

Kleine Anfrage

des Abgeordneten Dr. Dietrich (AfD)

und

Antwort

des Thüringer Ministeriums für Inneres und Kommunales

Zweite Fassung der Richtlinie zur Netzwerk- und Informationssicherheit (NIS 2), ihre Umsetzung in Thüringen und die Auswirkungen auf Thüringen

Anfang des Jahres 2023 ist die zweite Fassung der Richtlinie zur Netzwerk- und Informationssicherheit (NIS 2) EU-weit in Kraft getreten. Die EU-Mitgliedstaaten müssen NIS 2 bis zum 17. Oktober 2024 in nationales Recht umsetzen. In Deutschland liegt bereits jetzt ein Referentenentwurf des Bundesministeriums des Innern und für Heimat zum NIS-2-Umsetzungsgesetz vor. Daraus geht hervor, dass nicht nur die Zahl der betroffenen Unternehmen massiv ansteigt, sondern es zusätzlich auch noch wesentlich höhere Anforderungen geben wird. Die neuen IT-Sicherheitsregeln sollen kritische Infrastrukturen besser gegen Cyberangriffe sichern. Bund und Länder wollen jedoch Kommunen von den Vorgaben ausnehmen.

Das Thüringer Ministerium für Inneres und Kommunales hat die **Kleine Anfrage 7/5445** vom 6. Dezember 2023 namens der Landesregierung mit Schreiben vom 7. März 2024 beantwortet:

Vorbemerkung

Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS-2-Richtlinie)¹ weitet den Anwendungsbereich der Cybersicherheitsvorschriften auf neue Sektoren und Einrichtungen aus und soll die Resilienz- und Reaktionskapazitäten öffentlicher und privater Stellen, der zuständigen Behörden und der EU insgesamt weiter verbessern. Dafür werden zwei Gruppen von Betreibern ("Entities") definiert, die in insgesamt 18 Sektoren in der EU Dienstleistungen erbringen und überwiegend nach Größe, das heißt grundsätzlich allein anhand des Umsatzes und der Beschäftigtenzahl und nicht mehr anhand von Schwellenwerten der Versorgungskritikalität, reguliert werden.

Eine Gruppe sind die sogenannten wichtigen Einrichtungen ("Important Entities") mit mindestens 50 Beschäftigten und/ oder mehr als zehn Millionen Euro Jahresumsatz beziehungsweise Jahresbilanzsumme. Hierzu zählen beispielsweise Post- und Kurierdienste, Anbieter digitaler Dienste wie Marktplätze, Suchmaschinen und Soziale Netzwerke, das verarbeitende Gewerbe mit Herstellern von Medizinprodukten, Computern, Elektronik, Optik oder elektrischer Ausrüstung, Unternehmen aus dem Maschinen- und dem Fahrzeugbau, aber auch Forschungsinstitute (ohne Bildungseinrichtungen).

In elf Sektoren mit hoher Kritikalität, vergleichbar mit den bisherigen Sektoren für Kritische Infrastrukturen, finden sich Betreiber sog. wesentlicher Einrichtungen ("Essential Entities") mit mehr als 250 Beschäftigten oder einem Jahresumsatz von mehr als 50 Millionen Euro beziehungsweise einer Jahresbilanzsumme

¹ Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, Seite 80).

von mehr als 43 Millionen Euro. Neben diesen Betreibern werden unabhängig der Größe bestimmte Betreiber aus dem Sektor Digitale Infrastruktur sowie Teile der öffentlichen Verwaltung als wesentliche Einrichtungen reguliert.

Zu beiden Gruppen können Sonderfälle hinzutreten, welche die Mitgliedsstaaten als "wesentlich" oder "wichtig" festlegen können. Das betrifft nationale Betreiber, die essentiell für Gesellschaft und Wirtschaft sind, Betreiber, deren Ausfall einen signifikanten Effekt auf öffentliche Sicherheit oder Gesundheit hätte, Betreiber, deren Ausfall ein signifikantes systemisches Risiko für Sektoren und grenzüberschreitende Abhängigkeiten darstellt sowie Betreiber, die wegen spezieller nationaler oder regionaler Wichtigkeit kritisch sind.

Sowohl der Bund als auch die Länder sind verpflichtet, die Vorgaben der NIS-2-Richtlinie im Rahmen ihrer jeweils eigenen Zuständigkeit und in eigener Verantwortung umzusetzen. Ein Gesetzentwurf des Bundes liegt - entgegen der Vorbemerkung des Fragestellers - noch nicht vor. Es existieren lediglich Eckpunkte des Bundesministeriums des Innern und für Heimat (BMI) für ein Bundesgesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) vom Februar 2023 sowie ein im Internet veröffentlichtes Diskussionspapier des BMI für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland vom Oktober 2023.

1. Wie ist der aktuelle Stand der Umsetzung der NIS-2-Richtlinie in Thüringen?

Antwort:

Die NIS-2-Richtlinie entfaltet im Sektor öffentliche Verwaltung grundsätzlich nur für die Einrichtungen der Zentralregierung² und der regionalen Ebene Wirkung (Artikel 2 Abs. 2 Buchst. f der Richtlinie). Optional besteht die Möglichkeit die Regelungen auch auf die lokale Ebene anzuwenden. Eine über die Richtlinie hinausgehende verpflichtende Einbeziehung des kommunalen Bereichs und der Bildungseinrichtungen wird überwiegend angesichts bereits bestehender Regelungen und nationaler Standards zur Orientierung nicht als zielführend angesehen und ist vielfach unter dem Zeitdruck nicht sinnvoll umsetzbar. In der Landesverwaltung ist geplant, die Umsetzung mittels einer Verwaltungsvorschrift zu gestalten. Hierzu wird das durch den IT-Planungsrat beschlossene Identifizierungskonzept der Länder zur Umsetzung der NIS-2-Richtlinie auf regionaler Ebene Anwendung finden.

2. Wie viele private Unternehmen in welchen Branchen werden in Thüringen voraussichtlich welche Maßgaben der NIS-2-Richtlinie umsetzen müssen?

Antwort:

Wie viele Unternehmen in Thüringen unter diese Regulierung fallen werden und welche Maßnahmen durch diese konkret umzusetzen sind, kann derzeit nicht abgesehen werden, weil ein Gesetzentwurf der Bundesregierung zur Umsetzung der NIS-2-Richtlinie noch nicht vorliegt. Aus Unternehmensstatistiken des Landesamts für Statistik kann - unter Berücksichtigung unterschiedlicher Klassifizierungsvorgaben - abgeschätzt werden, dass eine große Zahl von mittelständischen Unternehmen in Thüringen betroffen sein werden. Diese Unternehmen wären zumindest als wichtige Einrichtungen gemäß Artikel 2 Abs. 1 NIS-2-Richtlinie anzusehen.

Unternehmen, welche als wesentliche oder wichtige Einrichtungen gelten, müssen gemäß Artikel 21 NIS-2-Richtlinie eine Reihe von technischen, operativen und organisatorischen Maßnahmen umsetzen, um die IT und Netzwerke ihrer kritischen Dienstleistungen zu schützen. Bei der Auswahl und Umsetzung der Maßnahmen sollen Betreiber einen Allgefahrenansatz ("All-Hazards-Approach") einsetzen. Sie müssen zudem die zuständige nationale Behörde unverzüglich über signifikante Störungen, Vorfälle und Cyberbedrohungen ihrer Dienstleistungen unterrichten, gegebenenfalls auch die Empfänger (Kunden) ihrer Dienstleistungen.

² Nach Kenntnis der Landesregierung fasst der Bund darunter die Bundesministerien und das Bundeskanzleramt.

3. Mit welchen Kosten, welchem Personalaufwand und welchen sonstigen Folgen rechnet die Landesregierung für die Umsetzung der NIS-2-Richtlinie in Thüringen insgesamt (bitte getrennt nach privaten Unternehmen, Behörden und Ministerien des Landes sowie kommunalen Verwaltungen inklusive Zweckverbänden und Eigenbetrieben angeben)?

Antwort:

Mangels Vorliegens eines Gesetzentwurfs des Bundes ist derzeit nicht bekannt, welche Maßnahmen und Anforderungen die betroffenen Einrichtungen jeweils treffen müssen. Deshalb ist es der Landesregierung nicht möglich, die Kosten, den Personalaufwand oder die sonstigen Folgen für private Unternehmen und Betriebe in kommunaler oder Landesträgerschaft abzuschätzen.

Der zu erwartende Erfüllungsaufwand für die öffentliche Verwaltung kann derzeit noch nicht eingeschätzt werden. Aktuell werden die Anforderungen an ein einheitliches Informationssicherheitsniveau innerhalb der Thüringer Landesverwaltung über Verwaltungsvorschriften, Richtlinien und Konzepte geregelt. Vorgesehen ist eine Anpassung dieser Regelungen an die Anforderungen der NIS-2-Richtlinie. Gegebenenfalls sind durch die Änderung des BSI-Gesetzes mit dem oben angegebenen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz weitere Erfüllungsaufwände zu erwarten.

4. Welche Landes- sowie kommunalen Unternehmen und Behörden werden in Thüringen voraussichtlich welche Maßnahmen der NIS-2-Richtlinie umsetzen müssen?

Antwort:

Welche Unternehmen in kommunaler oder Landesträgerschaft vom Anwendungsbereich der NIS-2-Richtlinie betroffen sein werden, steht noch nicht fest. Die Bestimmung hängt auch von dem ausstehenden Gesetzentwurf des Bundes ab.

Gemäß Artikel 2 Abs. 2 Buchst. f Doppelbuchst ii der Richtlinie sind Einrichtungen der öffentlichen Verwaltung auf der regionalen Ebene nur dann betroffen, wenn sie nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnten. Hierzu wird das durch den IT-Planungsrat beschlossene Identifizierungskonzept der Länder zur Umsetzung der NIS-2-Richtlinie Anwendung finden. Eine konkrete Angabe ist noch nicht abschließend möglich. Aktuell ist davon auszugehen, dass alle obersten Landesbehörden durch die NIS-2-Richtlinie erfasst werden.

Zentraler Bestandteil bei der Umsetzung der NIS-2-Richtlinie stellen hierbei die Mindestsicherheitsanforderungen des Artikel 21 Abs. 2 NIS-2-Richtlinie (Risikomanagementmaßnahmen im Bereich der Cybersicherheit) dar.

5. In welcher Form plant die Landesregierung, die betroffenen Unternehmen und Behörden bei der Umsetzung der NIS-2-Richtlinie zu unterstützen?

Antwort:

Ob etwaige Anpassungen der Unternehmen mit den Fördertatbeständen der Thüringer Förderprogramme kompatibel sind (beispielsweise durch investive Maßnahmen von förderfähigen Unternehmen) kann derzeit nicht bewertet werden. Eine direkte, auf den Sachverhalt bezogene Förderung ist indes derzeit durch die Landesregierung nicht intendiert.

6. Wie viele Cyberangriffe gab es in den letzten fünf Jahren in Thüringen auf kommunale Behörden, Landesbehörden und kommunale Unternehmen (bitte in Jahresscheiben aufführen)?

Antwort:

Zum Begriff des Cyberangriffs wird auf die Antwort der Landesregierung vom 2. Mai 2021 (Drucksache 7/3277) zur Frage 1 der Kleinen Anfrage 7/1798 vom 17. Februar 2021 des Abgeordneten Prof. Dr. Voigt (CDU) Bezug genommen.

Die nachfolgend aufgelisteten Cyberangriffe beruhen auf Informationen über die das ThüringenCERT informiert wurde.

Jahr	Landesbehörden	kommunale Behörden
2018	2	-
2019	8	-
2020	6	-
2021	7	1
2022	11	1
2023	14	1

(Stand 8. Februar 2024)

Das ThüringenCERT ist dabei vorrangig für die Landesbehörden zuständig. Informationen über Cyberangriffe auf kommunale Behörden und Unternehmen sind nicht vollständig und beruhen auf den gemeldeten Sachverhalten.

7. Sofern es in den letzten fünf Jahren erfolgreiche Cyberangriffe auf kommunale Behörden, Landesbehörden und kommunale Unternehmen gegeben hat, welche Leistungen und Angebote mussten wie lange eingeschränkt werden oder konnten nicht angeboten werden (bitte getrennt nach Behörden, Ministerien des Landes und kommunalen Verwaltungen inklusive Zweckverbänden und Eigenbetrieben angeben)?

Antwort:

Die Cyberangriffe auf Landesbehörden führten zu Ausfällen von deutlich unter einem Tag bis zu mehreren Tagen. Eine Auflistung von konkret betroffenen Leistungen oder Angeboten ist nicht möglich, da diese statistisch nicht erfasst werden. Aussagen zu kommunalen Verwaltungen oder Unternehmen in kommunaler Trägerschaft sind der Landesregierung nicht möglich.

Maier
Minister