov.br

** Marcelo Branquinho é engenheiro eletricista com especialização em sistemas de computação e MBA em gestão de negócios, sendo fundador e CEO da TI Safe. Especialista em segurança cibernética industrial, é autor de diversos livros técnicos e trabalhos publicados e frequente apresentador de estudos técnicos em congressos internacionais. Membro sênior da ISA Internacional, atua em diversos grupos de trabalho, como o da atual ISA/IEC-62443.*

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.