18121/J XXVII. GP

Eingelangt am 15.03.2024

Anfrage

der Abgeordneten Dr.in Petra Oberrauner, Robert Laimer, Genossinnen und Genossen

an den Bundesminister für Arbeit und Wirtschaft

betreffend **Umsetzung der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)**

In dem Bestreben die Mitgliedsländer der Europäischen Union besser vor Cyberangriffen und Cyberkriminalität zu schützen hat die EU am 14. Dezember 2022 die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) beschlossen. Sie ist am 16. Januar 2023 in Kraft getreten und wird die bisherige NIS-Richtlinie aus dem Jahr 2016 ersetzen. Dazu müssen die Mitgliedstaaten die neue Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen.

Damit kommt auf einen großen Teil der österreichischen Unternehmen, auf die öffentliche Verwaltung und die zuständigen Behörden ein erheblicher Handlungsbedarf zu, denn im Vergleich zur bisherigen NIS-Richtlinie wurde bei NIS-2 der Geltungsbereich massiv ausgeweitet und umfasst nun neben kritischen Bereichen, wie bspw. Energieversorgung und digitale Infrastruktur auch die öffentliche Verwaltung und mittlere sowie große Unternehmen, bspw. aus den Bereichen der Lebensmittelindustrie, der Chemie sowie dem verarbeitenden und herstellenden Gewerbe. Ob NIS-2 neben der zentralen auch auf die regionalen öffentlichen Verwaltungseinrichtungen angewendet werden soll, liegt in der Entscheidung der Mitgliedstaaten.

Die betroffenen Unternehmen und öffentlichen Verwaltungseinrichtungen sind verpflichtet, in ihrer IT-Sicherheit den Stand der Technik zu implementieren und umfangreiche Risikomanagementmaßnahmen umzusetzen, was bei den Unternehmen auch ihre Lieferketten betrifft und zudem Angelegenheiten der betrieblichen Mitbestimmung berührt. Außerdem sind sie verpflichtet, die zuständigen nationalen Behörden unverzüglich über signifikante Störungen, Vorfälle und Cyber Threats, die ihre kritischen Dienstleistungen betreffen, zu unterrichten. Verantwortlich für die Umsetzung und die Einhaltung der neuen Sicherheitsverpflichtungen sind die Leitungsorgane der betroffenen Einrichtungen, die auch schadensrechtlich haften, wenn dem Unternehmen durch die Nichteinhaltung ein schuldhaft verursachter Schaden entstanden ist. NIS-2 sieht zudem umfangreiche Sanktionen von bis zu 10 Mio.€ vor, sollten diese Verpflichtungen nicht eingehalten werden.

Um die Beaufsichtigung der Einhaltung der NIS-2-Richtlinie zu stärken, sieht die Richtlinie eine Reihe von Aufsichtsmitteln für die zuständigen Behörden vor, darunter gezielte Audits, Vor- und Nachprüfungen, Informationsanfragen und Zugang zu Dokumenten oder Beweismitteln.

Die unterfertigten Abgeordneten stellen daher folgende

ANFRAGE

1. Bis wann werden Sie dem Nationalrat ein entsprechendes Gesetz zur nationalen Umsetzung der NIS-2-Richtlinie vorlegen?
2. Wie viele Unternehmen in Österreich werden die in der NIS-2-Richtlinie genannten Maßnahmen ungefähr umsetzen müssen ?
3. Wie viele Kleinunternehmen werden von NIS-2 betroffen sein?
4. Wie viele Einrichtungen der öffentlichen Verwaltung werden die in der NIS-2-Richtlinie genannten Maßnahmen ungefähr umsetzen müssen ?
5. Wird in Österreich die NIS-2-Richtlinie auch auf regionale/lokale Verwaltungseinrichtungen angewendet werden? Wie werden dabei z.B. Gemeindeverbände und ähnliche Konstruktionen betroffen sein?
6. Welche Maßnahmen werden von ihrer Seite gesetzt, um sicherzugehen, dass all diejenigen Unternehmen und Verwaltungseinrichtungen, die von der NIS-2-Richtlinie betroffen sind, rechtzeitig darüber informiert werden?
7. Welche Maßnahmen werden von ihrer Seite gesetzt, um insbesondere betroffene Kleinunternehmen, für die die Umsetzung und Einhaltung der NIS-2-Richtlinie sowohl vom Knowhow her als auch aus personeller und finanzieller Sicht eine Herausforderung darstellen kann, zu unterstützen?
8. Welche Maßnahmen werden ergriffen, um sicherzustellen, dass betroffene KMU und Einrichtungen der öffentlichen Verwaltung Zugang zu qualifizierten Cybersicherheitsexperten bekommen, insbesondere angesichts des Mangels an Fachkräften auf diesem Gebiet?
9. Wird das nationale Gesetz, mit dem die NIS-2-Richtlinie in Österreich umgesetzt werden soll, eine Klarstellung beinhalten, dass die betriebliche Mitbestimmung von diesem Gesetz unberührt bleibt? Falls nein, warum nicht?
10. Auf wie viele Behörden sollen die mit der Beaufsichtigung der Einhaltung der NIS-2-Richtlinie verbundenen Zuständigkeiten aufgeteilt werden? Welche Behörde wird für welche Aufgaben zuständig sein?
11. Wie viele Planstellen und welche finanziellen Mittel sind von Ihnen in den zuständigen Behörden für die Beaufsichtigung der Einhaltung der NIS-2-Richtlinie eingeplant?
12. Wie werden Sie sicherstellen, dass den zuständigen Behörden, in Zeiten wo es an IT-Experten mangelt, ausreichend Fachkräfte für die Beaufsichtigung zur Verfügung stehen?
13. Bei wie vielen Unternehmen und Einrichtungen der öffentlichen Verwaltung sollen regelmäßige Audits stattfinden?
14. Wie viele Audits sowie vor Ort & Off-Site Kontrollen sollen jährlich durchgeführt werden?
15. Werden die in der Richtlinie angeführten Strafen für alle Leitungsorgane gelten oder sind die öffentlichen Einrichtungen von den Strafen, wie bei der DSGVO, ausgenommen?