WIRTSCHAFTSKAMMER ÖSTERREICH

An das
Bundeskanzleramt
z Hdn Herrn Gruppenleiter
Erich Albrechtowitz
Ballhausplatz 2
1010 Wien

per E-Mail: NIS@bka.gv.at

Abteilung für Rechtspolitik
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900DW | F 05 90 900
E rp@wko.at
W wko.at/rp

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
COM (2020) 823 final	Rp 487.0001/2021/WP/Zl Dr. Winfried Pöcherstorfer	4002	11.05.2021

EU-Cybersicherheitsstrategie und Vorschlag für eine NIS 2-RL - Stellungnahme

Sehr geehrter Herr Gruppenleiter,

die Wirtschaftskammer erlaubt sich, zur EU-Cybersicherheitsstrategie und insbesondere zum Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (fortan kurz: NIS 2-RL) folgende Stellungnahme abzugeben:

I. Allgemeines

Wir befürworten das Ansinnen der Europäischen Kommission, die digitale Zukunft der EU aktiv zu unterstützen und die Abwehrfähigkeit der EU gegen Cyberbedrohungen zu stärken.

Insbesondere begrüßen wir den Umstand, dass im Rahmen der EU-Cybersecurity Strategie speziell für KMU Investitionen in Höhe von EUR 4,5 Mrd EUR in Aussicht gestellt werden und halten dies auch für dringend erforderlich, um die europäische Wirtschaft cybersicher machen zu können.

Auch die gezielte Unterstützung der heimischen und der europäischen Wirtschaft, wenn es darum geht, eigene Cybersicherheitslösungen zu entwickeln, um die Abhängigkeit von außereuropäischen Anbietern im Technologiebereich langfristig zu durchbrechen, erscheint uns wesentlich. Dafür sollten entsprechende Maßnahmen gesetzt werden, wie beispielsweise gezielte Investitionen durch staatliche Abnehmer, Exportförderung, Forschungsförderung mit Vertriebsaussicht, Förderung von Kooperationen.

Ferner ist positiv anzuführen, dass Lehren aus der Umsetzung der bestehenden NIS-RL gezogen werden und in diesem Sinne klare Regelungen für EU-weiten Informationsaustausch geschaffen werden und eine EU-weite Harmonisierung erfolgen soll.

Allerdings erscheint uns die Ausweitung des Anwendungsbereiches der geplanten Richtlinie – ungeachtet der Bedeutung von Cybersicherheit für die Wirtschaft – eindeutig zu weitreichend.

Anstatt mittlere und unter bestimmten Voraussetzungen auch kleine Unternehmen in die Verpflichtungen der künftigen Richtlinie mit einzubeziehen, sollten stattdessen mittlere Unternehmen (solche mit weniger als 250 Mitarbeitern, einem Jahresumsatz bis 50 Mio EUR oder einer Jahresbilanzsumme bis 43 Mio EUR) grundsätzlich ausgenommen sein und nur, sofern es besondere Umstände rechtfertigen, in die Verpflichtungen der Richtlinie einbezogen werden können. Ferner sollten in solchen Fällen die zu treffenden Sicherheitsmaßnahmen beschränkt und die Frist für Meldungen von Sicherheitsvorfällen verlängert werden. Kleine Unternehmen und Kleinstunternehmen sollen generell vom Anwendungsbereich der Richtlinie ausgenommen werden.

Vor diesem Hintergrund sollte die vorgeschlagene Ausweitung des Anwendungsbereichs nur Unternehmen von systemischer Relevanz umfassen, wobei die Versorgungskritikalität maßgeblich bei der Definition eines wesentlichen oder wichtigen Unternehmens auf nationaler Ebene sein sollte.

Des Weiteren muss darauf Bedacht genommen werden, dass die österreichische Wirtschaft etwas mehr als zwei Jahre nach Inkrafttreten der Umsetzung der ersten NIS-RL durch das NISG nicht damit konfrontiert wird, erst vor kurzer Zeit implementierte Systeme und Maßnahmen schon nach kurzer Zeit wieder umstellen zu müssen.

Darüber hinaus gilt es auch sicherzustellen, dass gegenüber anderen thematisch verwandten Rechtsvorschriften Abgrenzungen klar und eindeutig vorgenommen werden, wie zB dem Digital Operational Resilience Act (DORA) im Finanzsektor, dem TKG oder auch dem zeitgleich mit dem vorliegenden RL-Vorschlag präsentierten Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen COM (2020) 829 final vom 16.12.2020. Hier gilt es Rechtssicherheit zu schaffen und Doppelzuständigkeiten von Behörden und mehrfache, womöglich divergierende (Melde-) Verpflichtungen zu vermeiden.

Der Umstand, dass beispielsweise im wichtigen Bereich der Anbieter öffentlicher Kommunikationsdienste offenbar nur mehr eine einzige Behörde für alle Themen zuständig sein soll, ist positiv zu bewerten. Dies wäre eine deutliche bürokratische Erleichterung für die betroffenen Unternehmen.

Leitlinie sollte generell sein, die Cybersicherheit zu stärken – ohne dabei zusätzlichen bürokratischen Mehraufwand zu schaffen, der die Unternehmen unnötig belastet. Es sollte daher dahingehend eine Empfehlung geben, dass im Fall einer gesetzlichen sektorspezifischen Regelung nur die sektorspezifische Behörde zuständig ist und diese als Ansprechstelle für die andere NIS-Behörde fungiert.

Aktuell besteht die Problematik für Telekommunikationsunternehmen durch das Anbieten eines DNS-Dienstes, einer nativen Serviceleistung eines Anbieters von Internetdiensten, dass Betreiber sich Prüfungen durch zwei unterschiedliche Behörden unterziehen müssen. Das gleiche trifft für die Meldepflicht bei Störungen und Ausfällen zu.

In der neuen Richtlinie sollte zumindest eine gesetzliche Möglichkeit und Empfehlung enthalten sein, dass eine einzige Behörde zu bevorzugen wäre und diese Rollen (Überprüfungen, Meldestelle) auch ausüben darf.

II. Im Detail

Zu Art 1, 2 sowie Anhang I und II (Anwendungsbereich)

Der Anwendungsbereich soll gegenüber der ursprünglichen NIS-RL signifikant ausgeweitet werden. Dies wird dazu führen, dass zusätzlich zu dem bislang recht eingeschränkten Adressatenkreis - per Bescheid festgestellte Betreiber wesentlicher Dienste und ex lege verpflichtete Anbieter digitaler Dienste - eine Vielzahl weiterer heimischer Unternehmen als ex lege Verpflichtete in den Anwendungsbereich fallen soll.

Unabhängig davon ist eine klare Abgrenzung entscheidend, damit die Rechtsanwender erkennen können, ob sie Adressaten der Bestimmungen sind.

Besonders problematisch ist, dass bestimmte Kategorien von Unternehmen unabhängig von der Größe Adressaten der Richtlinie sein sollen:

Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn

a) die Dienste von einer der folgenden Einrichtungen erbracht werden:

- öffentliche elektronische Kommunikationsdienste
- Vertrauensdiensteanbieter
- top-level domain name registries and DNS service providers
- einziger Anbieter eines MS
- Auswirkung auf öffentliche Ordnung/Sicherheit/Gesundheit möglich
- Systemrisiken möglich
- kritische Einrichtung.

Typischerweise ist das Risiko bei Kleinst- und Kleinunternehmen sehr begrenzt, die generelle Normunterworfenheit unter die RL ist daher strikt abzulehnen. So würde es am Beispiel von DNS-Diensteanbietern Sinn machen, diese erst ab einer gewissen Größe (zB abhängig von einer gewissen Anzahl von Domains, die verwaltet werden) unter den Anwendungsbereich fallen zu lassen.

Allein für die Bereiche Kommunikationsdienste und Kommunikationsnetze gehen wir hier von einer Betroffenheit hunderter Unternehmen aus (das Firmen A-Z der WKO weist hier bereits 189 Kommunikationsdienste und 458 Kommunikationsnetze aus, die sich freiwillig eingetragen haben). Darunter finden sich viele Unternehmen, die nur regional oder anderweitig sehr eingeschränkt tätig sind und insofern keine Relevanz für die Vorgaben der RL haben.

Die vorgeschriebenen Maßnahmen und Meldepflichten für Klein- und Kleinstunternehmen im selben Ausmaß wie für mittlere und große Unternehmen vorzuschreiben, erscheint unverhältnismäßig. Klein und Kleinstunternehmen sind mit den umfangreichen Verpflichtungen (zB einer defacto 24/7-Bereitschaft aufgrund der 24 Stunden Meldefrist) der Richtlinie überfordert. Die Vorgaben bedeuten eine hohe organisatorische und finanzielle Belastung für die Unternehmen, die für kleinstrukturierte Unternehmen nicht leistbar ist und zu einer zusätzlichen „Ausdünnung“ regionaler Betriebe führen würde. Dies wäre neben gesamtwirtschaftlichen

Überlegungen (Erhaltung von Arbeitsplätzen, etc) auch im Widerspruch zum Anliegen der EU auf heimische Anbieter zu setzen, um die Abhängigkeit von Anbietern in Drittstaaten zu reduzieren. Wir fordern daher, wie bereits eingangs dargelegt, dringend, Klein- und Kleinstunternehmen generell aus dem Anwendungsbereich auszunehmen.

Mit Blick auf Mischbetriebe ist sicherzustellen, dass Unternehmen nur dann in den Anwendungsbereich fallen, wenn sie die Größenschwelle mit den im Anhang genannten Sektorentätigkeiten erreichen.

Soweit aus dem Text zu erkennen ist, fallen die Unternehmen ex lege in den Anwendungsbereich. Die MS haben aber bei den Einrichtung gemäß Art 2 Abs 2 lit b bis f eine Liste zu erstellen und der Kommission binnen 6 Monaten zu übermitteln. Wie die Umsetzung hier erfolgen soll, ist gänzlich offen.

Es wird als positiv angesehen, dass mit NIS 2 nun auch der öffentliche Bereich im selben Maße betroffen ist, da zur Erreichung der Ziele Anstrengungen im öffentlichen und privaten Bereich und eine damit einhergehende Bewusstseinsbildung erforderlich ist.

Zu Anhang I Z 2 lit b (Schienenverkehr)

Wir sind der Ansicht, dass die derzeit geltenden bzw angewendeten Sicherheitsmaßnahmen im Bereich der Cybersicherheit für den Eisenbahnbereich ausreichend sind. Die im Entwurf der NIS 2-RL angestrebten Ziele würden vor allem kleinere, aber auch mittlere Unternehmen finanziell und organisatorisch überproportional belasten. Daher sollte auf jeden Fall eine Ausweitung der Ausnahmen auch auf mittlere Unternehmen im oben beschriebenen Sinne angestrebt werden. Laut Anhang I (wesentliche Einrichtungen) sollen all jene Eisenbahnunternehmen unter NIS 2 fallen, die eine Sicherheitsgenehmigung oder Sicherheitsbescheinigung haben. Dazu gehören jedoch auch Betreiber von örtlichen bzw regionalen Eisenbahninfrastrukturen, die für das Funktionieren des Schienenverkehrsmarktes nicht von strategischer Bedeutung sind (Art 4 Abs 2 RL 2012/34/EU), weshalb diese nicht als „wesentliche Einrichtung“ iSd Anhangs I Z 2 lit b des NIS 2-RLV einzuordnen wären.

Zusätzlich schlagen wir vor, dass im Anhang I Z 2 lit b eine Ausnahme für Eisenbahninfrastrukturunternehmen (EIU), die entsprechend Art 2 Abs 4 RL 2012/34/EU für das Funktionieren des Schienenverkehrsmarktes als nicht von strategischer Bedeutung eingestuft wurden, vorgesehen werden sollte.

Diese Argumentation sollte auch auf die übrigen Branchen des Anhang 1 und 2 übertragen werden.

Darüber hinaus sollte im Anhang I Z 2 lit b klargestellt werden, dass NIS 2 nicht für jene Eisenbahninfrastrukturunternehmen und Eisenbahnverkehrsunternehmen (EVU) gilt, die von den Bestimmungen der RL 2012/34/EU schon aufgrund der RL 2012/34/EU selbst oder aufgrund einer entsprechenden Ermächtigung durch nationales Recht ausgenommen sind (wie zB nicht vernetzte Bahnen, Anschlussbahnen).

Zu Anhang I Z 8 (Digitale Infrastruktur)

Nach geltender Rechtslage unterliegt die Telekommunikationsbranche gemäß § 20 NISG iVm § 10 Abs 3 NISV aufgrund der für geltenden spezielleren Normen des TKG nicht den Verpflichtungen nach § 17 und § 19 NISG (Sicherheitsvorkehrungen und Meldepflichten), sondern jenen des TKG.

Hier wurde von Art 1 Abs 7 der NIS 1 Richtlinie Gebrauch gemacht, wonach, wo es sektorspezifische Rechtsakte zur Sicherheit der Netz- und Informationssysteme oder der Meldung von Sicherheitsvorfällen gibt, die mindestens gleichwertig sind, diese gelten und nicht jene der Richtline. Nun werden im TKG 2021 über den EECC sogar neue, umfangreichere sektorspezifische Security-Regelungen für die Branche eingeführt. Dass diese nun, nach voraussichtlich kurzer Geltungsdauer, durch allgemeinere, nicht sektorspezifische, Regelungen der NIS 2 Richtlinie ersetzt werden sollen, wird klar abgelehnt, da dies lediglich zu mehr Bürokratie nicht aber zu mehr Sicherheit führen würde.

Zu Anhang II Z 1 (Post- und Kurierdienste)

Wie in ErwG 41 ausgeführt, sollten die Anforderungen an das Cybersicherheitsrisikomanagement in einem angemessenen Verhältnis zu den Risiken stehen. Die Risiken, die bei wichtigen Einrichtungen entstehen, unterscheiden sich deutlich von jenen, die von einem Ausfall der Dienstleistungen der wesentlichen Einrichtungen ausgehen.

Generell umfasst der vorliegende Vorschlag sämtliche IKT-Systeme, die bei Post- und Kurierdiensten im Einsatz sind. Grundsätzlich sollte indes klar zwischen den unterschiedlichen internen Systemen unterschieden werden. Mit Blick auf die Zielsetzung, Versorgungsstörungen durch Cyberangriffe zu vermeiden, erscheint es ausreichend, nur jene IT-Systeme in Betracht zu ziehen, die für die Erbringung der Dienstleistung unerlässlich sind.

Im Falle von Post- und Kurierdiensten lässt sich der grundlegende Betrieb - also die Dienstleistung als Paketdienst - auch analog erbringen. Bei Wegfall der begleitenden IT-Unterstützung könnte die operative Abwicklung – wenngleich unter Inkaufnahme von Ineffizienzen und reduzierter Convenience – weiter aufrechterhalten werden. Wir empfehlen daher, den Wirkungsbereich der Richtlinie auf jene IT-Systeme zu beschränken, deren Ausfall die Leistungserbringung gänzlich verunmöglichen würde.

Konkret ist es verhältnismäßig einfach, die Kernkomponenten, die den Paketumschlag und die Paketzustellung unterstützen, abzusichern. Diese Systeme sind nur intern erreichbar und lassen sich problemlos nach außen abschirmen. Andere Systeme, die für den operativen Ablauf verzichtbar sind und beispielsweise als zusätzliche Serviceleistung oder als Erweiterung der Dienstleistung für die Kunden zur Verfügung stehen, sind entsprechend schwerer abzusichern. Um eben für Kunden erreichbar zu sein, muss eine Website oder ein Server definierte Zugriffe aus dem Internet zulassen. Hier können leicht Sicherheitslücken entstehen und ausgenützt werden. Erfolgt ein Cyberangriff auf eine solche Komponente, beeinträchtigt das die Erbringung der Dienstleistung aber nicht. Lediglich der Komfort für die Kunden und die Paketempfänger wird reduziert.

Ist die Erbringung der Dienstleistung auch dann möglich, wenn ein IKT-System ausfällt, so sollte dieses System auch nicht von der Richtlinie berücksichtigt werden. Ist der Pakettransport auch analog möglich und lässt sich das mit entsprechenden Notfallkonzepten und Ablaufbeschreibungen belegen, sollte das aus unserer Sicht ausreichend sein. Sind die Auswirkungen eines Cyberangriffs auf ein IKT-System für die Empfänger der Dienstleistung nicht spürbar, sollte die Richtlinie für dieses IKT-System keine Anwendung finden.

Zu Anhang II Z 2 (Abfallbewirtschaftung)

Wir fordern die Streichung der Abfallbewirtschaftung aus Anhang II. Die Betriebe der öffentlichen und der privaten Abfallwirtschaft sind im Bereich der Daseinsvorsorge tätig. Sie helfen dabei, die Abfälle der Bevölkerung und der Wirtschaft zu sammeln und einer entsprechenden Behandlung zuzuführen. Im Bereich der Abfallbewirtschaftung führen

Cybersicherheitsvorfälle aber weder zu Sammlungs- noch zu Behandlungsengpässen und führen insofern zu keinen negativen Auswirkungen für die Allgemeinheit.

Selbst wenn die IT in einem Abfallsammlungsbetrieb, der die Müllabfuhr von Haushalten durchführt, ausfällt, hat dies keine Auswirkungen auf die Durchführung der Abfallsammlung. Die Betriebe haben sowohl die Abfuhrordnungen der Gemeinden, für die sie tätig sind, als auch die Dienstpläne für die Belegschaft immer zusätzlich in Papierform, sodass keine zeitkritische Abhängigkeit von IT-Systemen besteht.

Sollten überraschend Aufträge bei einem Abfallsammelbetrieb eingehen, so werden diese in der Regel ohnehin telefonisch abgewickelt. Der Disponent weist auch den Fahrer des Abfallsammelfahrzeuges telefonisch an, zu diesem oder jenem Ort zu fahren, um die Abfälle einzusammeln. Auch hier wird kein Computer benötigt. Somit ist die Einbeziehung der Abfallwirtschaft für diesen Bereich nicht notwendig.

Wird die IT in einem Abfallbehandlungsbetrieb lahmgelegt, sodass es zu einem Ausfall der Behandlungsanlage (zB einer Sortieranlage) kommt, so hat dies unmittelbar keine großen Auswirkungen. Speziell mittlere oder größere Abfallbehandlungsanlagen verfügen über entsprechend große Lagerflächen. Eine „just in time-“Abfallbehandlung ohne Lagerflächen ist ohnehin nicht möglich.

Sollte auf Grund der Cyberattacke der Abfallbehandlungsbetrieb längere Zeit stillstehen, sodass die Lager langsam voll werden, so wird sich der Unternehmer alternative Entsorgungsmöglichkeiten bei einem anderen Abfallbehandler suchen, wobei Österreich über ein hervorragendes Netz an Abfallbehandlungsanlagen verfügt (www.bundesabfallwirtschaftsplan.at).

In der Praxis kam es bereits vor, dass Behandlungsbetriebe aufgrund von Bränden durch falsch entsorgte Lithiumbatterien für längere Zeit ausfielen. Obwohl durchaus auch größere Betriebsanlagen längere Zeit stillgestanden sind, kam es zu keinerlei Entsorgungsengpässen, da die betroffenen Unternehmer immer alternative Entsorgungswege finden konnten. Auch bei einer Cyberattacke auf eine Deponie passiert übrigens mehr oder weniger gar nichts. Lediglich die Brückenwaage könnte außer Funktion gesetzt werden. Die tatsächliche Entsorgungstätigkeit (das Abkippen des Abfalls auf der Deponie) ist unabhängig von einem Computersystem.
Da im Bereich der Abfallbewirtschaftung bei Sicherheitsvorfällen keine negativen Auswirkungen auf Dritte zu befürchten sind, ist dieser Sektor vom NIS 2-Regime auszunehmen.

Zu Anhang II Z 4 (Produktion, Verarbeitung und Vertrieb von Lebensmitteln)

Der österreichische Lebensmittelsektor setzt bereits jetzt im eigenen Interesse umfassende Maßnahmen für seine IT-Sicherheit und spricht sich gegen den bürokratischen und verwaltungstechnischen Mehraufwand aus, den eine Einbettung in den Geltungsbereich der NIS 2-RL mit sich bringen würde.

Zu Art 4 Z 21 (Definitionen)

Wir gehen davon aus, dass unter „content delivery network“ TV broadcasting nicht umfasst ist.

Zu Art 5 (Nationale Cybersicherheitsstrategie)

Gemäß Art 5 Abs 2 lit a müssen Mitgliedstaaten Maßnahmen hinsichtlich der Cybersicherheitsstrategie in der Lieferkette von IKT-Produkten und Services treffen, die wesentliche oder wichtige Einrichtungen bei der Bereitstellung ihrer Dienste nutzen. Während hier nicht klar ist, ob eine EU-Harmonisierung der Anforderung getroffen wird, sollte jedenfalls sichergestellt werden, dass im Sinne einer ausgewogenen Haftungsverteilung Hersteller von Hardware und Software bzw Anbieter von IKT Produkten/Systemen für die kritischen Infrastrukturen in die Regelungen miteinbezogen werden.

Zu Art 14 (EU-CyCLON)

Die Aufgaben und die Rollen der „EU-CyCLON“ sind aus unserer Sicht unklar, da die ENISA bereits viele Themen abdeckt und die neue „Communications Group“ die Kommunikation koordinieren soll.

Zu Art 18 Abs 2 lit d (Risikomanagementmaßnahmen)

Die Sicherheit der gesamten Lieferkette sicherzustellen und das Einstehen Müssen für Defizite in der gesamten Lieferkette, erscheint jedenfalls im KMU-Bereich unverhältnismäßig.

Zu Art 18 Abs 2 lit g (Risikomanagementmaßnahmen)

Kryptographie und Verschlüsselung sind sinnvolle und wichtige Maßnahmen. Dies gilt allerdings nicht uneingeschränkt in allen Bereichen. Teils ist es nicht notwendig, teils aus rechtlichen oder technischen Gründen nicht durchführbar.

Die Nennung von Kryptographie und Verschlüsselung als Mindestmaßnahmen wird daher abgelehnt.

Angelehnt an Art 32 DSGVO könnten wir uns eine Formulierung wie folgt vorstellen:
„Einsatz von Kryptographie und Verschlüsselung unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos“.

Zu Art 19 (EU-weit koordinierte Risikobewertungen kritischer Lieferketten)

Die koordinierte Risikobewertung der Sicherheit von Lieferketten von IKT Prozessen bei wichtigen Einrichtungen kann einen unverhältnismäßig hohen Verwaltungsaufwand bei Lieferanten der IKT-Systeme mit sich bringen. Außerdem muss klargestellt werden, dass die Lieferung von IKT-Dienstleistungen und nicht die physische Lieferung bewertet werden soll. Andernfalls wären Post- und Kurierdienstleister ebenfalls von dieser Risikobewertung betroffen.

Zu Art 19 und 21 (Risikobewertungen kritischer Lieferketten und Nutzung europäischer Systeme für Cybersicherheitszertifizierung)

Die in Artikel 19 und 21 vorgesehenen weitreichenden Maßnahmen gegenüber Herstellern können zu massiven betrieblichen Auswirkungen bei Betreibern von Kommunikationsnetzen und -diensten führen. Wir fordern daher:

- Die dringend notwendige Berücksichtigung von Übergangszeiten von bis zu 4 Jahren,
- die Möglichkeit des Bezuges von Patches und Updates für den sicheren Betrieb von Seiten des Herstellers,
- eine Abstufung der Maßnahmen und Erläuterung dieser, so dass klar ist, welche Rolle nicht zertifizierte ICT-Lieferanten haben (erhöhte Sicherheitsanforderungen, Unzulässigkeit, etc),
- Erleichterungen beim Einsatz zertifizierter Lieferanten nach Art 21 bei der NIS-Prüfung (zB kein zusätzliches Screening bei einer Überprüfung der Netzsicherheit),
- ein Anreizsystem; konkrete Anreize sollten bereits in der RL angesprochen werden und würden wohl national umgesetzt werden (zB steuerliche Vorteile für den Einsatz von ICT-zertifiziertem Equipment).

Zu Art 20 (Meldepflichten)

Eine Meldung an die Empfänger der Dienstleistungen ist für Anbieter von Post- und Kurierdiensten nicht durchführbar. Es sind dort keine durchgängigen Kontaktdaten aller Paketempfänger und durch die Organisation auch keine durchgängigen Daten zu allen Absendern verfügbar. Der Aufwand für eine Meldung an alle bekannten Kontakte erscheint außerdem unverhältnismäßig. Die Formulierung entspricht in dieser Form wohl nicht dem eigentlichen Ziel der Reglung.

In Abs 3 wird definiert, dass ein Sicherheitsvorfall auch dann erheblich ist, wenn (Buchstabe b) andere natürliche und juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt werden. Gemäß § 57 Buchstabe d der Allgemeinen Österreichischen Spediteurbedingungen ist die Haftung des Spediteurs für unmittelbare und mittelbare Folgen jedes unverschuldeten Ereignisses ausgeschlossen. Da die materiellen und immateriellen Folgen einer nicht oder verspätet zugestellten Sendung nicht abgeschätzt werden können, lehnen wir diesen Passus in der bestehenden Form ab. Wir empfehlen eine Einschränkung, oder Präzisierung.

Die in Abs 4 Buchstabe a angeführte Frist von 24 Stunden bedeuten einen immensen administrativen Aufwand. Es muss bedacht werden, dass im Fall eines Sicherheitsvorfalls zusätzliche Ressourcen für die Abwehr und die Behebung etwaiger Schäden gebunden sind. Wir empfehlen aus diesen Gründen eine Verlängerung der Frist.

Weiters erscheint die Bezeichnung als Abschlussbericht in Abs 4 Buchstabe c unzutreffend. Dauern die Recherche und Umsetzung der Maßnahmen länger als einen Monat, dann kann zu diesem Zeitpunkt lediglich ein Zwischenbericht abgegeben werden.

Zu Art 20 Abs 4 (Meldepflichten)

Die Einrichtungen müssen unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls eine erste Meldung übermitteln.

Obgleich es schon in Branchenregelungen bereits „kurze“ Meldepflichten (zB „unverzügliche“ Meldung und Folgemeldung innerhalb 24 Stunden bei Sicherheitsvorfall mit beträchtlicher Auswirkung nach § 4 Telekom-Netzsicherheitsverordnung) gibt, sind 24 Stunden als Frist äußerst kurz bemessen. Es ist zu bedenken, dass auch kleine Unternehmen Normunterworfene sind, die bisher keinem derart strengen Regime unterlegen sind und gar nicht die personellen Ressourcen haben, eine 24 Stunden Meldepflicht über Wochenenden und Feiertage zu gewährleisten.

Zu überlegen wäre hier einerseits eine Fristverlängerung, andrerseits auch eine Einschränkung auf Sicherheitsvorfälle mit beträchtlichen Auswirkungen.

Die Formulierung „24 Stunden nach Kenntnisnahme“ umfasst auch zu viele Vorfälle bzw unplausible, überschießende Meldungen, die auch die Behörden unnötig belasten. In der Praxis wird man oft zuerst prüfen müssen, ob überhaupt ein Sicherheitsvorfall im Sinne des Art 4 Z 5 vorliegt, dh nachdem entsprechende Evidenz vorliegt. Eine „Evidenz“ liegt in der Regel vor, sobald die Geschäftsleitung von einem Sicherheitsvorfall informiert wird.

Zu Art 20 Abs 4 lit c (Abschlussbericht)

Angesichts dessen, dass es schwere Angriffe gibt, die auch einen längeren Zeitraum dauern (zB mehrmonatiger Spionageangriff), sollte anstelle des Wortlautes „Abschlussbericht“ durch „Abschluss- oder Fortschrittsbericht“ (bei andauerndem Angriff) ersetzt werden.

Da es sich um äußerst sensible Informationen handelt, sollte der Meldungsgeber das Recht haben, seine Information zumindest als „RESTREINT UE/EU RESTRICTED“ oder in einem vergleichbaren Sinne zu klassifizieren. In Absprache mit der nationalen NIS-Behörde sollten auch andere, stärkere Schutzklassen zulässig sein.

Zu Art 21 Abs 1 (Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung)

Kommt es zu einer Verpflichtung, IKT-Systeme nach spezifischen europäischen Systemen zur Cybersicherheitszertifizierung zertifizieren zu lassen, dann kann das unverhältnismäßig hohe Aufwände verursachen. Außerdem besteht die Möglichkeit, dass die Einhaltung, der für die Zertifizierung erforderlichen Richtlinien, technisch nicht realisierbar ist.

Zu Art 21, 22 (Cybersicherheitszertifizierung und Normung)

Es gibt eine Vielzahl von Normen und Standards. Es ist unbedingt darauf zu achten, dass hier nicht zusätzlich neue Regelungen geschaffen werden. Bestehende Regelungen dürfen im Sinne der Rechtssicherheit nicht in Widerspruch zueinanderstehen.

So muss beispielsweise im Telekommunikationsbereich sichergestellt sein, dass der vorgesehene „Use of European cybersecurity certification schemes“ nicht dazu führen darf, dass es zu einer zusätzlichen, parallel zur verpflichtenden Erfüllung internationaler Zertifikationsstandards – die für die Branche etwa über die TK-NSiV 2020 angeordnet wird – bestehenden Notwendigkeit zu Zertifizierungen kommt.

Wünschenswert wäre eine Auflistung bestehender Standards, bei deren Einhaltung EU-weit sichergestellt ist, dass die geforderten Sicherheitsmaßnahmen erfüllt sind. Die Überprüfungen aller Betreiber in Europa sollten sich an diesem Katalog orientieren.

Zu Art 26 (Informationsaustausch)

Im Sinne eines echten Informationsaustausches ist hier sicherzustellen, dass der Informations(rück-)fluss an die Unternehmen gewährleistet ist. Es müssen geeignete Kommunikationsstrukturen aufgebaut werden, um den Austausch zu fördern und alle Betroffenen über bestehende Bedrohungen zu informieren. (Wenn zB ein spanischer Betreiber einen

Sicherheitsvorfall meldet, müssen auch potentiell betroffene österreichische Betreiber umgehend verständigt werden bzw Informationen erhalten.)

Zu Art 27 (Freiwillige Meldung)

Der Wortlaut ist derzeit so formuliert, dass nur Einrichtungen, die nicht in den Anwendungsbereich der RL fallen, eine freiwillige Meldung machen können. Dies ist entsprechend des § 23 NISG dahingehend zu korrigieren, dass auch wesentliche oder wichtige Einrichtungen im Sinne der RL freiwillig Meldung von (nicht meldepflichtigen) Risken und Vorfällen abgeben können. Der Vorschlag wäre den Wortlaut „falling outside the scope of this directive" zu streichen.

Zu Art 29 (Aufsicht und Durchsetzung in Bezug auf wesentliche Einrichtungen)

Allgemein ist anzumerken, dass die Aufsichts- und Durchsetzungsbefugnisse ausgesprochen umfassende ex-ante und ex-post Befugnisse enthalten und diese äußerst kritisch zu durchleuchten sind. Insbesondere gilt dies für Art 29 Abs 4 lit g.

Zu Art 29 Abs 4 lit g

Dies kann nur bei einem gerechtfertigten Anlass erfolgen. Fraglich ist, wer hier die Kosten übernehmen soll. Falls daran gedacht ist, dass das betroffene Unternehmen zahlt, kann dies nur im Verschuldensfall und in einem angemessenen Rahmen zum Tragen kommen.

Weiters ist zu beachten, dass sichergestellt werden muss, dass der Überwachungsbeauftragte keinesfalls Daten, die er aus seiner Tätigkeit bekommt, für andere Zwecke nutzt oder weitergibt.

Zu Art 29 Abs 4 lit i

Die behördliche Anweisung einer öffentlichen Erklärung über den Verstoß ist an sich kritisch zu beurteilen. Dass darin auch die Person genannt werden soll, die für den Verstoß verantwortlich ist, ist unseres Erachtens grundrechtswidrig und strikt abzulehnen.

Zu Art 29 Abs 5 lit b

Die Verhängung eines Verbots von Leitungsaufgaben gegenüber Personen auf Geschäftsführungs- bzw Vorstandsebene oder Ebene des rechtlichen Vertreters ist ein unverhältnismäßiger Eingriff in die Geschäftsleitung und ebenso strikt abzulehnen.

Zu Art 29 Abs 6

Es ist unklar, welche Rechtsfolgen gemeint sind, wenn natürliche Personen für Verstöße haftbar gemacht werden können sollen. Bedeutet das in Österreich einen Verweis auf das Verwaltungsstrafrecht oder wird hier Bezug genommen auf die Sanktionen gemäß Art 31?

Zu Art 30 (Aufsicht und Durchsetzung in Bezug auf wichtige Einrichtungen)

In Abs 1 wird ausgeführt, dass bereits ein Hinweis darauf, dass eine wichtige Einrichtung ihren Verpflichtungen nicht nachkommt, für die Einleitung von Aufsichtsmaßnahmen ausreicht. Wir empfehlen, die Hinweise als Anlass für Aufsichtsmaßnahmen aus dem Passus zu streichen und nur Nachweise als Begründung zu definieren.

Die Anweisungen und Anordnungen, die gemäß Artikel 30 Abs 4 bei festgestelltem Mangel oder Verstoß verbindlich von der Behörde ausgesprochen werden, sind im Sinne der Verhältnismäßigkeit zu konkretisieren.

Für Post- und Kurierdienstleister ist die Information von natürlichen und juristischen Personen, die potentiell von erheblichen Cyberbedrohungen betroffen sind, die in Abs 4 Buchstabe e vorgesehen ist, wie oben bereits dargelegt, nicht umsetzbar. Es liegen keine Kontaktdaten zu potentiell betroffenen Paktversendern und Paketempfängern vor, auf die man zurückgreifen könnte. Die Nennung einer natürlichen Person, die für einen Verstoß verantwortlich ist, wie in Abs 4 lit h gefordert, verstößt unserer Ansicht nach gegen grundrechtlich abgesicherte Rechtspositionen und wird daher abgelehnt.

Im Übrigen gelten die entsprechenden Anmerkungen zu Art 29 im Kontext von Art 30 analog.

Zu Art 31 (Sanktionen)

Die Höhe der vorgesehenen Strafen kann sich für Unternehmen als existenzvernichtend erweisen, was nicht Sinn und Zweck einer Regelung zur Erreichung eines hohen Cybersicherheitsniveaus sein kann. Die Notwendigkeit erhöhter Strafandrohungen für die generalpräventive Wirkung ist zwar nachvollziehbar, erscheint in diesem Kontext jedoch ohne weitere Einschränkung unzumutbar.

Bei ausschließlich regionalen Vorfällen ist es gerechtfertigt, dass auch das Strafausmaß entsprechend eingeschränkt wird.

Technisch vollkommen getrennte Unternehmensteile sollten auch bei der Strafbemessung entsprechend berücksichtig werden. Hier den gesamten weltweiten Umsatz des Unternehmens, dem die wesentliche Einrichtung zuzuordnen ist, heranzuziehen, scheint unverhältnismäßig. Insbesondere für den ebenfalls betroffenen KMU-Bereich muss es hier massive Einschränkungen geben.

Zu Art 38 (Umsetzung)

Der Umsetzungszeitraum von 18 Monaten ist zu eng bemessen.

Der RL unterliegen vermutlich hunderte heimische Unternehmen, die bislang – außer Art 32 DSGVO eingeschränkt auf den Schutz personenbezogener Daten Dritter - keinen rechtlichen Vorgaben bezüglich Cybersicherheit unterworfen waren.

Aber auch bei den Normunterworfenen der bestehenden NIS-RL müssen durch die Neuregelungen teils ressourcenintensive Systemumstellungen geplant und umgesetzt werden bzw. Zertifizierungen gemacht werden.

NIS 2 baut auf das Regime von NIS 1 auf, was bedeutet, dass ein gewisses Schutzniveau bereits besteht. Um die gewünschten Verbesserungen durch NIS 2 zu erreichen, ist es notwendig, den Unternehmen ausreichend Zeit für eine solide Umstellung ihrer Prozesse und Systeme zu geben. Wir fordern daher dringend eine Erweiterung des Umsetzungsreitraums auf mindestens 24 Monate.

III. Zusammenfassung

Der vorliegende Vorschlag für eine NIS 2-Richtlinie wird seiner Zielsetzung nach grundsätzlich begrüßt, ebenso wie der Umstand, dass die EU im Rahmen der Cybersicherheitsstrategie Fördermittel für Unternehmen in Aussicht gestellt hat, um die europäische Wirtschaft cybersicher machen zu können. Cybersicherheit und generell IT-Sicherheit sind ohne Zweifel Themen von hoher Bedeutung.

Allerdings geht eine Reihe der vorgeschlagenen Maßnahmen über das hinaus, was zur Erreichung des Zieles erforderlich ist und sollte daher noch überdacht werden.

Zunächst erscheint die geplante Erweiterung des Anwendungsbereichs zu weitreichend. Nicht nur kleine Unternehmen und Kleinstunternehmen, sondern auch mittelgroße Unternehmen sollten grundsätzlich aus dem Anwendungsbereich der Richtlinie ausgenommen bleiben. Die Ausweitung des Anwendungsbereichs sollte nur Unternehmen von systemischer Relevanz umfassen, wobei die Versorgungskritikalität maßgeblich bei der Definition eines wesentlichen oder wichtigen Unternehmens auf nationaler Ebene sein sollte.

Da die Versorgungskritikalität und Abhängigkeit von inforationstechnologiebasierten Lösungen in einzelnen Branchen eine vergleichsweise geringe Rolle spielen, sollten bestimmte Branchen aus dem Anwendungsbereich der Richtlinie ausgenommen werden. Dies betrifft insbesondere die Abfallwirtschaft, bestimmte Dienste im Bereich Verkehr, Post- und Kurierdienste sowie Lebensmittelunternehmen.

Die Abgrenzungen im Rahmen der Richtline selbst und gegenüber anderen Rechtsakten sowie die Formulierung rechtlicher Vorgaben bedarf klarer und transparenter Kriterien, die es den verpflichten Unternehmen ermöglichen, zweifelsfrei zu erkennen, ob sie den Verpflichtungen der NIS 2-RL unterliegen und welche Verpflichtungen im Einzelnen erfüllt werden müssen. In diesem Sinne erscheint es ferner auch wünschenswert, statt der ex lege Einbeziehung von Unternehmen in die Verpflichtung der Richtline eine bescheidmäßige Bestimmung durch die zuständige Behörde vorzusehen und damit Rechtsunsicherheit für betroffene Unternehmen zu reduzieren.

Die Meldepflicht betreffend bestimmte Vorfälle sollte in zeitlicher Hinsicht großzügiger bemessen werden und es sollte danach gestrebt werden, dass – ungeachtet der konkret ausgeübten Aktivität im Sektor - je Sektor immer nur eine NIS-Behörde als Meldestelle und für Überprüfungen der einschlägigen Verpflichtungen zuständig ist.

Die Verschärfung des Sanktionsrahmens erscheint uns in mehrfacher Hinsicht unverhältnismäßig. Sowohl die extreme Strafhöhe als auch einzelne Sanktionen für Verantwortliche in Unternehmen sollten vor diesem Hintergrund angepasst werden, um für betroffene Unternehmen nicht existenzgefährdend zu werden.

Abschließend sprechen wir uns für eine Ausweitung des Umsetzungszeitraums auf 24 Monate hin, um sicherzustellen, dass die bedeutende Zahl heimischer Unternehmen, die erstmals von spezifischen Cybersicherheits-Regelungen betroffen sein wird, über genügend Zeit für erforderliche Anpassungsschritte verfügt.

Wir ersuchen um Berücksichtigung unserer Anmerkungen.

Freundliche Grüße

Dr. Harald Mahrer
Präsident

Karlheinz Kopf
Generalsekretär

WIRTSCHAFTSKAMMER ÖSTERREICH WKO ELEKTRONISCHE SIGNATUR	**Unterzeichner**	**Wirtschaftskammer Österreich**
	Datum/Zeit-UTC	**2021-05-18T13:31:08+02:00**
	Aussteller-Zertifikat	**a-sign-corporate-light-02**
	Serien-Nr.	**1716778599**
	Hinweis	**Dieses Dokument wurde amtssigniert.**
	Prüfinformation	**Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter https://www.signaturpruefung.gv.at/.**