VisionWare since 2005

ESTADO CIVIL DA NAÇÃO: NUMA RELAÇÃO COMPLICADA COM A GEOPOLÍTICA

HOJE, UM CONFLITO NO MÉDIO ORIENTE, UMA ESCALADA ENTRE POTÊNCIAS OU UMA NOVA VAGA DE TENSÕES INTERNACIONAIS PODE TRADUZIR-SE, POUCOS DIAS DEPOIS, NUM ATAQUE AOS SISTEMAS DE UMA EMPRESA PORTUGUESA

Não porque essa empresa tenha tomado partido até porque tal seria improvável, mas simplesmente porque faz parte de uma cadeia de abastecimento global, presta serviços a um determinado setor ou Estado, ou representa um alvo suficientemente visível para servir uma causa política.

Nos últimos meses, grupos hacktivistas têm reivindicado ataques contra entidades portuguesas ligadas à energia, aos portos, aos media e ao setor público. Em muitos casos, o impacto operacional foi limitado, mas esse não é o ponto. O verdadeiro significado destes episódios é outro: Portugal entrou definitivamente no radar de campanhas que têm origem em conflitos e interesses internacionais e que utilizam o ciberespaço para amplificar mensagens políticas, provocar disrupção ou testar capacidades.

Entretanto, o Centro Nacional de Cibersegurança britânico alertou para o aumento do risco dirigido a organizações com cadeias de abastecimento ligadas ao Médio Oriente. Não se trata apenas de empresas instaladas na região. Basta depender de fornecedores, parceiros tecnológicos ou operações críticas localizadas em geografias expostas para que o perfil de risco se altere significativamente. A questão

BRUNO CASTRO, VISIONWARE

é saber quantas empresas portuguesas conhecem realmente esse risco. Provavelmente, menos do que imaginam.

Durante demasiado tempo, habituámo-nos a medir a maturidade da cibersegurança pelo número de soluções tecnológicas implementadas. Compraram-se firewalls, sistemas de deteção, plataformas de monitorização e ferramentas de autenticação. Tudo isso continua a ser indispensável. Mas nenhuma dessas tecnologias consegue responder à pergunta mais importante: como é que um conflito geopolítico altera o perfil de risco da minha organização?

Os relatórios do World Economic Forum (WEF) têm vindo a mostrar que o contexto geopolítico passou a ser uma das principais preocupações dos líderes empresariais quando definem as suas estratégias de cibersegurança. As empresas reconhecem que a fragmentação internacional, os conflitos regionais e a crescente rivalidade entre Estados estão a aumentar a probabilidade de ataques, interrupções nas cadeias de abastecimento, campanhas de desinformação e operações de espionagem.

Em Portugal, essa consciência ainda parece avançar a duas velocidades. As grandes organizações começam, lentamente, a integrar a geopolítica na gestão do risco. Não apenas porque a realidade o exige, mas também porque diretivas como a NIS2 vieram lembrar que a resiliência deixou de ser uma opção. Os conselhos de administração falam hoje mais de continuidade de negócio e serviços de Intelligence sobre ameaças, do que falavam há cinco anos, e isso já é positivo.

As PME continuam a acreditar que são demasiado pequenas para interessar aos atacantes e esse é um dos mitos mais perigosos da atualidade. Não são atacadas apesar de serem pequenas. Muitas vezes, são atacadas precisamente por serem pequenas.

Os cibercriminosos e os grupos patrocinados por Estados perceberam há muito tempo que é mais fácil comprometer um fornecedor do que atacar diretamente uma grande empresa. É a lógica da cadeia de abastecimento: a resistência do sistema depende muito da resiliência, ou ausência dela, do elo mais fraco.

É por isso que o debate sobre geopolítica deixou de ser uma preocupação exclusiva das empresas exportadoras ou das multinacionais. Uma pequena empresa industrial em Leiria, um fornecedor tecnológico em Braga ou uma empresa de logística em Setúbal podem estar expostos a riscos internacionais sem nunca terem aberto um escritório fora de Portugal, basta integrarem a cadeia de valor errada no momento errado. Talvez esse seja o maior equívoco da atualidade, pensar que a distância geográfica oferece proteção, num mundo digital onde essa distância praticamente desapareceu.

A pergunta que as empresas deveriam fazer não é se serão alvo de um ataque motivado por fatores geopolíticos. É perceber quando, por que motivo e através de que dependência esse impacto poderá chegar. ◀