oesterreichs energie.

GENERALSEKRETARIAT

Europäische Kommission
Have Your Say
Cybersicherheitsrisikomanagement und
Berichtspflichten für digitale Infrastrukturen,
Anbieter und IKT-Servicemanager
Online über: https://have-your-say.ec.europa.eu/

Kontakt	DW	Unser Zeichen	Ihr Zeichen	Datum
DI Armin Selhofer	232	ARS/DM – 10/2024		18.07.2024

Stellungnahme zum Entwurf der NIS2-Durchführungsverordnung Cybersicherheitsrisikomanagement und Berichtspflichten für digitale Infrastrukturen, Anbieter und IKT-Servicemanager

Sehr geehrte Damen und Herren!

wir bedanken uns für die Möglichkeit zum aktuellen Entwurf der NIS2-Durchführungsverordnung Cybersicherheitsrisikomanagement und Berichtspflichten für digitale Infrastrukturen, Anbieter und IKT-Servicemanager Stellung nehmen zu können.
Wir begrüßen, dass mit diesem Dokument die Vorgaben aus NIS2 für digitale Infrastrukturen, Anbieter und IKT-Servicemanager konkretisiert werden.

Allgemein
Der vorliegende Entwurf der NIS2-Durchführungsverordnung richtet sich allgemein an digitale Diensteanbieter. In der Verordnung wird jedoch nicht ausreichend zwischen Drittanbietern (vgl. Annex 1 NIS-2-RL Z 8 und 9) oder konzerninternen IKT-Dienstleistern differenziert.

In vielen Konzernen, so auch im Energiebereich, werden Installation, Verwaltung, Betrieb und Wartung von IKT-Produkten, IKT-Netzen und entsprechende IKT-Anwendungen von einer konzerninternen Servicegesellschaft übernommen. Diese internen Dienstleister erbringen ihre Dienstleistungen innerhalb des Konzerns und fallen damit gemäß NIS2-Richtlinie unter die Kategorie der Anbieter verwalteter Dienste (und häufig auch verwalteter Sicherheitsdienste). Die vorliegende Durchführungsverordnung beträfe sie daher uneingeschränkt.
In Hinblick auf die Meldepflichten und die Risikomanagementmaßnahmen erscheint es uns als überschießend, dass dieselben strengen Vorgaben für konzerninterne Dienstleistungen

Österreichs E-Wirtschaft
Brahmsplatz 3 Tel +43 1 501 98-0 info@oesterreichsenergie.at
1040 Wien Fax +43 1 501 98-900 www.oesterreichsenergie.at

DVR 0422100, UID ATU37583307, ZVR 064107101; Raiffeisenlandesbank Niederösterreich-Wien AG, SWIFT/BIC: RLNWATWW, IBAN: AT12 3200 0000 1264 4787

wie für Dritte gelten sollten. Oft werden konzerninterne IT-Dienste (z.B. Fuhrparkmanagement, Essensausgabe) erbracht, die am freien Markt nicht verfügbar sind und keinen Einfluss auf den Endkundenmarkt haben. Diese Dienste sollten unserer Ansicht nach von den strengen Risikomanagementmaßnahmen und Meldepflichten ausgenommen sein. Wir plädieren daher stark dafür, zwischen konzerninternen und externen Dienstleistungen zu unterscheiden.

Interne Dienstleister, die bereits im Rahmen der Leistungserbringung für wesentliche und wichtige Einrichtungen im Sektor Energie im Anwendungsbereich der nationalen NIS-Anforderungen erfasst sind, könnten auf Grund der vorliegenden Durchführungsverordnung doppelten Anforderungen unterliegen. Eine solche Doppelverpflichtung führt ausschließlich zur Erhöhung der Komplexität der Anforderungen innerhalb der betroffenen Unternehmen und erhöht nicht die Sicherheit der Netz- und Informationssysteme. Daher empfehlen wir die oben angesprochenen internen Dienstleister von dieser Durchführungsverordnung auszunehmen.

Wir regen daher als Klarstellung an, dass konzerninterne Dienstleister anderer NIS-Sektoren als der in Annex 1 NIS-2-RL Z 8 und 9 gelistet, explizit von dieser Durchführungsverordnung ausgenommen werden.

Zu Artikel 10
Zu Artikel 10 lit a)
Gemäß Artikel 10 lit a) gilt ein Sicherheitsvorfall als signifikant, wenn einer oder mehrere der verwalteten Dienste oder verwalteten Sicherheitsdienste länger als 10 Minuten gar nicht verfügbar sind. Gemäß obigen Ausführungen werden diese Dienste in Energiekonzernen zumeist rein intern im selben Konzern erbracht. Ein Ausfall von länger als 10 Minuten kann hier durchaus vorkommen, ohne merkliche Auswirkung auf die Endkunden. Die Regelung ist unscharf, da sie nicht auf eine vorsätzliche oder böswillige (externe) Handlung abzielt. Die Meldepflicht für einen solchen (internen) Ausfall (z.B. Netzwerk oder einzelne Dienste) stellt einen großen administrativen Aufwand dar, betrifft aber unter Umständen gar nicht die Endkunden des Konzerns (Energiekunden). Eine solche Meldung wäre überschießend, siehe obige Ausführungen zu den rein internen Diensten.
Wir regen an, diese Bestimmung entweder ganz zu streichen oder zumindest auf die Gegebenheiten hin anzupassen: Meldepflicht nur, wenn ein bestimmter Prozentsatz an Endkunden des Konzerns betroffen ist.

Zu Artikel 10 lit e)
Nach Artikel 10 lit e) liegt ein signifikanter Sicherheitsvorfall vor, wenn die Integrität, Vertraulichkeit oder Authentizität der gespeicherten, übermittelten oder verarbeiteten Daten im Zusammenhang mit der Bereitstellung des verwalteten Dienstes oder des verwalteten Sicherheitsdienstes beeinträchtigt ist, wobei dies Auswirkungen auf mehr als 5 % der Nutzer des verwalteten Dienstes oder des verwalteten Sicherheitsdienstes in der Union hat.

Im Hinblick auf diese Bestimmung und die einleitenden Ausführungen ist eine klare Unterscheidung zwischen konzerninternen und externen Diensten erforderlich. Unser Verständnis ist, dass diese Vorgabe nicht für Dienste gilt, die innerhalb des Konzerns

erbracht werden. Andernfalls stellt sich die Frage, wer bei konzerninternen Diensten die „Nutzer“ wären – das Personal der Konzerngesellschaften oder die Konzerngesellschaften selbst?
Die Intention dieser Bestimmung ergibt nur bei großen IT-Dienstleistern, welche ihre Dienste am freien Markt anbieten, einen Sinn und sollte entsprechend diesem Anwendungsfall präzisiert und klarer formuliert werden.
Durch eine klare Differenzierung kann sichergestellt werden, dass die regulatorischen Anforderungen zielgerichtet und verhältnismäßig bleiben, ohne unnötige Belastungen für konzerninterne Dienstleister zu schaffen, die keinen direkten Einfluss auf wesentliche bzw. wichtige Einrichtungen haben.

Wir danken für die Kenntnisnahme der Anliegen von Österreichs E-Wirtschaft und ersuchen um deren Berücksichtigung.

Mit freundlichen Grüßen

Mag. Dr. Michael Strugl
Präsident

Dr. Barbara Schmidt
Generalsekretärin

Über Oesterreichs Energie
Oesterreichs Energie ist die Interessenvertretung der österreichischen E-Wirtschaft. Im Auftrag seiner rund 140 Mitgliedsunternehmen vertritt der Verband im Sinne einer sicheren, sauberen und leistbaren Energiezukunft die Brancheninteressen gegenüber Politik, Verwaltung und Öffentlichkeit. Als erste Anlaufstelle zum Thema Energie arbeitet Oesterreichs Energie eng mit politischen Institutionen, Behörden sowie anderen Verbänden zusammen und bringt seine Expertise lösungsorientiert und kundenzentriert in laufende Debatten ein.