BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

DEZEMBRO 2023 | n.º 5/2023

DESTAQUES

SRI2

A 16 de janeiro de 2023, a Diretiva (UE) 2022/2555 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (vulgo SRI2) entrou em vigor, substituindo a Diretiva (UE) 2016/1148 (SRI1). A nova diretiva tem como principal objetivo melhorar a resiliência e a capacidade de resposta a incidentes no domínio da cibersegurança na União Europeia (UE) (CE, 2020a).

Resultados

A SRI1 estabeleceu o primeiro regime jurídico relativo à cibersegurança na UE, tendo sido crucial na capacitação dos Estados-Membros, através da adoção de estratégias nacionais de cibersegurança e da designação de autoridades nacionais competentes neste domínio, assim como para a ciber-resiliência de serviços essenciais, com o estabelecimento de requisitos de segurança e de notificação de incidentes (CE, 2020a).

Desafios

A implementação da SRI1 trouxe novos desafios. A heterogeneidade na sua adoção levou a que vários tipos de organizações relevantes tenham ficado fora do seu âmbito de aplicação. Igualmente, as diferenças ao nível dos requisitos mínimos de segurança e dos poderes/recursos atribuídos às autoridades competentes, assim como falhas na partilha de informação, ameaçaram o nível comum de cibersegurança na UE (CE, 2020b).

PANORÂMICA

- No âmbito da SRI1, os colegisladores europeus delegaram a identificação dos operadores de serviços essenciais (OSE) aos Estados-Membros. Além desta flexibilidade, os Estados-Membros elaboraram diferentes metodologias para identificar OSE, o que gerou inconsistências tanto quantitativas como qualitativas (CE, 2019).
- Por exemplo, enquanto alguns Estados-Membros incluíram quase todos os seus hospitais no âmbito de aplicação da sua transposição da SRI1, outros deixaram a maioria de fora (CE, 2020a).
- Igualmente, note-se que o número de OSE identificados pelos Estados-Membros varia bastante. Em 2019, mostrava-se que os números disponíveis não estavam fortemente correlacionados com a dimensão dos Estados-Membros (CE, 2019).

Outros setores incluídos na transposição da diretiva SRI1 em 17 Estados-Membros (fonte: CE, 2019)

- Para além de inconsistências ao nível da identificação de OSE previstos na SRI1, 11 dos 28 Estados-Membros (ainda inclui Reino Unido) identificaram serviços essenciais em setores não abrangidos pela SRI1. A destacar a inclusão de domínios agora abrangidos pela SRI2, tais como a Administração Pública (caso de Portugal), e setores como as águas residuais, a produção alimentar, as infraestruturas de informação ou logística e os serviços postais.

PERSPETIVA

1 A diretiva SRI2 é composta por 46 artigos, distribuídos por 9 capítulos, a que acrescem 3 anexos. As principais mudanças trazidas pela nova diretiva abordam os seguintes aspetos: i) o alargamento do âmbito de aplicação; ii) o reforço dos quadros coordenados em matéria de cibersegurança; iii) a consolidação da cooperação internacional e na UE; iv) a intensificação das abordagens de gestão do risco e notificação de incidentes; e v) a expansão da supervisão.

2 A SRI2 é aplicada a entidades públicas ou privadas de média ou grande dimensão que operem em setores de importância crítica (anexo I) ou outros setores críticos (anexo II) (art. 2.º/1 SRI2)*. Independentemente da sua dimensão, a SRI2 aplica-se também a entidades presentes nos anexos e que prestem certos serviços digitais, sejam os prestadores únicos de serviços essenciais, prestem serviços cuja perturbação impacte a segurança pública ou possam gerar riscos sistémicos, determinadas entidades pertencentes à administração pública ou entidades críticas (art. 2.º/2).

3 Mantém-se a adoção obrigatória de estratégias nacionais de cibersegurança, contudo os colegisladores clarificaram e alargaram os requisitos materiais das mesmas (art. 7.º SRI2). Os Estados-Membros passam também a designar autoridades para a gestão de cibercrises (art. 9.º). A SRI2 prevê ainda a criação de uma base de dados europeia de vulnerabilidades, cabendo a intermediação na divulgação coordenada de vulnerabilidades às CSIRTs nacionais (art. 12.º).

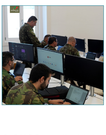
4 Mantém-se o grupo de cooperação SRI e a rede europeia de CSIRTs, embora com algumas atualizações relativas ao seu âmbito de atividade (arts. 14.º e 15.º SRI2). A SRI2 reforça os esforços de cooperação com a formalização da Rede Europeia de Organizações de Coordenação de Cibercrises (*UE-CyCLONe*), um fórum dedicado à "gestão coordenada de crises e incidentes de cibersegurança em grande escala" (art. 16.º/1).

5 Enquanto a SRI1 deixou aos Estados-Membros a definição das medidas de gestão de risco, a SRI2 estabelece uma série de medidas de gestão de risco mínimas tais como a elaboração de políticas de análise dos riscos, adoção da autenticação multifator ou formação em ciber-higiene (art. 21.º SRI2). À obrigação de notificação de incidentes (art. 23.º/1 SRI2), acrescenta-se a obrigação de notificação de cibera meaças (ibid. n.º 2), assim como prazos máximos para o cumprimento destas (ibid. n.º 4).

6 Expandem-se os poderes de supervisão das autoridades competentes, passando a incluir medidas tais como inspeções no local, supervisão remota através de controlos aleatórios ou auditorias *ad hoc* (art. 32.º/2 SRI2). Do mesmo modo, ao lado de um aumento do montante máximo das coimas (art. 34.º SRI2), amplia-se o arsenal de medidas de execução à disposição das entidades competentes (art. 32.º/4 e a 33.º/4 SRI2).

* Excetuando as situações em que existam outros atos jurídicos da União setoriais que estabeleçam medidas de gestão dos riscos de cibersegurança e de obrigações de notificação pelo menos equivalentes às que são exigidas pela SRI2.

PUBLICAÇÕES E NOTÍCIAS



O **Exército Português**, entre os dias 6 e 10 de novembro, realizou o exercício de cibersegurança *CIBER PERSEU 23* destinado a treinar e avaliar os procedimentos e a capacidade técnica do Exército na resposta a incidentes na sequência de ciberataques de âmbito nacional ou internacional, incidindo sobre infraestruturas críticas para a condução de operações militares.

O **CNCS**, no dia 14 de novembro, lançou mais um episódio do *podcast Comunicar Cibersegurança*, desta feita sobre o tema "desinformação" e com a convidada Inês Narciso, investigadora do ISCTE-IUL. Neste sexto episódio, abordam-se várias questões na interseção entre a desinformação e a cibersegurança, tais como o papel das novas tecnologias digitais, como a inteligência artificial, na produção de desinformação.

A **ENISA – Agência da UE para a Cibersegurança**, no dia 16 de novembro, publicou a quarta edição do relatório *NIS Investments* relativo ao ano de 2023, no qual analisa os investimentos feitos no domínio da cibersegurança por parte de 1080 operadores de serviços essenciais e prestadores de serviços digitais identificados no âmbito da diretiva SRI1. Entre outros resultados, a análise revelou um aumento médio de 0.4% em investimentos no domínio da cibersegurança relativamente ao ano anterior, ainda que apenas 7.1% do orçamento para tecnologias de informação tenha sido dedicado a investimentos em cibersegurança.

A **ENISA**, o **Parlamento Europeu** e a **Comissão Europeia** promoveram, no dia 21 de novembro, o exercício de cibersegurança *EU ELEx23: Towards cyber-secure European Parliament elections* para avaliar a eficácia dos planos de gestão de crises e resposta a incidentes relacionados com as próximas eleições para o Parlamento Europeu a junho de 2024. O CNCS, através do CERT.PT, e a Secretaria Geral do Ministério da Administração Interna participaram neste exercício.

O **Governo Regional dos Açores** e o **CNCS**, no dia 29 de novembro, realizaram a conferência *C-DAYS AÇORES 2023* na Ilha Terceira, Açores, com o tema "Mais Confiança". Esta iniciativa representou uma oportunidade para discutir a cibersegurança, partilhando assim a visão de algumas das entidades com mais experiência na matéria. Assista ao vídeo aqui.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança