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

Não subestime o risco

BRANQUINHO, Marcelo: "Não subestime o risco". Brasil Energia, Rio de Janeiro, 09 de setembro de 2018.

Nos próximos 30 anos, o consumo energético do brasileiro deverá triplicar, chegando a 1.624 terawatt-hora (TWh), segundo levantamento da Empresa de Pesquisa Energética (EPE). Um dos caminhos para aumentar a produção e obter um aproveitamento melhor da energia é a digitalização das operações. Além da busca por maior eficiência operacional, a modernização das redes elétricas permite a oferta de novos serviços, maior interação com os clientes e novas fontes de energia. Como vemos, a evolução tecnológica traz uma nova perspectiva para o setor e cria oportunidades, mas, por outro lado, aumenta a vulnerabilidade dos sistemas e redes, principalmente a ataques cibernéticos.

Invasão *hacker* em infraestruturas críticas, como o sistema elétrico, é particularmente preocupante, pois pode causar impactos econômicos, financeiros, ambientais e até mesmo perdas cíveis.

Atualmente, o *ransomware* é a principal arma utilizada por *hackers* no mundo e um dos maiores pesadelos dos gerentes de redes industriais. Além dos recursos destrutivos inerentes a esse *malware*, os mecanismos de dispersão geralmente sobrecarregam as redes de automação com pacotes de dados indesejados e afetam, gradualmente, o tempo de resposta da rede até que ela paralise completamente.

Com esse ataque, um *hacker* pode bloquear o acesso à interfaces homem-máquina; criptografar estações de trabalho de engenharia; bloquear o acesso a sistemas utilitários; infectar outras plantas através da rede de automação, só para citar alguns exemplos. É também um tipo de vírus que "sequestra" as informações do computador e cobra um preço para devolvê-las, ou seja, pode ser bem utilizado por ataques realizados por motivações financeiras. Nessa categoria, está o *WannaCry*, que, em 2017, atingiu hospitais, empresas de telefonia, tribunais de justiça e levou várias empresas e órgão públicos a paralisar as suas atividades. Então, não estamos mais imaginando se invasões desse tipo vão acontecer, mas quando acontecerão.

A introdução de soluções "inteligentes" para melhorar a gestão da eletricidade aumenta o número de pontos de entrada para invasores, mas há outros fatores que agravam esse cenário. As redes mais antigas não conseguem passar por atualizações de segurança por incompatibilidade com os softwares atuais, o que exigirá das empresas investimento financeiro. Aliás, esse é outro motivo que inibe a devida atenção à proteção cibernética: as empresas veem segurança como custo por não gerar retorno financeiro. Mas as consequências de um ataque a uma rede de automação podem sair mais caras do que o investimento necessário para a defesa dos ativos, dos prejuízos financeiros e da reputação da companhia. A imprevisibilidade dos ataques cibernéticos, que evoluem mais rápido que as contramedidas, agravada pela dificuldade de realizar nas empresas análises de riscos de segurança cibernética, e o baixo índice de incidentes no Brasil também minoram a percepção ao risco.

Como as empresas brasileiras ainda não são obrigadas a informar tentativas de ataques nem invasões bem sucedidas, o que tende a mudar com o Regulamento

Geral sobre a Proteção de Dados europeu e com a Lei Geral de Proteção de Dados brasileira, pois elas se protegem. Diante desse cenário, observamos que os investimentos em segurança cibernética como precaução são exceção. Os motivos para investir estão mais relacionados às exigências de *compliance*, o que aumentou com a operação de multinacionais no Brasil, e aos ataques sofridos.

É preciso mudar a cultura da não prevenção aos riscos no Brasil. Nos Estados Unidos e Europa, agências governamentais como NIST, NERC/CIP, ENISA, CENELEC desenvolveram diversas publicações de melhores práticas e procedimentos para atender às necessidades de proteção das empresas de energia elétrica e suas infraestruturas de missão crítica. São documentos que, sem dúvida, podem ajudar na regulamentação da cibersegurança do setor elétrico brasileiro. Obter uma maior resiliência a esse risco, adotando requisitos mínimos de segurança, modelos de padronização de procedimentos e certificação é fundamental não só para a sustentabilidade dos negócios como para a segurança do sistema elétrico, da sociedade e da economia de um país.

Marcelo Branquinho é CEO da TI Safe, graduado em engenharia elétrica, especialista em segurança de sistemas SCADA e membro da International Society of Automation (ISA)