Uma abordagem sistêmica para segurança cibernética[1]

Nivalde de Castro[2]
André Clark[3]

Entre as muitas transformações que têm impactado os setores produtivos em escala global, a segurança cibernética (SC) merece destaque, principalmente em razão dos ataques que empresas estão sofrendo, como retratado em matérias recentes do Valor Econômico. Estes crimes cibernéticos colocam em risco os fluxos de produção e a interação com clientes, além de acarretar furto de dados e cobranças de resgates em dinheiro, indicando a gravidade crescente desta questão.

A ainda frágil interação regulatória entre os agentes públicos e privados, a necessidade de regras e o aprimoramento de instrumentos de defesa cibernética tornam-se uma exigência crítica. Este contexto preocupante ganha uma dimensão prioritária nos Conselhos Administrativos de grandes empresas, transformando-se em tema estratégico de governança. A cada novo ataque, aumentam as responsabilidades dos CEOs em garantir a segurança dos dados de seus clientes, fornecedores, funcionários e demais *stakeholders*.

Às empresas não bastará dispor só de estruturas seguras, mas será exigida uma segurança cibernética certificada

A preocupação com a segurança cibernética cresce em uma velocidade exponencial especialmente para o setor de energia, em função do aumento da

[1] Artigo publicado no Valor Econômico. Disponível em: https://valor.globo.com/opiniao/coluna/uma-abordagem-sistemica-para-seguranca-cibernetica.ghtml . Acesso em 01 de setembro de 2021.

[2] Professor do Instituto de Economia da UFRJ e coordenador no GESEL - Grupo de Estudos do Setor Elétrico.

[3] General Manager da Siemens Energy Brasil

percepção social e política decorrente da transição energética mundial, focada na descarbonização dos setores produtivos, com metas exigentes e ambiciosas, na descentralização da geração de energia, ampliando os recursos energéticos distribuídos na matriz elétrica, e na digitalização da interação entre os processos produtivos, determinando uma economia cada vez mais intensiva em dados, que assumem valor crescente.

Recentemente, os impactos da pandemia impondo medidas de *lockdown* e de *home office*, que se mostrou essencial para a manutenção das atividades produtivas, de ensino e de vários serviços, com destaque para o comércio virtual, aceleraram e dinamizaram o processo de digitalização mundial.

Além disso, a difusão da tecnologia 5G no aparato produtivo e social vai intensificar as perspectivas da digitalização da sociedade. Se, hoje, o grau de interconectividade entre smartphones e outros equipamentos eletrônicos é expressivo, pode-se esperar um mundo ainda mais interligado, com a inclusão de equipamentos residenciais, veículos elétricos, ativos físicos das empresas e infraestruturas econômicas dos países, em especial o setor elétrico, que garante, em última instância, a interação de praticamente tudo.

Em suma, a digitalização é um caminho irreversível, com a certeza de que os seus benefícios têm potencial para tornar as empresas mais eficientes e a qualidade de vida da sociedade melhor.

Uma contrapartida preocupante da aceleração da digitalização, porém, é o aumento das superfícies de ataques cibernéticos, que ampliam ainda mais os riscos de invasão aos sistemas de empresas e instituições públicas. Por isso, é preciso endereçar a questão dos ataques cibernéticos para a segurança dos negócios e dos países.

Durante a pandemia, o número de ataques cresceu de forma alarmante. Nos Estados Unidos, o governo precisou enfrentar ameaças a seu sistema de defesa. No Brasil, por exemplo, ações na *dark web* possibilitaram o acesso a mais de 240 milhões de CPFs.

Contudo, a ameaça já não está apenas nas estruturas das tecnologias da informação das corporações. A tecnologia operacional das empresas também está sob risco. Os crimes cibernéticos podem produzir prejuízos de diferentes naturezas e gravidades, desde o furto de dados de clientes até o bloqueio do fornecimento de energia.

No caso do setor elétrico brasileiro, que 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. Este exemplo, per se, já qualifica os riscos cibernéticos como uma questão de segurança nacional.

Em outro nível, há uma tendência crescente de exigir garantias dos investidores e das fontes de financiamento com compromissos efetivos com o nível de segurança cibernética, além da conformidade com o meio ambiente e com o respeito aos direitos humanos. E, nesta linha, às empresas não bastará dispor somente de estruturas cibernéticas seguras, mas, cada vez mais, será exigida uma segurança cibernética certificada.

A boa notícia é que o Brasil é um país com um histórico positivo em relação à incorporação de novas tecnologias. Desde os anos de 1990, a sociedade brasileira absorveu práticas como transações bancárias pela internet, declaração de Imposto de Renda online, além do voto eletrônico há mais de duas décadas. Portanto, os exemplos citados indicam a capacidade econômica, social e científica de desenvolver e assimilar tecnológicas disruptivas. O desafio, no entanto, é a velocidade com que a digitalização avança. A política nacional de segurança cibernética do Brasil já existe, mas a sua atualização deve ser constante, como se as estruturas sob ameaça fossem uma espécie de alvo em movimento.

Quando o alvo dos ataques são as infraestruturas de energia, as consequências para a sociedade podem ser altamente danosas com prejuízos econômicos e sociais imensuráveis. Tão importante quanto uma política de Estado que regulamente a segurança dessas estruturas são os investimentos das empresas para criar continuamente barreiras aos ataques cibernéticos.

Este movimento, para ser realmente efetivo, deve ocorrer de forma dinâmica com participação integrada entre as instituições de Estado, setores econômicos e Academia em uma abordagem sistêmica criando instâncias e centros de excelência, pois o tempo urge.