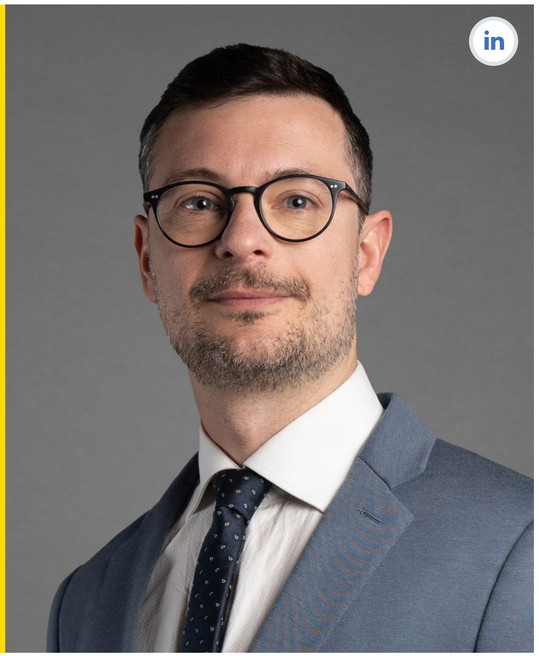

CONSULTOR SÉNIOR
DA ÁREA DE TMT DA
CCA LAW FIRM

POR DR. EDUARDO MAGRANI,
CONSULTOR SÉNIOR DA ÁREA DE TMT DA CCA LAW FIRM

CIBERSEGURANÇA EM PORTUGAL: TENDÊNCIAS E *COMPLIANCE*

SE O CIBERCRIME FOSSE UM ESTADO SERIA A TERCEIRA MAIOR ECONOMIA DO MUNDO, DEPOIS DOS ESTADOS UNIDOS E CHINA, COM UM PIB DE US$ 10 TRILHÕES" AFIRMOU O PRIMEIRO-MINISTRO DA ALBÂNIA, CONSIDERANDO A POTENCIAL FATURAÇÃO DO CIBERCRIME EM 2025.

A verdade é que atualmente a indústria do cibercrime representa uma das mais lucrativas áreas tecnológicas e cresce à medida que organizações criminosas evoluem e profissionalizam o desenvolvimento e distribuição de atividades maliciosas, como ransomware, phishing, roubo de credenciais, entre outros ataques[1].

Com números e impactos significativos, uma das principais preocupações e prioridades da União Europeia (EU) nos últimos anos é justamente a cibersegurança, com um reflexo claro na elaboração de novas estratégias e regulações que têm vindo

a ser aprovadas e discutidas de modo a garantir uma Europa mais segura, mais conectada e mais digital.

A primeira lei da UE sobre cibersegurança, a Diretiva NIS de 2016, ajudou a alcançar um nível comum de segurança de rede e sistemas de informação em todos os Estados-membros. De forma complementar, a Lei de Cibersegurança da UE, em vigor desde 2019, muniu a Europa de uma estrutura de certificação de cibersegurança de produtos, serviços e processos e reforçou o mandato da Agência para a Cibersegurança na UE (ENISA).

Nunca, no entanto, o âmbito de aplicação destas regras foi tão abrangente como o da Diretiva NIS 2 (Diretiva 2022/2555), em vigor desde 2023. Este novo documento revoga a Diretiva NIS (Diretiva 2016/1148/EC) e melhora a gestão de riscos de segurança digital ao introduzir obrigações de relatórios em setores específicos. O seu objetivo principal é a aplicação de medidas que garantam um alto nível de cibersegurança comum em toda a União Europeia[2]. Existe hoje, portanto, uma concertação geral sobre a necessidade de uma aplicação eficaz e medidas efetivas de Cibersegurança em cada um dos países.

Em Portugal, especificamente, o Governo tem vindo a adotar medidas de cibersegurança contra essas ameaças, possuindo, desde 2015, uma estratégia nacional voltada para o cibercrime. Quatro anos mais tarde, em 2019, este sistema foi revisto e alterado, dando origem à atual Estratégia Nacional para a Segurança do Ciberespaço.

Conforme informação do Governo português[3], o cumprimento e aplicação desta estratégia tem como objetivo tornar Portugal um país mais seguro, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade. Deste modo, o Centro Nacional de Cibersegurança está também encarregue de coordenar a elaboração, o acompanhamento da implementação e a revi-

COM NÚMEROS E IMPACTOS SIGNIFICATIVOS, UMA DAS PRINCIPAIS PREOCUPAÇÕES E PRIORIDADES DA UNIÃO EUROPEIA (EU) NOS ÚLTIMOS ANOS É JUSTAMENTE A CIBERSEGURANÇA, COM UM REFLEXO CLARO NA ELABORAÇÃO DE NOVAS ESTRATÉGIAS E REGULAÇÕES QUE TÊM VINDO A SER APROVADAS E DISCUTIDAS DE MODO A GARANTIR UMA EUROPA MAIS SEGURA, MAIS CONECTADA E MAIS DIGITAL.

são do Plano de Ação da Estratégia Nacional para a Segurança do Ciberespaço, em cooperação com todas as entidades responsáveis pela segurança do ciberespaço nacional.

Quanto aos números de incidentes de cibersegurança em Portugal, os episódios recentes demonstram que, mais do que nunca, a segurança digital deve ser vista como um tópico essencial e central, já que é notório o crescimento significativo de crimes tipificados na Lei do Cibercrime (crimes informáticos) e de incidentes com elevado potencial disruptivo, registados pelas autoridades policiais. O número de incidentes registados pelo CERT.PT aumentou 14%, passando de 1781 em , para 2023 em 2022. De entre esses incidentes, ocorreram diversos ciberataques de grande impacto nas infraestruturas e serviços em Portugal[4], sendo os setores mais afetados os da Banca (sobretudo através de phishing aos clientes), a Educação e Ciência, Tecnologia e Ensino Superior, os Transportes e a Saúde.

QUANTO AOS NÚMEROS DE INCIDENTES DE CIBERSEGURANÇA EM PORTUGAL, OS EPISÓDIOS RECENTES DEMONSTRAM QUE, MAIS DO QUE NUNCA, A SEGURANÇA DIGITAL DEVE SER VISTA COMO UM TÓPICO ESSENCIAL E CENTRAL, JÁ QUE É NOTÓRIO O CRESCIMENTO SIGNIFICATIVO DE CRIMES TIPIFICADOS NA LEI DO CIBERCRIME (CRIMES INFORMÁTICOS) E DE INCIDENTES COM ELEVADO POTENCIAL DISRUPTIVO, REGISTADOS PELAS AUTORIDADES POLICIAIS

Conforme informações do CNCS, verificou-se nos últimos meses um aumento na sofisticação e impacto de alguns incidentes. As ciberameaças a afetar o ciberespaço de modo mais contundente foram o ransomware, a cibersabotagem/indisponibilidade, o phishing/smishing/vishing, a burla online, além de incidentes de negação de serviços distribuída (DDoS) e outros ataques.

Muitos dos casos de phishing, smishing e vishing e burla online estão ligados a técnicas de manipulação de indivíduos, o que reflete uma falta de cultura na prevenção destes crimes. Incidentes de comprometimento de contas e tentativa de login, são muitas vezes resultado de palavras-passe comprometidas e de extrações de dados pessoais que poderiam, por vezes, ser contornadas com a implementação de duplo fator de autenticação, entre outras medidas técnicas e organizativas.

As organizações devem, por isso, estar atentas e dispostas a investir nesta área uma vez que precisam de proteger os seus ativos de negócio críticos, gerar confiança e evitar danos financeiros e de reputação,

bem como garantir a conformidade com os regulamentos existentes.

Por esta razão os números de investimento em cibersegurança cresceram 10,7% em Portugal, fixando-se, este ano, nos 300 milhões de euros, demostrando representar uma prioridade para as empresas e organizações, dado o crescente risco e sofisticação dos ataques informáticos.

Uma boa estratégia de cibersegurança deve começar com um mapeamento adequado das regulações existentes como forma de compliance e um programa de gestão de dados e conscientização apropriado para cada negócio. O desenho de um programa de segurança da informação deve atender fundamentalmente a três pilares: Governação, tecnologia e cultura.

O pilar da Governação está ligado às estruturas de liderança e responsabilidade estabelecidas para garantir que as políticas, contratos e práticas de segurança da informação sejam implementadas e corretamente geridas. Já o pilar da tecnologia refere-se ao conjunto de ferramentas e sistemas utilizados para proteger a informação. Por último, o pilar cultural remete-se ao conjunto de valores, crenças e comportamentos que promovem a segurança da informação. Estes pilares desdobram-se em diferentes ações como a identificação e prevenção de riscos, a deteção de incidentes, a resposta e recuperação de ativos, entre outros.

Atualmente, revela-se fundamental para as organizações terem esta governação adequada, com bons indicadores de risco, capacidade de defesa adequada a ataques e gestão de crises, envolvendo as principais áreas da empresa, através de objetivos e estruturas claras, e bem implementadas, de modo a garantir que possuem capacidade para reagir com competência e rapidez aos novos desafios de Cibersegurança, com o compromisso e a expertise adequados. ◀

[1] *https://comunicado.inovativos.com.br/mid_guia_de_seg*
[2] *https://eur-lex.europa.eu/eli/dir/2022/2555*
[3] *https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-de-seguranca-do-ciberespaco/*
[4] *https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs15m.pdf*

UMA BOA ESTRATÉGIA DE CIBERSEGURANÇA DEVE COMEÇAR COM UM MAPEAMENTO ADEQUADO DAS REGULAÇÕES EXISTENTES COMO FORMA DE COMPLIANCE E UM PROGRAMA DE GESTÃO DE DADOS E CONSCIENTIZAÇÃO APROPRIADO PARA CADA NEGÓCIO. O DESENHO DE UM PROGRAMA DE SEGURANÇA DA INFORMAÇÃO DEVE ATENDER FUNDAMENTALMENTE A TRÊS PILARES: GOVERNAÇÃO, TECNOLOGIA E CULTURA.