18 Oct 2024 -03:00

Belgium sets the standard: first member state to fully implement new European rules on cyber security (NIS2)

Companies can now really get down to business

Belgium is the first European member state to fully implement the new NIS2 legislation. These rules significantly strengthen the level of cyber security. An estimated at least 2,500 Belgian organisations are required from today to register on the website atwork.safeonweb.be and take security measures. They thus hold the key to taking their cyber security to the next level.

In attacks involving ransomware and data theft, vulnerable organisations fall victim daily to cybercriminals who capitalise on visible security holes or the lack of two-step verification (2FA). The new European Network and Information Security Directive (NIS2) aims to put a stop to this. Designed to increase the resilience of EU countries against cyber threats, it was transposed into the NIS2 law in Belgium.

Positive impact on cybersecurity

"Currently, around 200 organisations are already registered with us, but we expect this to rise sharply in the coming weeks," Miguel De Bruycker, director general of the Centre for Cybersecurity Belgium (CCB), told IANS.

"The NIS2 legislation extends the existing cybersecurity rules to more sectors. Organisations should not see NIS2 as a burden, but as an opportunity to strengthen their resilience," says Valéry Vander Geeten, Head of Legal at the Centre for Cybersecurity Belgium (CCB). "The legislation distinguishes between important and essential organisations, depending on sector and size."

With some exceptions, the NIS2 law applies to organisations of a certain size that are established in Belgium and provide at least one of the services listed in the annexes to the law within the European Union. The size criterion means that the entity must have at least 50 full-time employees or an annual turnover (or annual balance sheet total) of more than €10 million. The number of affected sectors has thus increased significantly, from 7 to 18.

Notification of incidents and registration are the first steps

From 18 October, organisations must report significant incidents to the CCB within 24 hours, followed by further information within 72 hours and a final report within 30 days.

In addition, all NIS2 companies and organisations must register on the portal at atwork.safeonweb.be through a legal representative by 18 March 2025. Registration requires information about the organisation, including contact person, sector and size. After registration, companies will get access to additional services to help identify and mitigate cyber threats tailored to each company's network and domain.

CyberFundamentals framework: a step-by-step approach

All entities must take the necessary measures to increase their cyber security. The CCB has provided the

CyberFundamentals framework for this purpose. The CCB supports organisations with a risk assessment that allows each organisation to determine the appropriate level of CyberFundamentals. This innovative framework contains step-by-step additional measures for each security level, based on international cyber security standards and insights according to experience from thousands of incidents.

The final piece: certification

"Essential entities must also undergo regular assessments based on the CyberFundamentals or the ISO 27001 standard" says Johan Klykens, Director of Certification at the Centre for Cybersecurity Belgium (CCB). "This certification provides companies with a clear method to demonstrate that they have taken their responsibilities regarding cyber security."

However, in cases where IT services are outsourced, the legal responsibility remains with the organisation itself. It is crucial to request guarantees and certifications from suppliers, which is possible through the CyberFundamentals framework. Moreover, the CCB recommends including the cybersecurity requirements of key IT suppliers in the organisation's tailored assessment.

It goes without saying that the CCB encourages all organisations, which are not covered by the NIS2 legislation, to work on cyber security through the CyberFundamentals. Just because an organisation is not considered an entity covered by the NIS2 legislation does not mean it can ignore the requirements of the legislation. In practice, a large number of organisations will have to comply with the requirements because they provide services to NIS2 entities.

All resources are available at atwork.safeonweb.be

Centre for Cyber Security Belgium
Rue de la Loi 18
1000 Brussels
Belgium
http://www.ccb.belgium.be

Katrien Eggers
Spokesperson(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

Michele Rignanese
Spokesperson(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

© 2024 - news.belgium.be