devoteam
Cyber Trust

por Alexandra Palma,
Information Security Consultant na Devoteam Cyber Trust

NIS 2: NA VANGUARDA DA CIBERSEGURANÇA

MAIS DO QUE UMA OBRIGAÇÃO, UMA OPORTUNIDADE

AS EMPRESAS ENFRENTAM DESAFIOS DEVIDO AO AUMENTO EXPONENCIAL DE AMEAÇAS CIBERNÉTICAS E AO SURGIMENTO DE LEGISLAÇÃO CADA VEZ MAIS EXIGENTE, COMO É A DIRETIVA NIS 2, QUE DEVE SER ENCARADA COMO UM MOMENTO DE AUMENTO DA MATURIDADE A NÍVEL DE CIBERSEGURANÇA.

Estar em conformidade com a legislação em vigor é uma oportunidade para seguir as melhores práticas, uma vez que é nelas que o legislador encontra a sua inspiração para regular o ecossistema digital.

Portugal, muito em breve, irá transpor para o ordenamento jurídico a NIS 2 o que significa que será através de lei nacional que iremos conhecer a granularidade da Diretiva sendo expectável que o legislador adote uma posição cada vez mais exigente. Enquanto Diretiva, define as regras que os Estados-Membros têm que cumprir sendo clara a adoção de um regime sancionatório bastante penalizador, com coimas a ascender aos 10 milhões de euros ou a 2% do volume de negócios a nível global da empresa, no exercício financeiro anterior, em caso de incumprimento e um aumento de poderes de atuação das autoridades supervisoras competentes, no nosso caso CNCS (Centro Nacional de Cibersegurança).

Estar em conformidade com uma nova Diretiva implica uma avaliação sobre o nosso estado atual, sobre aquilo que temos e aquilo que pretendemos alcançar. Com a


ALEXANDRA PALMA, DEVOTEAM CYBER TRUST

"A NIS 2 É UMA OPORTUNIDADE DE MELHORIA, NÃO SÓ PARA EMPRESAS QUE AINDA NÃO ESTÃO SENSIBILIZADAS PARA AS PRÁTICAS GERAIS DE CIBERSEGURANÇA, MAS TAMBÉM PARA AQUELAS QUE JÁ INICIARAM A SUA JORNADA".

adoção da NIS 2 não será diferente. A resposta às suas exigências pode tornar-se desafiadora na medida em que exige a alocação de recursos tanto a nível de tempo, investimento financeiro e de profissionais especializados. Outro dos desafios expectáveis é a própria resistência à mudança, que a NIS 2 combate através de medidas como promoção da consciencialização e formação e a adoção de medidas sancionatórias cada vez mais pesadas, responsabilizando a Administração da empresa. Perante estes desafios, não é demais reforçar a necessidade de uma abordagem proativa por parte das empresas para que não só atinjam a sua conformidade regulatória, mas aumentem também a sua resiliência contra ameaças cibernéticas.

Para adotar a NIS 2 em empresas com algum tipo de sistema de gestão de segurança implementado é necessária uma abordagem holística, abrangendo tecnologia, pessoas e processos. Possíveis certificações existentes têm um âmbito de aplicabilidade definido, fronteiras que delimitam a sua aplicação. A NIS 2 aplica-se, porém a toda a empresa, de forma transversal, em todas as áreas de negócio que sejam consideradas críticas, e não apenas a um determinado âmbito de aplicabilidade definido em sede de implementações de sistemas de gestão já existentes. Posto isto, deve existir um esforço no sentido de cumprimento com todas as exigências normativas da Diretiva na empresa alinhado com todas as políticas, processos e procedimentos já implementados, sendo que existirão adaptações que são necessárias realizar. A NIS 2 é uma oportunidade de melhoria, não só para empresas que ainda não estão sensibilizadas para as práticas gerais de cibersegurança, mas também para aquelas que já iniciaram a sua jornada.

O surgimento da NIS 2 é uma clara evolução e tudo indica que não ficaremos por aqui. As exigências legais podem correr atrás da permanente atualização tecnológica, mas não se desvirtuam da sua relevância, em particular pela preocupação demonstrada pela harmonia da cadeia de abastecimento, mas acima de tudo pelo carácter preventivo que assume. Devemos antecipar, em uníssono, eventuais disrupções e a promoção de comunicação entre entidades permite prever com maior rapidez e eficácia potenciais ameaças. Ditam as melhores práticas e a sabedoria popular que "a porta deve ser trancada" e que para isso não é frutífero aguardar pela consubstanciação de um determinado incidente. Prevenir é tão importante quanto a capacidade de garantir a reação e recuperação. É sabido que a cibersegurança é uma viagem de longo curso, que se torna menos turbulenta com recurso às ferramentas certas de navegação. ◀