Estarão as empresas e as autoridades nacionais preparadas para responder a uma onda de ciberataques (bem-sucedidos)?

itsecurity.pt/news/blue-team/estarao-as-empresas-e-as-autoridades-nacionais-preparadas-para-responder-a-uma-onda-de-ciberataques-bem-sucedidos

Este ciberataque causou uma violenta interrupção de um pilar da nossa sociedade, as comunicações (dado e voz) entre todos nós. Na sequência dos restantes ciberataques ocorridos nos últimos meses, e face ao impacto causado, acrescido de não ter existido qualquer conclusão efetiva da origem, causador e motivação dos mesmos, ficamos com a sensação de que as autoridades estão com dificuldades em concluir com sucesso, os vários processos de investigação.

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.

Face ao incremento quase explosivo do número de ciberataques, as autoridades não dispõem de recursos necessários para responder a todas as solicitações. Para além de mais ataques, e com maior taxa de sucesso, são também cada vez mais complexos e sofisticados, e, portanto, obrigam a um esforço muito superior no processo da sua e investigação. Seguir o rasto da pegada digital deste tipo de grupos criminosos, que atuam de forma encoberta, prolongada no tempo, e tecnicamente aprimorada, é cada vez mais exigente – tecnologicamente, na capacidade de resposta e conhecimento especializado envolvido - para quem tenta investigar e prevenir este tipo de ciberataques. As autoridades competentes estão perante um enorme desafio, que, para além da capacidade de resposta, ainda se prende com o binómio técnico vs. know-how especializado. Eventualmente, poderemos associar grupos cibercriminosos especializados por setor de atividade, como a saúde, indústria, ou a administração pública, onde a sua atuação é cada vez mais personalizada ao setor e com uma maior probabilidade de sucesso e eficácia.

A importância da aposta na literacia digital

Após uma cobertura mediática e crescente awareness a este tema, acabam por ser visíveis alguns resultados e mudanças urgentes de mentalidade, ainda que, insuficientes. Na VisionWare, temos vindo a registar um número avultado de solicitações de empresas, as quais começam agora a preocupar- -se com a questão da segurança da informação e da cibersegurança, colocando-as no topo das suas prioridades de gestão. Finalmente, o chip e o mindset dos administradores das empresas, que detêm o poder de decisão, está a mudar, pelo que as autoridades competentes terão de facto, um gigantesco desafio pela frente, dada a rápida adaptação a uma nova realidade de cibercrimes.

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. Na VisionWare acreditamos que é crucial investir na implementação de um modelo de segurança que seja evolutivo, dinâmico e contínuo, abordando todos setores da segurança, nomeadamente, tecnologia, procedimentos e pessoas. É vital que as organizações conheçam em detalhe o seu nível de risco, e quais as suas fraquezas, para que possam investir corretamente, e caso não seja possível, saibam precisamente onde residem as suas fragilidades, de modo a promover ações imediatas de mitigação. A aposta em ações de sensibilização e formação das pessoas, para que estas estejam conscientes e não se transformem elas próprias em veículos de ameaça face a este novo paradigma de risco cibernético é por isso, urgente.

Conteúdo co-produzido pela MediaNext e pela VisionWare

VisionWare