EU Directive

NETWORK AND INFORMATION SECURITY

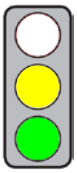
cep**PolicyBrief** No. 2013-26

Centrum für Europäische Politik

KEY ISSUES

Aim of the Directive: To ensure a minimum level of network and information security in the EU.

Parties affected: Suppliers of critical infrastructures, internet companies, public authorities



Pro: (1) National NIS strategies increase awareness of risks and the ability to respond to cyber dangers.

(2) The mandatory requirement for operators of critical infrastructures to take security measures is appropriate.

Contra: (1) Small and medium-sized companies should be exempt from the reporting duty.

(2) There are no minimum criteria for the reporting of security incidents.

(3) The establishment of a central national authority for NIS is not compatible with the federal structure of the German state.

CONTENT

Title

Proposal COM(2013) 48 of 7 February 2013 for a **Directive** concerning measures to **ensure a high** common level of **network and information security** across the Union

Brief Summary

- **Context and objectives**
  - The objective of the Directive is to ensure a high level of network and information security (NIS) across the EU.
  - The Directive forces Member States to (Art. 1 (1), (2) and (4)):
    - adopt national strategies for network and information security,
    - work together with the EU Commission to detect and respond to "security incidents",
    - impose technical requirements and reporting obligations on "market operators" and public authorities.
  - The Member States may set more stringent security requirements (minimum harmonisation) (Art. 2).

- **Scope**
  - The Directive applies to "networks and information systems" relating to information technology (IT). These are (Art. 3 (1))
    - electronic communication networks - e.g. telecommunications networks, mobile telephony and radio networks,
    - devices for processing computer data - e.g. computers, mobile telephones - and
    - computer data which is to be stored, processed, accessed or transmitted.
  - The Directive applies to "market operators" and public authorities.
    - Market operators are (Art. 3, No. 8)
      - providers of "information society services" - e.g. search engines and social networks - and
      - operators of "critical infrastructures" that are essential to the maintenance of vital economical functions - e.g. banks, energy supply companies, hospitals, stock exchanges, transport companies.
    - Entities not regarded as market operators because they are already covered by other provisions are (Art. 1 (3)):
      - operators of public communication networks, such as mobile telephone networks,
      - providers of publicly available electronic communications services, such as telephone services
      - trust service providers, such as electronic seals.

- **Central national authority, national NIS strategies, emergency team**
  - Each Member State has to designate a national competent authority to monitor the application of this Directive at national level (Art. 6 (1) and (2))
  - Each Member State must define and adopt a national NIS strategy.
  - This strategy has to address the following issues (Art. 5 (1) and (2)):
    - the definition of the objectives and priorities based on an up-to-date risk and incident analysis,
    - a "governance framework" to achieve the objectives,
    - general measures on "preparedness, response and recovery"
    - a national NIS cooperation plan defining, inter alia, communication processes to ensure "prevention, detection, response, repair and recovery".

Authors: Ariane Kiesow and Philipp Eckhardt | kiesow@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-246 | www.cep.eu

– Each Member State must set up a "Computer Emergency Response Team", CERT). CERT is under the supervision of the competent national authority and "may" be established within it (Art. 7 (1) and (5)).
– The CERT is responsible, inter alia, for the following tasks (Art. 7 (1) in conjunction with Annex 1):
  - Monitoring and analysis of, as well as response to, security risks and incidents.
  - Providing early warning and dissemination of information about security incidents to those potentially affected or involved such as companies and private individuals.
– The CERT must have a "secure and resilient communication and information infrastructure" (Art. 7 (3)).

► **Cooperation between Member States and EU Commission**
– The national authorities and the Commission work together via a "cooperation network" (Art. 8 (1)).
– The national authorities and the Commission circulate early warnings on risks and incidents where these (Art. 8 (3) a, Art. 10)
  - (may) grow "rapidly" in scale,
  - (may) exceed national response capacity,
  - (may) affect more than one Member State.
– The national authorities and the Commission have to communicate any relevant information that may be useful for assessing risks or incidents (Art. 10 (2). Where there is a "suspected" criminal background, the European Cybercrime Centre must be informed (Art. 10 (4)).
– Where there has been an early warning, the authorities have to agree on a "coordinated response" (Art. 8 (3) b, Art. 11).
– The Commission specifies the details
  - of the criteria for an early warning, in delegated acts (Art. 10 (1) and (5)),
  - of the "coordinated responses", by way of implementing acts (Art. 12 (2) b).
– The authorities shall, inter alia, (Art. 8 (3) c, g and h)
  - publish "on a regular basis" their early warnings and coordinated responses on a website,
  - assist each other in "building capacity" on NIS,
  - organise regular peer reviews of capabilities and preparedness.
– Each Member State and the Commission may request that national NIS strategies, the NIS cooperation plans and the "effectiveness" of the CERTs be "jointly discussed and assessed". (Art. 8 (3) d and e).

► **Security measures and notification obligations**
– The Member States must ensure that public authorities and market operators take "appropriate technical and organisational" measures to "manage" security risks and incidents. The measures must, having regard to the "state of the art", guarantee a "level of security appropriate to the risk presented" and "ensure continuity" of services. (Art. 14 (1)). The Member States define the actual content of the measures.
– The market operators and public authorities must report, to the competent authority, any incidents having a "significant" impact on the security of the core services they provide. The Commission will define, by means of implementing acts, the "formats and procedures" applicable to the reporting duty and the "circumstances" under which it applies. (Art. 14 (2), (5) and (7)).
– "Micro-enterprises" are exempt from the security requirements and reporting duties (Art. 14 (8)).
– Where the disclosure of an incident is in the public interest, the competent authority may (Art. 14 (4))
  - inform the public of the incident or
  - require the public authorities or market operators to inform the public.
– The competent authority may
  - investigate breaches of the security requirements and reporting duties (Art. 15 (1)),
  - require the market operators and public authorities to provide information about their networks and information systems (Art. 15 (2) a),
  - carry out security audits of market operators and public authorities (Art. 15 (2) b),
  - issue binding instructions to market operators and public authorities (Art. 15 (3)).

► **Sanctions**
The Member States must lay down "effective, proportionate and dissuasive" sanctions for breaches of the Directive (Art. 17).

Main Changes to the Status Quo

► Until now, only companies providing publicly available communication networks and services, and trust service providers, have been obliged to comply with security standards and report security incidents (Directive 2002/21/EC).

Statement on Subsidiarity by the Commission

According to the Commission, an EU-wide standard minimum level of protection of NIS is necessary in order to achieve adequate preparedness and to enable cooperation based on trust. Considering the cross-border nature of security risks and incidents, the minimum standard protection can be achieved more effectively at EU level than by the Member States.

Policy Context

In 2009, in its Communication on the protection of critical infrastructures [COM (2009) 149], the Commission proposed higher security standards for these. The "Digital Agenda for Europe" [COM(2010) 245] dating from 2010 (see cep**PolicyBrief**) contains proposals aimed at improving the security of the digital single market. In 2011, in the Communication "Achievements and next steps: towards global cyber-security" [COM(2011) 163], the Commission established that a national procedure for handling security problems was insufficient and that closer cooperation between the Member States was necessary. This proposal is the most important measure in the "Cyber Security Strategy" which was announced in February 2013 [JOIN(2013) 1]. In parallel, the mandate of the European Network and Information Security Agency (ENISA) is to be extended and its area of responsibility widened [COM(2010) 521]. In future, ENISA will be able to coordinate and support to a greater extent the cooperation of the Member States with each other and with the Commission. Furthermore, it will in future be more closely involved in the work of the CERTs and will also have close links with national data protection authorities and Europol.

Legislative Procedure

7 February 2013	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorate General:	DG Connect
Leading Committee of the EP:	Internal Market and Consumer Protection (leading); Rapporteur Andreas Schwab (EVP Group, DE)
Leading Federal Ministry:	Federal Ministry of the Interior
Leading Committee of the BT:	Interior Committee
Decision mode in the Council:	Qualified majority (Adoption by a majority of the Member States and with 255 of 345 votes; Germany: 29 votes)

Formalities

Legal competence:	Art. 114 TFEU (Internal Market)
Form of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Legislative procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

Modern economies are dependent on effective information technology (IT) networks and systems. If attacks succeed in compromising IT networks or information systems, particularly those used by operators of "critical infrastructures" such as energy, gas or water supply companies, this can result in enormous economic damage. **The duty of the Member States to define national NIS strategies increases their awareness of risks and their ability to respond to cyber dangers** and is therefore appropriate. The requirements of the Directive are, however, very abstract so it remains to be seen how detailed the national NIS strategies actually turn out to be.

The mandatory requirement for security measures constitutes considerable interference with entrepreneurial freedom and may involve substantial costs. **In this case, however, it is certainly justified**. It is in the interest of the companies who are subject to the Directive ("market operators") to protect their networks and information systems against technical failures by investing in IT security because such events can result in loss of revenue and of reputation. Unlike technical failures, intrusions into networks and information systems are not (immediately) apparent to the public. Although customers may discover at a later date that misuse - such as the unlawful use of personal data for criminal purposes - has taken place, it is rarely possible for them to identify the source - such as the hacked website. The direct consequence of this information asymmetry is that companies do not have to take account of being liable for loss caused by deficient IT security. The result of this is insufficient investment in IT security. Since the principle of liability does not work properly due to this lack of direct accountability for loss, the mandatory requirement for companies to take security measures is justified.

For operators of "critical infrastructures" these requirements should form part of the permit conditions if the operator is unable to show that it has appropriate insurance. Here, although technical failures are immediately apparent and attributable, the consequential loss is generally so high that compensation - such as for a power cut in a city lasting several days - may exceed the operator's financial capacity.

It would make sense to determine the security measures on a standard EU-wide basis instead of leaving it to the Member States. Otherwise there is a risk of a distortion of competition because, for example, companies compete via online mail-order business with companies in other Member States or because the consequences of incidents - such as in the case of banks - are not limited to individual Member States.

Differing levels of national security do not constitute a locational advantage because the technical details of the security measures are not comprehensible to the layperson.

A large number of reported security incidents means that gaps in security - such as in software or hardware - can be identified quickly and reliably. Since all market operators and public authorities gain from this, reporting takes on the character of a public good. At the same time, every company has a rational incentive to refrain from reporting incidents, such as to avoid damage to reputation or to save reporting costs. **A duty to report incidents is** therefore **appropriate.** However, the Commission should prescribe not only the "formats and procedures" and "circumstances" of the reporting, but also the minimum criteria for the content of the report. This could ensure that the reports enable conclusions to be drawn as to the gaps in the security of the compromised system because only a high quality database can give rise to valid recommendations for action.

The analysis of an incident necessary for the report is generally very involved and costly because finding and evaluating the underlying gaps in security requires specialist knowledge. Small and medium-sized companies generally do not have suitable staffing or technical capabilities to formulate meaningful reports or deal with queries. **It would therefore make sense to exempt not only micro-enterprises from the reporting duty,** as proposed by the Commission, **but also all small and medium-sized companies.**

The fact that the Directive is not intended to apply to software and hardware manufacturers is misconceived because it is precisely these market operators who would be able to close the gaps in their systems, identified as a result of the reporting duty, and provide their customers with security updates. Thus the Commission could achieve the increase in network and information security more quickly and efficiently.

Legal Assessment

Legislative Competency

The Directive is correctly based on Art. 114 TFEU (Internal Market).

Subsidiarity

Unproblematic.

Proportionality

Unproblematic. The Commission has chosen the Directive as the legislative form and is only aiming for minimum harmonisation.

Compatibility with EU law

Unproblematic.

Compatibility with German law

The requirements of the Directive are, to a certain extent, already included in German law, particularly the Telecommunications Act (*Telekommunikationsgesetz -TKG*), or are planned in Germany. In March 2013, the Federal Ministry of the Interior submitted the first draft of a law to increase the security of IT systems. This states that "the operators of critical infrastructures" in the areas of energy, information technology and telecommunications, transport and traffic, health, water, food, as well as the finance and insurance sector, are to be under a duty to protect the relevant "information technology systems, components or processes" in accordance with the last available technology. In addition, they will have to report serious incidents to the Federal Office for Information Technology Security (BSI). [*BSI-Gesetz* (First Draft)]

The secrecy of telecommunications and personal data already have to be protected in accordance with the latest available technology (Section 109 (1) TKG). In future, the telecommunications infrastructure will also be protected according to the latest available technology [Section 109 (2), page 5 TKG (Draft)]. The Federal Network Agency and the Federal Data Protection Officer already have to be informed if the protection of personal data is breached (Section 109a (1) TKG). In future, the Federal Network Agency will also have to be informed of interference with services and networks which disrupt the availability of services or which could lead to unlawful access to telecommunications and data processing systems [Section 109a (4) TKG (Draft)].

The establishment of a central national authority for NIS is in breach of the federal structure of the German state as laid down in the Grundgesetz (GG, German Constitution) (Art. 83 et seq. GG). As an exception, Art. 91c GG only permits collaboration between national government (Bund) and the Länder in respect of the planning, setting up and operation of its IT systems.

Conclusion

The duty of the Member States to define national NIS strategies increases their awareness of risks and their ability to respond to cyber dangers. The mandatory requirement for security measures constitutes considerable interference with entrepreneurial freedom and may involve substantial costs. It is however appropriate in this case. Security measures should be laid down on a standard EU-wide basis. A reporting duty with regard to incidents is appropriate but small and medium sized companies should be exempt from it. The establishment of a central national authority for NIS is in breach of the federal structure of the German state as laid down in the Grundgesetz (GG).