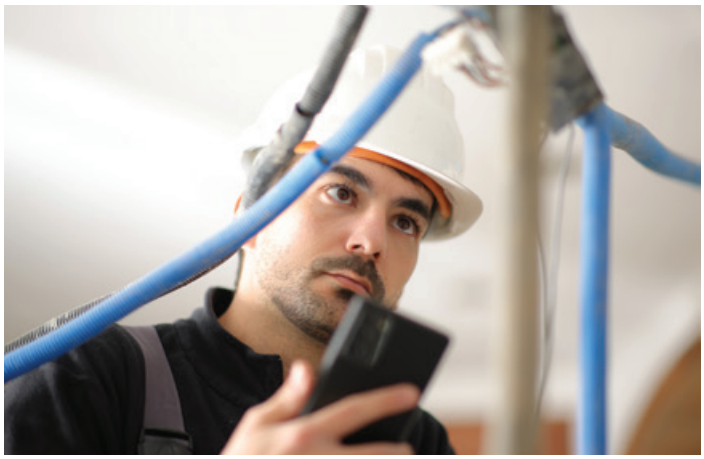
Manter a segurança a longo prazo nas instalações elétricas críticas

Alexandre Monteiro
Business Development Industry Cross Selling Iberia
Schneider Electric



À medida que a rede elétrica se digitaliza, torna-se um alvo privilegiado dos ciberataques. A digitalização permite uma melhor gestão da energia, através da monitorização e do ajuste da rede em tempo real, o que é benéfico tanto do ponto de vista climático, como económico. No entanto, pôr fim ao isolamento dos sistemas elétricos aumenta a sua vulnerabilidade. Um ciberataque a um operador de rede pode pôr em perigo a sociedade através de um efeito dominó que causa impacto noutras infraestruturas críticas, levando por exemplo ao encerramento de hospitais e até à paralisação da economia.

Já há muito tempo que a segurança das instalações elétricas foi identificada como um problema, levando as autoridades a pressionarem os *players* do setor da energia para que protegessem as suas instalações – uma preocupação que em Portugal está refletida no Decreto-Lei n.º 62/2011, que estabelece medidas específicas para a proteção de infraestruturas críticas, incluindo as do setor da energia. No entanto, a crescente sofisticação dos ataques e o número crescente de *players* nas redes elétricas dos países exigem a revisão e o aumento dos controlos, requisitos e regulamentos para manter uma boa cibermaturidade a longo prazo. Para atingir este objetivo, a colaboração entre todos os *stakeholders* do ecossistema – fornecedores de soluções de energia, gestores da rede e outros – parece ser a melhor estratégia a seguir.

UMA ABORDAGEM DE SEGURANÇA DO PROJETO DE CONCEÇÃO À OPERAÇÃO

Com o desenvolvimento das energias renováveis, novos produtos digitais, como painéis solares, estações de carregamento de veículos elétricos (VE) e outros produtos relacionados, estão a ser integrados na rede elétrica. Tal como os sistemas elétricos originais, estes novos produtos não foram necessariamente concebidos com um requisito de segurança desde a conceção, oferecendo aos *hackers* pontos de entrada novos e mais acessíveis. Embora seja cada vez mais aceite que a segurança "*por defeito*" é essencial para alcançar a cibermaturidade, esta é uma condição necessária, mas não suficiente.

Tendo em conta o volume muito elevado de exposições de produtos ou de automação na Internet e as lições aprendidas com a experiência no terreno, a segurança desde a conceção só pode dar frutos se for acompanhada de configurações adequadas ao longo do ciclo de vida dos equipamentos, o que se designa por "*secure-by-operations*".

A manutenção da segurança tornou-se crucial para proteger os sistemas de informação, incorporando, por exemplo, a monitorização de vulnerabilidades e a segurança do acesso remoto para a manutenção que não é realizada no local. Na prática, quando existem configurações com falhas de segurança, estas passam muitas vezes despercebidas devido à falta de conhecimento e de formação na matéria por parte dos operadores, que são mais eletricistas do que especialistas em TI.

MELHORAR, OTIMIZAR E DIVERSIFICAR AS CIBERCOMPETÊNCIAS DOS OPERADORES

Tendo em conta esta observação, é importante compreender que a maturidade de cibersegurança da rede elétrica só pode ser alcançada colocando os seres humanos no centro da equação. Compreender as ciberameaças exige uma educação para o risco. Para os trabalhadores dos setores industrial e elétrico, a formação e a sensibilização devem agora ser acompanhadas pelo desenvolvimento de