The NIS2 Directive will increase IT security

The upcoming EU directive on the protection of network and information systems places new demands on Danish companies, but also creates new opportunities.

By Martin Wex

Better IT security, greater personal responsibility and a better negotiating position with insurance companies. These are some of the immediate consequences for companies that are covered by and manage to comply with the rules of the upcoming EU directive on the protection of network and information systems, NIS2. The aim of the directive is to strengthen risk management in the digital area, and although it means new and increased requirements for companies in the EU, according to cybersecurity specialist Lars Schak from WTW, there are also very positive aspects of the directive from a business perspective.

»With NIS2, there are increased requirements for risk assessments, implementation of security measures, control and documentation, and this naturally means that there are a large number of tasks to be solved and new processes to be put in place. But if you keep an open mind, the companies that make it to the other side will find that their IT security has been significantly improved and that they are therefore better equipped to withstand a cyberattack,« says Lars Schak.

> “
>
> The companies that make it to the other side will find that their IT security has been significantly improved
>
> **Lars Schak**
> Cybersecurity specialist, WTW

The NIS2 Directive applies to companies with more than 49 employees and an annual turnover of more than DKK 75 million. In addition, the company must belong to a sector that the EU has characterized as either essential or important to society. Energy, transport, health and banking are among the essential sectors, while postal services and waste management as well as the production of chemicals, food and medical supplies are among the important sectors.

The directive requires covered organizations to have management approval and oversight of cyber risk management, but there are differences in how thoroughly authorities will monitor compliance. Significant organizations will be subject to a comprehensive preceding and subsequent supervision regime, while important organizations will only be subject to a subsequent supervision regime.

Many new requirements

The list of minimum requirements that companies will need to demonstrate compliance with in the future is long. It includes establishing policies and procedures for maintaining cybersecurity within the organization, creating contingency plans for handling data breaches and establishing secure supply chains.

Companies that are not directly covered by the directive may be indirectly affected through requirements from their clients.

»The NIS2 Directive requires secure supply chains, and therefore subcontractors may be required to comply with some of the rules in the directive if they want to continue to be suppliers to covered companies. This means that the NIS2 directive also becomes a competitive differentiator, where companies that comply with the rules will have a competitive advantage,« says Lars Schak.

WTW has drawn up ten recommendations that can serve as a roadmap for achieving the IT security required by the NIS2 directive. The recommendations include the use of multi-factor authentication (MFA), regular data backups and establishing a secure email and web communication.

A personal responsibility

The NIS2 Directive imposes a new personal responsibility on management and the board of directors to ensure effective cyber risk management, and the directive suggests that individual managers or board members may be fined for non-compliance. In the extreme, the directive even allows for the temporary suspension of individuals or parts of the organization.

> “
>
> With the NIS2 Directive we at least have a clear recipe for what to do to handle cyber security
>
> **Pernille Kornath Møller**
> FINEX Practice Specialist, WTW

»It is our impression, that this is a topic that is already being discussed in a lot companies. And it is our assessment that the directive can have a spill-over effect on the assessment of liability in relation to the management and board of directors if you are faced with a claim for compensation. It is too early to say what the consequences will be in practice, but with the NIS2 Directive we at least have a clear recipe for what to do to handle cyber security,« says FINEX Practice Specialist Pernille Kornath Møller, who together with Lars Schak assists WTW's clients with tendering and negotiation of cyber insurance and directors' and officers' liability insurance.

Directors' and officers' liability insurance generally covers claims based on the misconduct of the executive board and board of directors, but does not cover, for example, criminal fines, which cannot be insured under Danish law.

A better risk

Pernille Kornath Møller does not expect the NIS2 Directive to lead to any short-term changes in terms and conditions for cyber insurance or directors' and officers' liability insurance, but it may have a positive effect for companies that manage to meet the requirements.

»When you can document that you comply with the rules of the NIS2 Directive, you have a good starting point when negotiating new terms and conditions for your insurance policies,« says Pernille Kornath Møller.

The NIS2 Directive is a minimum directive that must be incorporated into Danish law before it officially comes into force. This means that the Danish rules must at least comply with the directive. WTW encourages Danish companies to start ensuring compliance now, if they have not already done so.

The directive is expected to come into force in early 2025.