Diretiva NIS 2[1]

Elevando os níveis de cibersegurança e resiliência nas organizações da União Europeia

Francisco Pereira, n.º 99814
Nelson Jesus, n.º 94789
Roberto Medina, n.º 120531

[1] acrónimo de Network and Information Security 2, publicada no Jornal Oficial da União Europeia (UE), sob a designação de Diretiva (UE) 2022/2555

NIS2 Directive

Introdução

A Diretiva NIS 2

Baseada na Diretiva (UE) 2016/1148, Cibersegurança das redes e dos sistemas de informação, a diretiva NIS2 visa o seguinte:

- Estabelecer regras mínimas para um quadro regulamentar eficaz
- Definir mecanismos para uma cooperação eficaz entre as autoridades competentes de cada Estado-Membro
- Atualizar a lista de setores e atividades sujeitos a obrigações em matéria de cibersegurança

Objetivos da NIS2

Conjunto de regras mínimas para um quadro regulamentar eficaz implementa

- Existência de uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT[2])
- Existência de uma autoridade nacional competente em matéria de redes e sistemas de informação (NIS[3])
- Uma cultura de segurança transversal a todos os operadores vitais para a sociedade e economia que dependem fortemente das TIC

[2] Computer Security Incident Response Team
[3] Network and information systems

Objetivos da NIS2

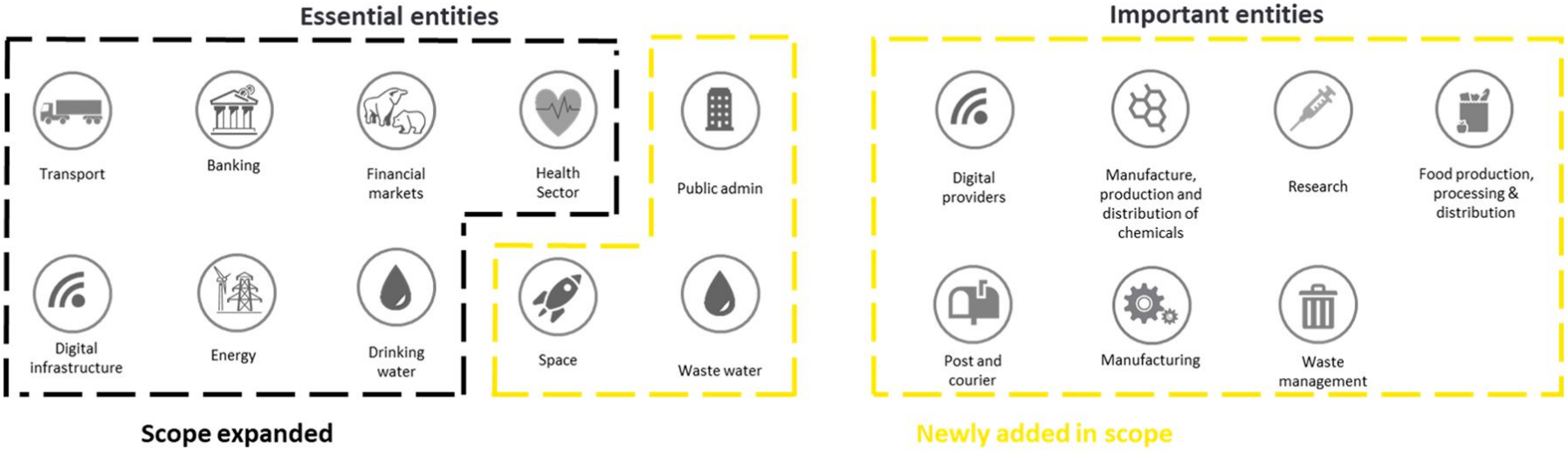
O mecanismo de cooperação passa pela criação de um grupo de trabalho composto por:

- Representantes dos Estados-Membros
- A Comissão
- ENISA[4] - European Union Agency for Cybersecurity (com papel reforçado e mandato permanente)
- European External Action[5] (como observador)
- Entidades de Supervisão Europeias (sob as condições do n.º 1 do artigo 47, do Regulamento (UE) 2022/2554[6])

[4] https://www.enisa.europa.eu/
[5] https://www.eeas.europa.eu/_en
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

Objetivos da NIS2

Lista de setores e atividades sujeitos a obrigações em matéria de cibersegurança:



fonte: https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive

Âmbito da NIS 2

De acordo com o Artigo 2.º da diretiva, esta é aplicada tanto a entidades públicas como privadas que se enquadrem no seguinte:

- Micro empresa que exceda os limites regulamentados para volume de negócios
- Média empresa que exerça a sua atividade ou serviços na União Europeia

Micro empresa[7]

1. **Emprega** 11 - 50 pessoas.
2. **Volume anual de negócios** ou **balanço total anual** não excede 10 milhões de euros.

Média empresa

1. **Emprega** 51 - 250 pessoas.
2. **Volume anual de negócios** não excede 50 milhões de euros.
   Ou
3. **Balanço total anual** não excede 43 milhões de euros.

[7] https://portugal2020.pt/glossario/pme-pequenas-e-medias-empresas/

Linha temporal legislativa da NIS2

2020.12.16	2021.04.27 a 22.04.11	2020.12.17 a 2022.11.10	2022.12.14	2022.12.27
Comissão Europeia	**Banco Central Europeu** **Autoridade Europeia para a Proteção de Dados** **Comité Económico e Social**	**Conselho da UE** **Parlamento Europeu**	**Parlamento Europeu & Conselho da UE**	**Publicação no Jornal Oficial**
Adoção pela Comissão (CELEX[8]: 52020PC0823)	Parecer do Banco Central Europeu (CELEX: 52022AB0014) Parecer da Autoridade Europeia para a Proteção de Dados (CELEX: 52022AB0014) Parecer do CESE (CELEX: 52020AE5749)	Discussões no Conselho da UE (de 2020.12.17 a 2022.11.22) Aprovação pelo Conselho da UE em 1.ª leitura (2022.11.28) Posição do Parlamento Europeu em 1.ª leitura (2022.11.10)	Assinatura pelo presidente do Parlamento Europeu e pelo presidente do Conselho da UE	Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.o 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2)(CELEX: 32022L2555)

[8] CELEX é o identificador único de cada documento no EUR-Lex (portal de acesso à legislação europeia

Requisitos de Conformidade

Estão plasmados no n.º 2 do artigo 21.º, da Diretiva NIS2 (**Medidas de gestão dos riscos de cibersegurança**):

- Políticas de análise dos riscos e de segurança dos sistemas de informação
- Continuidade de atividades como a gestão de cópias de segurança
- Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos
- Práticas básicas de ciberhigiene e formação em cibersegurança
- Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo o tratamento e a divulgação de vulnerabilidades
- Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem
- Utilização de soluções de autenticação multifatores ou de autenticação contínua, comunicações seguras de voz, vídeo e texto e sistemas seguros de comunicações de emergência no seio da entidade, caso seja necessário

Resposta a Incidentes

Foi desenhada uma nova cronologia de reporte de incidentes com impacto significativo:

- No prazo de 24 horas, deve ser emitido um aviso prévio de alerta ao CSIRT.
- Após 72 horas, terá que ser emitida uma comunicação completa.
- Após um mês o relatório completo deverá ser comunicado.

Sanções e Execução

- As penalizações por não conformidades podem atingir até 10% do volume de negócios anual da entidade.
- As entidades pertencentes aos setores críticos poderão ter multas até ao valor de €10 000 000 ou pelo menos 2% do volume de negócios anual (global) da entidade – será aplicado o valor mais elevado.
- Para as entidades pertencentes a outros setores críticos as multas serão até ao valor de €7 000 000 ou pelo menos 1,4% do volume de negócios anual (global) da entidade – será aplicado o valor mais elevado.

Benefícios da NIS2

- Maior colaboração entre os estados membros.
- Investimento na proteção de sistemas de informação.
- Aumento da eficiência através da simplificação de processos, melhoria de desempenho...
- Aplicar outras normas, regulamentos ou padrões que exijam cibersegurança (RGPD[9], ISO 27001[10]...).

[9] Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho)
[10] ISO 27001, é o padrão e a referência Internacional para a gestão da Segurança da informação.

Desafios

Partilhando da opinião de Nuno Teodoro[11], os principais desafios que se colocam são:

- Supervisão da correta implementação dos requisitos da diretiva.
- Aplicação do quadro sancionatório em caso de falha grave.

[11] https://www.linkedin.com/pulse/ser%C3%A1-nis2-grande-arma-da-europa-que-respeita-%C3%A0-nuno/?originalSubdomain=pt

Case Study

Applied Risk

Uma empresa multinacional de grandes dimensões do setor de petróleo e gás alcançou a conformidade com a Diretiva NIS2 em três países.

Seguiu um conjunto de diretrizes para apoiar a preparação das auditorias e impulsionar melhorias eficazes na sua segurança de OT.

Os requisitos da Diretiva NIS2 da UE foram integrados nos processos diários e no modelo de gestão da empresa.

Os insights obtidos contribuem para a redução do risco de paralisações inesperadas e perda de produção.

Conclusão

«A cibersegurança é um processo e não um produto»

Bruce Schneiner

Embora a legislação agora aprovada ser exigente, abrangente e, com isso, mais resiliente, não é fechada a futuras melhorias.
A cibersegurança é cenário de grande incerteza e diversidade. Por esse motivo, além das revisões periódicas necessárias, em 17 de outubro de 2027 será apresentado ao Parlamento Europeu e ao Conselho um relatório sobre esta matéria.

Bibliografia

Processo 2020/0359/COD - COM (2020) 823: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Retrieved 2023.10.05, from https://eur-lex.europa.eu/legal-content/en/HIS/?uri=CELEX:32022L2555

32016L1148 - EN - EUR-Lex (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).Retrieved 2023.10.08, from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

32022L2555 - EN - EUR-Lex (Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.o 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (Texto relevante para efeitos do EEE). Retrieved 2023.10.08, from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32022L2555

Regulation (EU) 2022/2554 of the European Parliament and of the Council. Retrieved 2023.10.08, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

Ajuda - EUR-Lex. Retrieved 2023.10.05, from https://eur-lex.europa.eu/content/help.html

Cybersecurity: how the EU tackles cyber threats - Consilium. Retrieved 2023.10.08, from https://www.consilium.europa.eu/en/policies/cybersecurity/

Centro Nacional de Cibersegurança. Retrieved 2023.10.08, from https://www.cncs.gov.pt

Rede Nacional CSIRT. Retrieved 2023.10.08, from https://www.redecsirt.pt/

Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (Diretiva SRI2) — Perguntas frequentes | Shaping Europe's digital future. Retrievef 2023.10.08, from https://digital-strategy.ec.europa.eu/pt/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Cibersegurança das redes e dos sistemas de informação. Retrieved 2023.10.08, from https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:4314915#keyterm_E0002

NIS 2 Directive. Retrieved 2023.10.08, from https://www.nis-2-directive.com/

PME Pequenas e Médias Empresas - PT2020. Retrieved 2023.10.08, from https://portugal2020.pt/glossario/pme-pequenas-e-medias-empresas/

How to prepare for the NIS2 Directive? Retrieved 2023.10.08, from https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive

STAND UP FOR DEMOCRACY / SPEAK UP FOR EUROPE | European Economic and Social Committee. Retrieved 2023.10.08, from https://www.eesc.europa.eu/en/about/political-organisation/eesc-president/priorities/manifesto

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Retrieved 2023.10.08, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

ISO 27001. Retrieved 2023.10.08, from https://www.27001.pt/

O que é NIS2? | Conformidade e Políticas | Akamai. Retrieved 2023.10.08, from https://www.akamai.com/pt/glossary/what-is-nis2

Case Study. Retrieved 2023.10.18, from https://applied-risk.com/assets/uploads/documents/EU-NIS-Directive-for-Oil-and-Gas-Case-Study.pdf

Obrigado pela atenção