BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

MARÇO 2021 | nº 1/2021

DESTAQUES

Estratégia

A União Europeia (UE) lançou uma nova Estratégia de Cibersegurança para a Década Digital, no dia 16 de dezembro de 2020, definindo 3 áreas de intervenção: 1) resiliência, soberania tecnológica e liderança; 2) reforço da capacidade operacional para prevenir, dissuadir e reagir; e 3) promoção de um ciberespaço à escala mundial aberto graças a uma maior cooperação.

SRI 2.0

Um dos resultados desta Estratégia é a revisão da Diretiva de Segurança das Redes e Sistemas de Informação (SRI 2.0), com o fim de alargar os setores de atividade e os tipos de organizações abrangidos, promover a gestão do risco das cadeias de fornecimento e reforçar as ações de supervisão e autoridade.

Entidades Críticas

A Estratégia propõe ainda alargar o âmbito de aplicação da diretiva das infraestruturas críticas europeias, de 2008, sujeitando aquelas entidades a estratégias nacionais de resiliência e avaliações regulares de risco.

(Comissão Europeia, Nova Estratégia da UE para a Cibersegurança)

VISUALIZAÇÃO

A Estratégia de Cibersegurança da UE para a Década Digital apresenta algumas iniciativas centrais:

- a criação de um "Cyber Shield" [Ciber-escudo], constituído por uma rede de centros de operações de segurança, e de uma "Joint Cyber Unit" [Unidade Conjunta Ciber], que procurará dar uma resposta mais eficaz às ameaças cibernéticas utilizando os recursos da UE;
- o desenvolvimento de soluções globais de cibersegurança;
- a implementação de elevados padrões de segurança para todos os equipamentos no âmbito da Internet das Coisas;
- e a aplicação de altos níveis de segurança da informação nas instituições europeias.

Esta Estratégia enquadra-se no reforço das preocupações da UE com a cibersegurança, fortalecendo o papel do Grupo de Cooperação da Diretiva SRI e complementando dinâmicas tais como o Cybersecurity Act, que institui um mandato permanente para a Agência Europeia para a Cibersegurança (ENISA), com novas responsabilidades, e estabelece um quadro de certificação da cibersegurança à escala da UE para produtos, serviços e processos digitais; ou a Rede EU-CyCLONe, que serve para apoiar a gestão coordenada de incidentes e crises de cibersegurança em grande escala na UE.

NEW STRATEGIC INITIATIVES:

- An EU-wide **Cyber Shield**
- A **Joint Cyber Unit**
- European solutions for strengthening Internet security globally
- Regulation to ensure **an Internet of Secure Things** and prevent a single badly protected object becoming a single point of failure
- Regulation for **high standards of cyber and information** security in EU institutions, bodies and agencies

(Comissão Europeia, Ficha informativa)

PERSPETIVA

1 O reforço pela UE das estratégias com vista à sua cibersegurança enquadra-se na importância que este tema adquiriu nos últimos anos. Este tipo de iniciativas procura melhorar a cooperação, envolver a sociedade e definir regras vinculativas para os mercados e os agentes sociais e económicos, de modo a reconfigurar o sentido do desenvolvimento digital e da sua adoção social.

2 Este movimento pode ser visto como um contraponto ao aceleramento que caracteriza o desenvolvimento técnico, bem como de outras esferas sociais, tais como as instituições e os ritmos de vida (Rosa, 2015). Deste ponto de vista, este esforço das organizações da UE é um mecanismo institucional de ajuste que visa desacelerar a digitalização em alguns domínios e reorientá-la noutros, tendo em vista a criação de um ciberespaço seguro.

3 A cibersegurança foi esquecida com frequência nos primeiros momentos da invenção das tecnologias digitais e da Internet, mas também nas dinâmicas posteriores de inovação. Hoje, a sua presença é um pilar da digitalização (CE, 2020), aspeto que exige ser recordado e reforçado sempre que se incentiva a transição digital.

4 A melhoria da capacitação e da resiliência europeias em cibersegurança só é possível através da mobilização de vastos setores da sociedade e não apenas daqueles que são definidos como tendo funções de cibersegurança. Este é um dos principais desafios deste mecanismo institucional de ajuste.

5 É possível identificar um conjunto de dificuldades que se pretendem mitigar: a falta de conhecimento situacional estandardizado sobre incidentes e ameaças a nível europeu (ENISA, 2020); a necessidade de articular setores sociais que não têm uma relação orgânica entre si; as dificuldades de coordenação quando é necessário responder a ameaças externas; a transversalidade e a dependência digitais; ou a falta de garantias de segurança de muitos dos produtos digitais.

6 O objetivo último deste processo é a naturalização da cibersegurança na vida das sociedades. Isso obriga ao enraizamento de dinâmicas institucionais (tais como as aqui descritas), mas também à integração da cibersegurança nos referenciais de educação formais e informais, e mesmo na socialização primária.

PUBLICAÇÕES

A Comissão Europeia (com o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança), no dia 16 de dezembro de 2020, lançou a nova Estratégia de Cibersegurança da UE para a Década Digital, renovando as iniciativas europeias neste domínio.

O **Gabinete Cibercrime**, do Ministério Público, no dia 12 de janeiro de 2021, divulgou a Nota Informativa Cibercrime: Denúncias Recebidas 2020, onde analisa o número de denúncias de cibercrime enviadas por correio eletrónico a este organismo, verificando-se um aumento muito significativo entre 2019 e 2020, de 193 para 546 denúncias.

O **World Economic Forum**, no dia 15 de janeiro, publicou mais um Global Risks Report 2021, onde analisa os principais riscos para 2021 com base num inquérito à perceção de risco. A "falha de cibersegurança" é considerada o 9º risco mais provável.

O **Centro Nacional de Cibersegurança**, no dia 18 de janeiro, pulicou os resultados do Inquérito Cibersegurança e Ensino a Distância, realizado em parceria com a Direção-Geral da Educação, aos docentes do ensino não superior, sobre as práticas de cibersegurança durante o primeiro período de confinamento de 2020. Entre outros aspetos, este inquérito mostra como, para os docentes, a dificuldade mais relevante neste âmbito é a carência de meios tecnológicos (37%).

A **APAV** (Associação Portuguesa de Apoio à Vítima), no dia 9 de fevereiro, divulgou as Estatísticas de 2020 da Linha Internet Segura, mostrando um aumento no número processos registados pela sua linha de apoio, de 102 em 2019 para 587 em 2020.

A **OCDE** (Organização para a Cooperação e Desenvolvimento Económico), no dia 9 de fevereiro, publicou a Policy Note com o título Smart policies for smart products: A policy maker's guide to enhancing the digital security of products, onde sumariza os resultados de dois relatórios relevantes: *Understanding the digital security of products: An in-depth analysis e Enhancing the digital security of products: A policy discussion.*

A **OCDE**, no dia 11 de fevereiro, publicou outra Policy Note de destacar, com o título *Encouraging vulnerability treatment: How policy makers can help address digital security vulnerabilities,* orientada a decisores, onde sublinha as vantagens das Políticas Responsáveis de Divulgação de Vulnerabilidades, remetendo ainda para outros dois documentos pertinentes neste domínio: *Encouraging vulnerability treatment: Overview for policy makers* e *Encouraging vulnerability treatment: Background report – Responsible management, handling anddisclosure of vulnerabilities.*

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança