Infraestruturas Críticas: O ataque cirúrgico ao coração das sociedades

digitalinside.pt/infraestruturas-criticas-o-ataque-cirurgico-ao-coracao-das-sociedades

Bruno Castro 3 de maio de 2024

As infraestruturas e setores críticos são cada vez mais o principal alvo da cibercriminalidade, ciberespionagem e, mais recentemente, de ciberataques destrutivos de larga escala. As redes de comunicação e computação não são apenas infraestruturas críticas por si só, mas sustentam muitos outros sectores de enorme criticidade para o bem-estar de uma nação, como a energia, petróleo, transportes, finanças, saúde, e, portanto, o seu mau funcionamento ou até a sua interrupção terá um efeito em cascata em várias outras infraestruturas ou serviços que dependem dos mesmos podendo gerar o caos pela sua inoperância.

Relativamente ao panorama europeu, a maioria das infraestruturas críticas da União Europeia (UE) são operadas através de plataformas de controlo industrial (ICS). Ora, estes sistemas foram projetados e desenvolvidos como sistemas autónomos, com conetividade limitada com o mundo exterior, e assentes em protocolos proprietários de cariz industrial que deveriam conviver num ecossistema extremamente controlado face à sua criticidade. No entanto, e com a crescente necessidade de interagir com esses mesmos ecossistemas, tem vindo a existir uma tendência de intercetar essas "cápsulas estanques" com o mundo exterior, permitindo que os componentes dos ICS acedam à internet, e assim, acabem por se tornar mais vulneráveis a interferências externas. Os esforços para incrementar os níveis de segurança dos ecossistemas onde vivem as infraestruturas críticas, nomeadamente os sistemas de ICS, devem ser devidamente acautelados na estratégia de segurança das organizações e instituições, algo que não será simples, nem rápido, nem económico – no entanto, tendo em consideração a sua criticidade para a estabilidade de uma (ou mais) nações, terá de ser colocado na agenda dos decisores.

Desta forma, o grande desafio reside na tensão entre impulsionar a modernização da tecnologia, nomeadamente, em áreas onde existe enorme resistência, e, simultaneamente, garantir a proteção das infraestruturas críticas face à transformação digital, e de cibersegurança, que a própria modernização obriga. A título de exemplo, muito se tem discutido sobre a aplicabilidade dos conceitos de inteligência artificial na modernização de infraestruturas críticas, resistentes a estes novos conceitos inovadores, contudo, também terá de ser ponderado o risco cibernético que a interceção destes dois mundos, um mais conservador e robusto versus outro mais inovador, experimental e menos seguro, tem como impacto no nível de cibersegurança a nível global.

Outra questão importante diz respeito ao facto de a UE importar muitos produtos e serviços de cibersegurança, o que aumenta de forma exponencial, o risco de dependência tecnológica de operadores de países terceiros. Esta realidade mina a segurança das infraestruturas críticas da UE, que também são apoiadas por complexas

cadeias de abastecimento globais. Assim, o desafio de proteger infraestruturas críticas passará também pelo desafio de a própria UE passar a ter uma estratégia de autonomia e independência tecnológica no que respeita a adquirir maior inovação e desenvolvimento de tecnologia de suporte a infraestrutura críticas, em particular, ao nível da cibersegurança.

Outro ponto fundamental tem ainda a ver com o facto de a maior parte das infraestruturas críticas da UE pertencer a operadores privados, e por muito que estes se esforcem para tornar essas mesmas infraestruturas mais seguras e resilientes, tal poderá não acontecer da forma mais célere e eficaz desejável sem a cooperação e o apoio contínuo das autoridades públicas, quer a nível nacional, quer da UE. A cooperação entre o setor privado e público será fundamental para robustecer o desenvolvimento das tecnologias de suporte às infraestruturas críticas, a curto prazo. Não poderá ficar apenas a cargo do setor privado.

Esta é uma responsabilidade partilhada, a qual carece de colaboração, cooperação ativa e partilha de informação entre os setores público e privado, bem como entre os diferentes setores verticais de infraestruturas críticas que suportam a estabilidade das sociedades. Eles têm a experiência e o conhecimento prático, e como tal, têm de ter um peso significativo na definição dos processos de tomada de decisão estratégica.

Atualmente, com a Diretiva NIS2, a UE terá um quadro jurídico atualizado e abrangente – ou pelo menos assim se espera – para reforçar a resiliência cibernética de infraestruturas críticas ao introduzir medidas mais rigorosas e responsabilidades acrescidas para proteger as infraestruturas e os serviços essenciais, ainda assim, ficam as considerações de que para que a cooperação atinja os objetivos desejados, serão relevantes para o setor público e privado as seguintes quatro premissas: 1) atribuição de responsabilidades; 2) identificação dos recursos existentes; 3) monitorização e investimento eficiente na proteção de infraestruturas críticas; e 4) diálogo e estreita coordenação nas respostas.

As infraestruturas críticas tornaram-se efetivamente uma parte integrante e essencial para o bem-estar das sociedades modernas, e a disrupção das mesmas implicará, certamente, consequências tão devastadoras e por vezes inimagináveis, sendo da responsabilidade de todas as partes – público e privado e indústria e academia/universidades -, garantir a segurança e zelar pela proteção deste órgão tão vital.
