A defesa da Nação também depende da ação dos privados

dinheirovivo.pt/opiniao/a-defesa-da-nacao-tambem-depende-da-acao-dos-privados-15931675.html

2 de março de 2023

As ameaças cibernéticas são um perigo real e crescente para as sociedades. Nesta era digital, estamos todos interligados, e com isso advém o risco de atores maliciosos utilizarem a Internet, para espalhar o medo e perturbar a ordem, gerando o caos nas sociedades modernas. Desde roubo de identidade a violações de dados, passando pela interrupção de serviços vitais para as comunidades, estas ameaças podem ter implicações de grande alcance para indivíduos, empresas e Governos.

Nos últimos anos, a ameaça da cibercriminalidade tornou-se proeminente. A comunidade cibercriminosa está a visar cada vez mais os setores público e privado, sem grande distinção, roubando informação sensível e perturbando as operações de forma altamente disruptiva. Além disso, temos comprovado toda a complexidade e polivalência dos recentes ciberataques, que podem ser utilizados para espalhar informação e propaganda errónea, resultando em agitação social e instabilidade política.

Nos últimos dias, este tema foi amplamente abordado na Conferência de Munique, um evento crítico na área da segurança. Nesse âmbito, uma das principais conclusões desta iniciativa de referência mundial, é que os Estados ocidentais, principalmente a Europa, não têm apostado na proatividade da segurança face a estes "novos" riscos, perante contextos distintos, voláteis e mais complexos, que se têm alterado, principalmente, desde o início da invasão russa à Ucrânia.

O que observamos nos últimos tempos, é que ninguém está a salvo. Nem mesmo as infraestruturas críticas (energia, telecomunicações, sistemas de transporte, etc.) dos países ocidentais, já bastante debatidas e cuja segurança exalta preocupações suplementares, tanto para os governos como para os cidadãos.

À medida que a tecnologia continua a avançar, o mesmo acontece com a sofisticação dos atores cibernéticos maliciosos. Estes atores, além de continuarem a explorar vulnerabilidades aplicacionais ou tecnológicas, apostam cada vez mais na interligação das fraquezas do fator humano - engenharia social - no intuito de tornar o ciberataque mais eficaz e de menor tempo de atuação, sempre com vista a obterem acesso ilegítimo a identidades e por aí em diante.

Para mitigar estas ameaças, governos e empresas privadas devem tomar medidas para proteger as suas infraestruturas tecnológicas de suporte à sua atividade digital. Basta pensarmos na percentagem de infraestruturas críticas e/ou setores vitais, em Portugal, que estão nas mãos dos privados.

A forma mais eficaz de proteção é assegurar que todos os sistemas e redes estejam devidamente protegidos. Isto envolve, a adoção de uma consciencialização de cibersegurança ao mais alto nível e a partir daí, o estabelecimento de modelos de governação de segurança que abranja os conceitos tecnológicos, procedimentais e humanos de forma a incrementar a maturidade "circular" de segurança na organização. Além disso, as organizações devem apostar numa cultura de segurança e prevenção interna, assegurando que todos os colaboradores estão cientes dos seus papéis na devida proteção da rede.

Por último, os governos e as empresas privadas devem trabalhar em conjunto para desenvolver uma estratégia abrangente de cibersegurança. Essa estratégia deve incluir tanto medidas defensivas como ofensivas - é preciso conhecer o contexto geopolítico e quem é o inimigo, os seus objetivos e o que está por detrás desse ataque -, bem como medidas para detetar e responder a ameaças cibernéticas.

Os Estados europeus têm-se posicionado como moderadores, no entanto, todos sabemos que os moderadores não ganham debates. A lógica é a mesma no âmbito da cibersegurança. É, portanto, fundamental que governos e empresas trabalhem em conjunto para partilhar informações e recursos, a fim de melhor detetar e responder a ameaças cibernéticas.

Temos de passar a assimilar que, com a evangelização da convivência no mundo cibernético, também as ameaças cibernéticas vieram para ficar. Teremos de aprender a conviver neste novo mundo. O ciberespaço não pode ser visto como antigamente; porque é, atualmente, um campo de interesses, mas, além disso, é também um campo de guerra. Por isso, é tempo de agir e proteger-nos a nós próprios - às nossas sociedades e costumes -, às nossas empresas e às nossas nações dos perigos da cibercriminalidade e do ciberterrorismo.

Fundador e CEO da VisionWare - Sistemas de Informação SA