The Critical Entities Resilience Directive (CER)

Strengthening Resilience

VON: JESPER FLORIN

Die CER-Richtlinie soll die Resilienz kritischer Infrastruktur stärken (Foto: Andreas64/ pixabay)

In response to the increasing threats posed by hybrid attacks, natural disasters, terrorist threats, and public health crises, the European Union has introduced the Critical Entities Resilience Directive (CER). This directive, which came into force in early 2023, aims to enhance the resilience of critical infrastructure across various sectors, ensuring the continuity of essential services and protecting societal functions.

Background and Objectives

The CER Directive, officially known as Directive (EU) 2022/2557, was adopted to replace the previous Directive 2008/114/EC, which focused primarily on the energy and transport sectors. The new directive expands its scope to include at least eleven sectors, addressing both digital and physical threats. The primary goal is to establish uniform minimum obligations for critical entities and ensure their implementation through coherent support and supervision measures.

National Strategies

Each Member state must on the background of the directive develop national strategies to identify critical entities, enhance their resilience, and conduct risk assessments at least every four years. These strategies should align with the overarching goals of the CER Directive.

Entities identified as critical under the Critical Entities Resilience (CER) Directive must also comply with the NIS2 Directive. However, not all entities regulated under the NIS2 Directive are necessarily covered by the CER Directive. The NIS2 Directive aims to enhance cybersecurity across the EU by setting common standards and requirements for network, OT, and information systems.

On the background of the national strategi and the identification of the critical entities, the entities must be ready to comply after the 17th of June 2026, there will be an implementation period after this date.

The directive aims into the following key points.

Scope and Implementation

The directive covers eleven sectors such as energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, and food. EU member states are required to transpose the directive into national law by October 17, 2024.

Risk Assessments and Reporting

Critical entities must conduct regular risk assessments and report to relevant authorities. These assessments should consider natural disasters, sabotage, supply chain disruptions, and other threats. Entities are also required to prepare contingency plans to enhance their resilience.

Physical Security

Ensure adequate physical protection of premises and critical infrastructure. Technical surveillance such as CCTV and other means of detection is a part of physical security.

Preparedness and Business Continuity Plans

Ensure recovery, consider continuity measures, and identify alternative supply chains.

Inclusion of Subcontractors

In contrast to NIS2 (Article 21(2)(d)), the CER Directive does not directly require the inclusion of supply chain security in risk management. Similarly, unlike DORA (Article 30), the CER Directive does not set minimum requirements for key (supply security) provisions in supplier contracts. However, it is difficult to imagine that supplier security requirements will not play a significant role in ensuring resilience and security in the supply chains. Regardless of the regulatory minimum requirements, the implementation of the CER Directive is likely to have a spill-over effect on suppliers to designated critical entities.

Relevant topics in tenders, service level agreements, and contracts may include:

- ❏ Inclusion of physical security requirements in evaluation criteria for public tenders
- ❏ Requirements for risk assessments and risk management frameworks
- ❏ Requirements to use (the principles of) certain standards for physical security
- ❏ Requirements for specific technical, security, and organizational measures
- ❏ Requirements for training, vetting, and screening of specific employee groups
- ❏ Requirements for handling insider threats and access controls
- ❏ Requirements for ongoing quality control and quality assurance
- ❏ equirements to ensure compliance with regulations (directly or indirectly)
- ❏ Requirements for documentation, disclosure obligations, and reporting
- ❏ Requirements for participation in supervision or audits
- ❏ Requirements for specific insurance coverages and amounts
- ❏ Modifications or exceptions to usual liability limitations and disclaimers

Awareness Training and Vetting of Staff

Ensure employee security management, including access rights, background checks, training requirements, and qualifications.

The Implementation in Denmark

The implementation work in Denmark is well underway, the Danish legislation was passed by the Parlement on the NIS2 and the CER directives, so that both directives is implemented in the Danish laws, there is in Denmark also a direct law for the energy sector ,this legislation was an broadening of the old NIS, the new legislation cowers all aspect in the energy sector, from Oil, Gass, Electricity, heating and cooling.

And for the tele sector a legislation on preparedness has also been passed in the tele sector and for the suppliers for the sector.

So, in Denmark we are on the way, and the timeline is the same in relation to critical infrastructure and a national strategy for this.

Resilience Center Denmark

The RTOs in Denmark with The Danish Institute for Fire and Security (DBI) as the lead has established Resilience Center Denmark to support the implementation and to guide the suppliers of Resilience in building solutions and establishing training and educations for the SMEs.

The Centre also aims to support the implementation of the new legislations in Denmark. You can read more about the center here: *resilienscenter.dk/en/*

Implementation in Germany

Germany has not yet transposed this directive into German legislation due to the end of the govern-

RTOs: *Research and Technology Organisations – in Dänemark ein System privater Non-Profit-Institute für den Aufbau technischer Kompetenzen in Wirtschaftsunternehmen*

DORA: *Digital Operational Resilience Act*

Ob Naturkatastrophen oder Sabotageakte – Verkehrsinfrastruktur ist vielfältig verwundbar (Foto: allenrobert/pixabay)

Der Autor dieses Beitrags, **Jesper Florin,** ist Head of Security and Resilience beim Dänischen Institut für Brand- und Sicherungstechnik (DBI) und Vice Chair der Security-Kommission bei CFPA Europe.

Kontakt:
jfl@brandogsikring.dk

ment in November 2024 and awaiting the election of a new government. The election in April and the appointment of the new chancellor are now in place, and hopefully, the work will continue.

Germany's approach to implementing the CER Directive involves the creation of the KRITIS-Dachgesetz (KRITIS-DachG), a comprehensive framework law aimed at strengthening the resilience of operators of critical infrastructure. This law will work alongside existing regulations such as the IT Security Act (BSIG) and the NIS2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG).

Key Elements of the KRITIS-DachG

Identification and Registration

Critical entities must be identified and registered. This includes entities providing essential services to at least six EU member states.

Resilience Measures

Entities are required to implement technical, security-related, and organizational measures to ensure their resilience. These measures must be documented in a resilience plan.

Reporting and Audits

Entities must report significant disruptions and undergo regular audits to verify compliance with resilience measures.

Support and Guidance

The Federal Office for Civil Protection and Disaster Assistance (BBK) will provide templates, guidelines, and training to support entities in meeting their obligations.

Implementation with Standards as the Framework

The directives point to known and existing standards as framework tools. This means that they often reference established standards and best practices to guide the implementation and compliance processes. For example, international standards like ISO and European standards such as those developed by CEN (European).

Special Provisions for Financial Entities

The CER Directive is complemented by the Digital Operational Resilience Act (DORA), which focuses on IT security for financial entities such as banks, insurance companies, and investment firms. This ensures a comprehensive approach to resilience across both physical and digital domains.

Conclusion

The CER Directive represents a significant step towards enhancing the resilience of critical infrastructure in the EU. By establishing uniform standards and requiring regular risk assessments and reporting, the directive aims to protect essential services from a wide range of threats. Germany's implementation through the KRITIS-DachG will play a crucial role in ensuring the country's critical infrastructure can withstand and recover from crises, thereby safeguarding societal functions and economic stability.

Der Verweis auf bestehende Normen im KRITIS-DachG erleichtert seine Anwendung (Foto: u_4xcm1iw8y9/pixabay)