NIS 2 e a formação na organização:mais do que um cumprimento legal

digitalinside.pt/nis-2-e-a-formacao-na-organizacaomais-do-que-um-cumprimento-legal

Cláudia Gomes

As vantagens são vastas, mas as desvantagens também são uma realidade. No uso massivo de tecnologia, se por um lado, os atacantes veem uma oportunidade de gerar o seu próprio negócio, por outro, as organizações e os cidadãos estão expostos a riscos de ciberataques. Como referem Mohammad Hijji e Gulzar Alam, no seu artigo "*Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees"*, o uso extenso de tecnologia é diretamente proporcional ao aumento do cibercrime.

Contudo, este panorama não é direcionado apenas a organizações e cidadãos, mas igualmente a sociedades e estados. No encalço da crescente necessidade de acompanhamento desta realidade, a regulamentação e legislação no ciberespaço tem estado na agenda da União Europeia. A confirmação disso é a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, ou mais conhecida como SRI 2 ou, ainda, NIS 2, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União Europeia, para entidades essenciais e importantes.

De um conjunto de medidas avançadas, esta diretiva assume em considerando e artigo próprio, a importância da formação em cibersegurança, destacando-se no considerando 89 – "As entidades essenciais e importantes deverão adotar uma vasta gama de práticas básicas de ciber-higiene, (…), organizar formações para o seu pessoal e aumentar a sensibilização para as ciberameaças, a mistificação da interface («phishing») ou as técnicas de engenharia social. (…)."; e no artigo 21.º, n.º 2, alínea g) – "Práticas básicas de ciber-higiene e formação em cibersegurança;".

Na era digital em que vivemos, a formação corporativa em cibersegurança não é apenas uma necessidade de cumprimento legal – ainda que cumpra este critério -, mas um pilar indispensável para a resiliência, mitigação do risco e proteção da informação e sistemas da organização. Mais do que uma mera obrigação, a capacitação contínua dos colaboradores deve ser encarada como uma prática natural e inerente à cultura da própria organização.

No artigo "*Reviewing Cyber Security Social Engineering Training and Awareness Programs — Pitfalls and Ongoing Issues*", de Hussain Aldawood e Geoffrey Skinner, é revelado que a confiança depositada na infraestrutura tecnológica da organização resulta, em alguns casos, nos colaboradores não a considerarem uma responsabilidade também sua.

Sendo a formação um ato bidirecional, não só as organizações devem ter esta prioridade definida, bem como os colaboradores compreenderem a relevância de formação nesta área, seja para proteção dos ativos da organização, seja para a sua vida pessoal.

Se há obrigatoriedade legal para a formação corporativa, os benefícios não se esgotam no cumprimento legal e no evitamento de sanções. Ela potencia elevados padrões de qualidade e segurança, manifestação de vantagem competitiva e confiança junto dos clientes e fornecedores.

A formação expõe os colaboradores a novos cenários, novas ameaças, novas ideias, novas ferramentas, novas estratégias e formas de pensar e abordar o problema, sendo uma mais-valia para colaboradores e organização. Reforçando o conhecimento individual e coletivo, ela eleva a probabilidade da adoção gradual de comportamentos de análise e resposta ajustada e unificada por parte dos intervenientes e favorece o sentido de confiança interna e tomadas de decisão mais informadas.

O cumprimento legal de um plano formativo na organização coloca-a em conformidade legal, mas o valor gerado pelo conhecimento apreendido extravasa o que determina o normativo.

Cláudia Gomes é Digital Learning Developer na VisionWare Academy