COMISSÃO
EUROPEIA

Bruxelas, 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Tirar o maior partido da SIR – Para uma execução efetiva da Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

PT

Introdução

A Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União[1] (a seguir designada «Diretiva SRI» ou a «diretiva»), adotada em 6 de julho de 2016, é o primeiro ato legislativo horizontal da UE que aborda os desafios em matéria de cibersegurança e constitui um ponto de viragem no que respeita às capacidades de resistência e cooperação da Europa em matéria de cibersegurança.

A diretiva tem três objetivos principais:

- Melhorar as capacidades nacionais em matéria de cibersegurança;
- Reforçar a cooperação a nível da UE; e
- Promover uma cultura de gestão dos riscos e comunicação de incidentes entre os principais agentes económicos, nomeadamente os operadores de serviços essenciais para a manutenção de atividades económicas e sociais e os prestadores de serviços digitais.

A Diretiva SRI é uma das pedras angulares da resposta da UE às crescentes ciberameaças e desafios que acompanham a digitalização da nossa vida económica e social, pelo que a sua transposição é uma parte fundamental do pacote de cibersegurança apresentado em 13 de setembro de 2017. A eficácia da resposta da UE será prejudicada enquanto a Diretiva SRI não for integralmente transposta em todos os Estados-Membros. Este aspeto foi também considerado um ponto crítico na comunicação da Comissão «Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora», de 2016[2].

O caráter inovador da Diretiva SRI e a necessidade urgente de fazer face à rápida evolução das ciberameaças justificam que se dê uma atenção especial aos desafios que todos os intervenientes enfrentam para garantir a transposição atempada e bem-sucedida da diretiva. Tendo em conta o prazo para a transposição da diretiva, 9 de maio de 2018, e o prazo para a identificação dos operadores de serviços essenciais, 9 de novembro de 2018, a Comissão tem vindo a apoiar o processo da transposição dos Estados-Membros, bem como o seu trabalho no âmbito do grupo de cooperação.

A presente comunicação, assim como o seu anexo, baseia-se na análise e nos trabalhos preparatórios da Comissão relacionados com a execução da diretiva até ao momento, no contributo da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e nos debates realizados com os Estados-Membros na fase de transposição da

[1] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. A diretiva entrou em vigor em 8 de agosto de 2016.
[2] COM(2016) 410 final.

diretiva, nomeadamente no âmbito do grupo de cooperação[3]. Esta comunicação complementa os esforços consideráveis desenvolvidos até ao momento, em especial mediante:

- O trabalho intensivo do grupo de cooperação, que acordou um plano de trabalho que incide principalmente na transposição da Diretiva SRI e, em especial, na questão da identificação de operadores de serviços essenciais e nas suas obrigações no que se refere aos requisitos de segurança e à notificação de incidentes. Embora a diretiva preveja alguma margem de apreciação para a transposição de disposições relacionadas com os operadores de serviços essenciais, os Estados-Membros reconheceram a importância de prever uma abordagem harmonizada e este respeito[4].
- A criação e o funcionamento célere da rede composta pelas equipas de resposta a incidentes de segurança informática (CSIRT), em conformidade com o artigo 12.º, n.º 1, da diretiva. Desde então, a referida rede tem vindo a estabelecer as bases para uma cooperação operacional estruturada a nível da UE.

Tanto em relação ao nível político como ao nível operacional representados por estas duas estruturas, é essencial o compromisso total de todos os Estados-Membros para atingir o objetivo de assegurar um elevado nível comum de segurança das redes e sistemas de informação em toda a União.

A presente comunicação, juntamente com o seu anexo, reforçará estes esforços, reunindo e comparando boas práticas dos Estados-Membros que são pertinentes para a transposição da diretiva, fornecendo orientações suplementares sobre como a diretiva deve ser executada e por intermédio de explicações mais pormenorizadas sobre disposições específicas. O objetivo global da comunicação consiste em ajudar os Estados-Membros a alcançarem uma execução eficaz e harmonizada da Diretiva SRI em toda a UE.

A presente comunicação será ainda complementada pelo futuro regulamento de execução da Comissão, que especifica mais pormenorizadamente os elementos e parâmetros relativos aos requisitos de segurança e de notificação de incidentes aplicáveis aos prestadores de serviços digitais, nos termos do artigo 16.º, n.º 8, da Diretiva SRI. O regulamento de execução facilitará a execução da diretiva no que diz respeito às obrigações relativas aos prestadores de serviços digitais[5].

A comunicação apresenta as principais conclusões da análise das questões consideradas como importantes pontos de referência e eventual inspiração na perspetiva da transposição para o

[3] Trata-se de um mecanismo de cooperação estratégica entre os Estados-Membros criado ao abrigo do artigo 11.º da Diretiva SRI.

[4] O grupo de cooperação está atualmente a elaborar documentos de orientação de referência, nomeadamente sobre: os critérios que definem o caráter crucial de um operador, nos termos do artigo 5.º, n.º 2, da diretiva; as circunstâncias em que os operadores de serviços essenciais são obrigados a notificar incidentes com base no artigo 14.º, n.º 7, da diretiva; os requisitos de segurança aplicáveis aos operadores de serviços essenciais, em conformidade com o artigo 14.º, n.[os] 1 e 2.

[5] O projeto de regulamento de execução está disponível para consulta pública em: https://ec.europa.eu/info/law/better-regulation/have-your-say_en.

direito nacional. O seu texto incide principalmente em disposições relacionadas com as capacidades e as obrigações dos Estados-Membros relativamente às entidades abrangidas pelo âmbito de aplicação da diretiva. O anexo apresenta um exame mais pormenorizado dos domínios em relação aos quais a Comissão considera ser do maior interesse fornecer orientações práticas em matéria de transposição, mediante a explicação e a interpretação de algumas das disposições da diretiva, bem como da apresentação de boas práticas e da experiência adquirida com a diretiva até ao momento.

Para uma aplicação eficaz da Diretiva SRI

A Diretiva SRI tem como objetivo garantir um elevado nível comum de segurança das redes e da informação em toda a União. Tal implica melhorar a segurança da Internet e das redes e sistemas de informação privados em que assenta o funcionamento da nossa sociedade e economia. O primeiro elemento importante a este respeito é o grau de preparação dos Estados-Membros, que deverá ser assegurado pela existência de estratégias nacionais de cibersegurança, tal como descrito na diretiva, pelo trabalho realizado pelas CSIRT, bem como pelo das autoridades nacionais competentes.

Abrangência das estratégias nacionais

É importante que os Estados-Membros aproveitem a oportunidade oferecida pela transposição da Diretiva SRI para reverem as respetivas estratégias nacionais de cibersegurança, tendo em conta as insuficiências, as boas práticas e os novos desafios abordados no anexo.

Embora, como é compreensível, a diretiva incida sobre as empresas e os serviços que se revestem da maior importância, é a cibersegurança da economia e da sociedade, no seu conjunto, que importa abordar de uma forma holística e coerente, atendendo à sua crescente dependência das TIC. Por conseguinte, a adoção de estratégias nacionais abrangentes, que superem os requisitos mínimos da Diretiva SRI (por exemplo, cobrindo mais setores e serviços do que os enumerados, respetivamente, nos anexos II e III da diretiva), aumentará o nível global de segurança das redes e dos sistemas de informação.

A cibersegurança continua a ser um domínio relativamente recente e em rápida expansão da política pública, pelo que, na maior parte dos casos, são necessários novos investimentos, mesmo se a situação global das finanças públicas exigir cortes e poupanças. Por conseguinte, é fundamental tomar decisões ambiciosas que garantam recursos financeiros e humanos adequados, indispensáveis para a eficácia da execução das estratégias nacionais, incluindo a disponibilidade de recursos suficientes para as autoridades nacionais competentes e para as CSIRT, a fim de concretizar os objetivos da Diretiva.

Eficácia da aplicação e execução

A necessidade de designar as respetivas autoridades nacionais competentes e pontos de contacto únicos, referida no artigo 8.º da diretiva, constitui um elemento fundamental para assegurar uma aplicação eficaz da Diretiva SRI, bem como a cooperação transfronteiriça. Neste caso, surgiram nos Estados-Membros abordagens de caráter mais centralizado ou

descentralizado. Nos casos em que os Estados-Membros adotam uma abordagem mais descentralizada em relação à designação das autoridades nacionais competentes, revelou-se ser essencial assegurar acordos de cooperação sólidos entre várias autoridades e o ponto de contacto único (*ver quadro 1 do ponto 3.2 do anexo*). Esta solução deverá aumentar a eficácia da aplicação, assim como facilitar a execução.

Recorrer a experiências anteriores em relação à proteção de infraestruturas críticas da informação poderá ajudar os Estados-Membros a conceberem um modelo ideal de governação, assegurando não apenas uma aplicação setorial eficaz da Diretiva SRI, mas também uma abordagem horizontal coerente (*ver ponto 3.1 do anexo*).

Reforço das capacidades das CSIRT nacionais

Caso não disponha de CSIRT nacionais eficazes e providas de recursos adequados em toda a UE, como previsto no artigo 9.º da Diretiva SRI, a União permanecerá demasiado vulnerável a ciberameaças transfronteiriças. Por conseguinte, os Estados-Membros poderão considerar alargar o âmbito de aplicação das CSIRT para lá dos setores e serviços que constam do âmbito de aplicação da diretiva (ver ponto *3.3 do anexo*). Tal permitirá que as CSIRT nacionais prestem apoio operacional em caso de incidentes de cibersegurança que ocorram em empresas e organizações que não são abrangidas pelo âmbito de aplicação da diretiva, mas que são também importantes para a sociedade e para a economia. Além disso, os Estados-Membros poderão aproveitar plenamente as oportunidades de financiamento adicionais oferecidas pelo programa de infraestruturas de serviços digitais (ISD) em matéria de cibersegurança, no âmbito do Mecanismo Interligar a Europa (MIE), destinado a reforçar as capacidades das CSIRT nacionais e a cooperação entre as mesmas *(ver ponto 3.5 do anexo*).

Coerência do processo de identificação dos operadores de serviços especiais

Em conformidade com o artigo 5.º da Diretiva SRI, os Estados-Membros são obrigados a identificar, até 9 de novembro de 2018, entidades que serão consideradas operadores de serviços essenciais. Em relação a esta tarefa, os Estados-Membros poderão considerar a possibilidade de utilizar, de forma coerente, as definições e as orientações que constam da presente comunicação, a fim de assegurar que as entidades do mesmo tipo que desempenham funções semelhantes no mercado interno serão sempre identificadas como operadores de serviços essenciais nos demais Estados-Membros. Os Estados-Membros poderão também ponderar o alargamento do âmbito de aplicação da Diretiva SRI às administrações públicas, atendendo ao papel que estas desempenham na sociedade e na economia em geral (*ver pontos 2.1 e 4.1.3 do anexo*).

Seria muito útil alinhar tanto quanto possível as abordagens nacionais à identificação de operadores de serviços essenciais, nomeadamente de acordo com as orientações desenvolvidas pelo grupo de cooperação (*ver ponto 4.1.2 do anexo),* uma vez que isso contribuiria para uma aplicação mais harmonizada das disposições da diretiva, reduzindo

dessa forma os riscos de fragmentação do mercado. Nos casos em que os operadores de serviços essenciais prestam serviços essenciais em dois ou mais Estados-Membros, é fundamental procurar alcançar um acordo entre Estados-Membros, no âmbito do processo de consulta previsto no artigo 5.º, n.º 4, sobre a coerência do processo de identificação dos operadores (*ver ponto 4.1.7 do anexo*), uma vez que isso evitaria um tratamento regulamentar diferenciado da mesma entidade ao abrigo de jurisdições de diferentes Estados-Membros.

Apresentação de informações à Comissão sobre a identificação de operadores de serviços essenciais

Em conformidade com o artigo 5.º, n.º 7, os Estados-Membros são obrigados a fornecer informações à Comissão sobre as medidas nacionais que permitem identificar os operadores de serviços essenciais, a lista dos serviços essenciais, o número de operadores de serviços essenciais identificados e a importância desses operadores para o setor. Além disso, os Estados-Membros são obrigados a fornecer os limiares, caso existam, utilizados no processo de identificação para determinar o nível de oferta relevante ou a importância de um operador em particular para a manutenção de um nível suficiente de oferta. Os Estados-Membros poderão considerar a possibilidade de partilhar com a Comissão as listas de operadores de serviços essenciais, se necessário, a título confidencial, uma vez que isso contribuirá para melhorar a precisão e a qualidade da avaliação da Comissão (*ver pontos 4.1.5 e 4.1.6 do anexo*).

Harmonização das abordagens relativas aos requisitos de segurança e de notificação de incidentes aplicáveis aos operadores de serviços essenciais

No que respeita às obrigações relativas aos requisitos de segurança e de notificação de incidentes aplicáveis aos operadores de serviços essenciais (artigo 14.º, n.^{os} 1, 2, e 3), a adoção de uma abordagem harmonizada, no sentido de facilitar a conformidade dos operadores de serviços essenciais entre as fronteiras dos Estados-Membros da UE, contribuirá para criar, tanto quanto possível, um efeito de mercado único. Neste caso, a referência continua a ser o trabalho desenvolvido no âmbito do grupo de cooperação relativo à elaboração de um documento de orientação (*ver pontos 4.2 e 4.3 do anexo).*

No caso de ocorrer um incidente de cibersegurança em grande escala, que afete vários Estados-Membros, é muito provável que seja apresentada uma notificação obrigatória do incidente, por parte de um operador de serviços essenciais ou de um prestador de serviços digitais, nos termos do artigo 14.º, n.º 3, e do artigo 16.º, n.º 3, ou por outra entidade não abrangida pelo âmbito de aplicação da diretiva, a título voluntário, nos termos do artigo 20.º, n.º 1. Em conformidade com a recomendação da Comissão sobre a resposta coordenada a incidentes em grande escala e crises de cibersegurança, os Estados-Membros poderão considerar a possibilidade de harmonizar a respetivas abordagens nacionais, de modo a poderem prestar informações relevantes, com a maior brevidade possível, baseadas nessas notificações às autoridades competentes ou às CSIRT dos outros Estados-Membros afetados. A divulgação de informações práticas exatas será crucial para reduzir o número de infeções ou para dar resposta a vulnerabilidades antes que estas sejam exploradas.

No espírito de parceria para beneficiar o mais possível do disposto na Diretiva SRI, a Comissão pretende alargar o apoio concedido ao abrigo do Mecanismo Interligar a Europa a todas as partes interessadas pertinentes abrangidas pela diretiva. Apesar de os esforços se terem concentrado no reforço das capacidades das CSIRT e numa plataforma que permita uma cooperação operacional rápida e eficaz, reforçando assim a rede de CSRIT, a Comissão analisará agora como pode o Mecanismo Interligar a Europa beneficiar igualmente as autoridades nacionais competentes, bem como os operadores de serviços essenciais e os prestadores de serviços digitais.

Conclusão

Tendo em conta o prazo imperativo para a transposição da Diretiva SRI para a legislação nacional, até 9 de maio de 2018, e atendendo ao prazo para a identificação de operadores de serviços essenciais, até 9 de novembro de 2018, os Estados-Membros devem adotar medidas adequadas para assegurarem que as disposições e os modelos de cooperação da Diretiva SRI podem proporcionar os melhores instrumentos possíveis a nível da UE para atingir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. A Comissão convida os Estados-Membros a tomarem em consideração, no âmbito deste processo, as informações pertinentes, as orientações e as recomendações que constam da presente comunicação.

A presente comunicação pode ainda ser complementada com outras ações, nomeadamente as que surgirem em resultado do trabalho em curso no âmbito do grupo de cooperação.