Ciberterrorismo e ameaças cibernéticas: como defender (o estado de) uma nação?

IT itsecurity.pt/news/blue-team/ciberterrorismo-e-ameacas-ciberneticas-como-defender-o-estado-de-uma-nacao

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, na VisionWare, temos comprovado toda a complexidade e polivalência dos recentes ciberataques, que podem ser utilizados para espalhar informação e propaganda errónea, resultando em agitação social, caos e instabilidade política.

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

À medida que a tecnologia avança, o mesmo acontece com a sofisticação dos atores cibernéticos maliciosos. Estes, para além de continuarem a explorar vulnerabilidades aplicacionais ou tecnológicas, apostam cada vez mais na interligação das fraquezas do fator humano – isto é, na engenharia social – com o intuito de tornar o ciberataque mais eficaz e de menor tempo de atuação, sempre com vista à obtenção de um acesso ilegítimo a identidades, e por aí em diante.

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

Os Estados europeus têm-se posicionado como moderadores, contudo, todos sabemos que os moderadores não ganham debates. A lógica é idêntica no âmbito da cibersegurança. É assim crucial, que governos e empresas trabalhem em conjunto,

para partilhar informações e recursos, a fim de melhor detetar e responder de forma eficaz e preventiva a ameaças cibernéticas.

Temos assistido semanalmente – se não, diariamente - a uma intensificação e sofisticação de ciberataques na sociedade portuguesa. Estes ataques, transversais a quase todos os principais setores da nossa sociedade – telecomunicações, saúde, banca, transportes, educação -, têm causado muita turbulência, visto que, em certos casos, também tem implicado um impacto direto para o core business das 'vítimas', e por inerência, ao próprio setor onde atuam.

O crime cibernético tem sido aquele que mais tem aumentado desde o início da pandemia, tanto ao nível do volume de ataques registados como de denúncias, reforçando que estas situações continuam sem conseguirem ser travadas pelas entidades competentes e, nelas, estão incluídas não só as autoridades que investigam este tipo de ataques, como as próprias empresas que continuam a não dar o devido valor ou investimento a esta área de atuação.

A aposta terá de ser sempre pela via da crescente literacia (em cibersegurança) de todos os cidadãos, independentemente da sua função/cargo, visto que, qualquer um de nós poderá ser vítima de um ataque malicioso ou fraudulento. O fator humano continua a ser um dos grandes responsáveis pela consumação das ameaças e estas tanto podem vir de fora, como dentro da própria organização.

O ciberespaço não pode ser visto como antigamente; hoje, é um campo (e batalha) 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 eminentes da cibercriminalidade e do ciberterrorismo.

Temos de passar a assimilar que, com a evangelização da convivência no mundo cibernético, também as ameaças cibernéticas vieram para ficar e nada será como antes.

Conteúdo co-produzido pela MediaNext e pela VisionWare