unsere energie

Per Mail: praesidiales@regierung.li

Ministerium für Präsidiales
Regierungsgebäude
Peter-Kaiser-Platz 1
9490 Vaduz

Datum 26. September 2022
Ihr Kontakt Herbert Müller
Telefon +423 236 01 03
E-Mail herbert.mueller@lkw.li
Thema **Vernehmlassung über die Schaffung eines Cybersicherheitsgesetzes, CSG**

Sehr geehrte Damen und Herren

Gerne nehmen wir zum Vernehmlassungsbericht betreffend der Schaffung eines Gesetzes über Cybersicherheit fristgerecht Stellung und bedanken uns für die Möglichkeit dies zu tun.

Als Anbieter kritischer Infrastrukturen begrüssen die Verantwortlichen der LKW die Festlegung einer nationalen Strategie für die Netz- und Informationssysteme in Verbindung mit Sicherheitsanforderungen und Meldepflichten für die Betreiber im Sinne einer angemessenen Risikomanagementkultur.
Die LKW begrüssen die Wahl eines risikobasierten Ansatzes entsprechend Art. 4, Abs. 1 sowie Art. 6, Abs 2 im Sinne des Kosten- Nutzen- Verhältnisses ausdrücklich.

Als «Betreiber wesentlicher Dienste» (kritische Infrastruktur in den Bereichen elektrische Energie und Telekommunikation) sowie als zukünftiger «Anbieter digitaler Dienste» (Strom-Handelsplattform) sind die LKW von diesem Gesetz besonders betroffen.

Anmerkungen zu den einzelnen Artikeln:

Art. 3, Abs. 1, Ziff. 3 sowie Art. 14 (NIS)
Der in der Vorlage verwendete Begriff «NIS (Netz- und Informationssystem) – Strategie bzw. Richtlinie» ist gerade im Zusammenhang mit den LKW irreführend, da der Begriff schon im Zusammenhang mit der Thematik «Nichtionisierende Strahlung» belegt ist. Wir verweisen auf LR-Nr. 814.011.3 und 31.

Art. 3, Abs. 1, Ziff. 9 bzw. Erläuterungen zu Art. 5, Abs. 3 (S. 22 der Vernehmlassung)
Zitat aus den Erläuterungen: «Dabei spielt es keine Rolle, ob es durch den Sicherheitsvorfall zu einem Schaden oder zu einer anderweitigen Störung gekommen ist.»
Hier ist aus Sicht der LKW eine Konkretisierung bei Art. 3, Abs. 1, Ziff. 9 vorzunehmen, da aus Sicht der LKW ohne weitere Ausführungen jeder Besuch einer Phishing Webseite oder Virenbefall eines einzelnen Endgeräts gemeldet werden müsste, was sowohl aus unternehmerischer Sicht als auch aus Sicht der Stabsstelle Cyber-Security zu Ineffizienz führt und die wesentlichen Vorfälle in den Hintergrund rückt.

Wir schlagen daher vor, Art. 3, Abs. 1, Ziff. 9 wie folgt zu erweitern:
«.... zugänglich sind, beeinträchtigen; *sofern nur einzelne Systeme (Endnutzergeräte, Nutzerkonten) von geringer Kritikalität betroffen sind und/oder der Angriff unter Anwendung geeigneter Schutzmassnahmen erfolgreich abgewehrt werden konnte, handelt es sich nicht um einen Sicherheitsvorfall im Sinne dieses Gesetzes.*»

Art. 5, Abs. 1 sowie Art. 7, Abs. 1 und 2 (Meldepflicht, Meldefrist)
Der Begriff «unverzüglich» ist in Abhängigkeit vom jeweiligen Angriffsszenario und der umgehend einzuleitenden Abwehrmassnahmen ein sehr harter Begriff. Gerade in den ersten Stunden eines erfolgreichen Cyber-Angriffs sollten den Abwehrmassnahmen erste Priorität geschenkt werden.
Die LKW würden es begrüssen, wenn der Artikel, in Anlehnung an die Meldefrist im Rahmen der DSGVO, wie folgt angepasst werden würde:
«Betreiber wesentlicher Dienste bzw. Anbieter digitaler Dienst haben einen Sicherheitsvorfall, der einen von ihnen bereitgestellten Dienst betrifft *innert 72 Stunden nach dem Erkennen* der Stabsstelle Cyber-Sicherheit zu melden».

Art. 5, Abs. 3 (Meldeverfahren)
Die LKW begrüssen die Meldung über ein standardisiertes Verfahren. Gerade im Ernstfall, wenn viele Aufgaben anstehen und alles sehr schnell gehen muss, kann so nichts Wesentliches vergessen werden.
Hier bitten wir wie folgt einzufügen: «... in einem standardisierten *gesicherten* elektronischen Format...»

Art. 5, Abs. 4 sowie Art. 7, Abs. 3 (Kommunikation)
Um Desinformation, wirtschaftlichen Schaden, Panik etc. in der Bevölkerung bzw. bei den Unternehmen zu vermeiden, ist eine Anhörung und Abstimmung mit dem jeweiligen Krisenkommunikationskonzept des betroffenen Unternehmens, gerade aus der Sicht als Anbieter kritischer Infrastrukturen, zwingend notwendig.

Art. 7, Abs. 2 (Meldepflicht/Meldefrist im Zusammenhang mit Dritten)
Auch hier wird bei der Meldefrist der Begriff «unverzüglich» verwendet. Wir verweisen auf unsere Ausführungen zur Art. 5, Abs. 1.
Ergänzend dazu kennen wir ein zeitnahes Beispiel, in dem die ausländischen Strafverfolgungsbehörden dem betroffenen Unternehmen (Dritten) ausdrücklich untersagt haben, die Beeinträchtigung ihrer Systeme im Rahmen eines Cybervorfalls an andere Unternehmen und Partner weiterzugeben, sprich diese wurden erst Tage später über den Sicherheitsvorfall informiert.

Um sich schad- und klaglos zu halten bedingt dieser Absatz, dass jeder Betreiber bzw. Anbieter digitaler Dienste einen rechtsverbindlichen Vertrag betreffend Meldepflicht und Meldefrist mit leistungserbringenden Dritten im In- und Ausland abschliesst.
Wir bitten die zuständigen Stellen zu prüfen, ob die Rechtslage in den verschiedenen Ländern dies zulässt und inwieweit sich insbesondere das Risiko, bei Nichteinhaltung der Meldefristen (Strafen), auf den/die Dritten überwälzen lässt. Bzw. wie ist damit umzugehen, wenn die Rechtsabteilung des betroffenen dritten Diensteanbieters solch einem Vertrag, insbesondere auf Grund der Unverhältnismässigkeit des Begriffes «unverzüglich» und dem bei einer Verletzung damit einhergehenden Strafausmass nicht zustimmt.

Liechtensteinische Kraftwerke | Im alten Riet 17, 9494 Schaan | Telefon +423 236 01 11, Telefax +423 236 01 12 | info@lkw.li, www.lkw.li

Art. 10, Abs. 1, Bst. h bzw. m (Internationale Zusammenarbeit)
Hier verweisen wir auf die bereits bestehende Zusammenarbeit der LKW mit dem Nationalen Zentrum für Cybersicherheit (NCSC) der Schweiz, sofern nicht unter Bst. m erfasst.

Art. 11, Abs. 1, Bst. a und b sowie Art. 11 und Art. 13 (Befugnisse)
Nachdem die Informationen etc. unentgeltlich zur Verfügung gestellt werden müssen, sollten sich die Überprüfungen etc. auf ein definiertes und kalkulierbares Zeitfenster beschränken. Wir schlagen daher vor, eine Anpassung der Bst. a und b wie folgt vorzunehmen:

a) die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen «*im Rahmen eines zeitlich befristeten Audits*», einschliesslich der dokumentierten Sicherheitsmassnahmen, zur Verfügung stellen, «*welche von der Stabsstelle Cyber-Sicherheit und beauftragten Dritten, innert einer Frist von 4 Wochen wieder vollständig vernichtet werden*»;
b) auf Grundlage des neuen Artikels a) kann b) gestrichen werden da ein Audit auch die Erbringung von Nachweisen umfasst.

Art. 11, Abs. 1 sowie Art. 12, Abs. 2 und Art. 13 (Schutz der Informationen, Kontrolle)
Als Anbieter wesentlicher und digitaler Dienste erwarten wir, dass die abgegeben Informationen von der Stabsstelle höchst vertraulich behandelt sowie gegen Angriffe gesichert übermittelt und aufbewahrt werden. Dies gilt auch für qualifizierte Dritte, welche gem. Art 13 im Auftrag der Stabsstelle Cyber-Security Kontrollen etc. durchführen.
Wenn die Informationen all dieser Betroffenen inkl. kritischer Infrastrukturen zentral an einem Ort aufbewahrt werden, gibt es kaum ein Angriffsziel welcher interessanter sein könnte. Die betroffenen Betreiber wesentlicher Dienste, als auch die Anbieter digitaler Dienste, sollten die Möglichkeit erhalten, sich über die getroffenen Sicherheitsvorkehrungen, Vertraulichkeitserklärungen etc. zu informieren.

Zudem bitten wir sie zu prüfen, inwieweit die Stabsstelle Cyber-Sicherheit bzw. das Land Liechtenstein und/oder von ihr beauftragte Dritte betr. Schadenersatz belangt bzw. haftbar gemacht werden können, sollte durch unzureichende Schutzmassnahmen etc. einem auditierten Unternehmen nachweislich Schaden entstehen.

Art. 11, Abs. 2 (statistische Daten, Empfänger, Schutz der Informationen,)
Nachdem es sich um anonymisierte oder nicht anonymisierte, in jedem Fall aber stets um hoch vertrauliche Informationen handelt, sollten diese nicht uneingeschränkt aufbewahrt werden dürfen. Wir schlagen daher folgende Ergänzung des Abs. 2 auch zum Schutz der Stabsstelle Cyber-Security als auch der von ihr mit Untersuchungen oder Kontrollen beauftragten Dritten vor:
«*Sofern zu statistischen Zwecken Originaldaten zur Verfügung gestellt werden müssen, müssen diese von der Stabsstelle Cyber-Sicherheit innert 6 Monate vollständig und unwiederbringlich vernichtet werden. Können die Daten anonymisiert zur Verfügung gestellt werden, sind diese innert einem Jahr vollständig und unwiederbringlich zu vernichten.*»

Zudem ist nicht ausgeführt, wem und in welcher Form die Stabsstelle Cyber-Sicherheit über die von ihr oder beauftragten Dritten erlangten, aus unserer Sicht auch auf Landesebene ggf. hoch vertraulichen Informationen und Erkenntnisse, öffentlich oder auch nichtöffentlich Bericht erstattet. Ebenso ist nicht ausgeführt, wie in diesem Zusammenhang einerseits die Informationswege (Thema: hoch verschlüsselte Datenübertragung) als auch die Geheimhaltung geregelt sind, um einen unbefugten Zugriff zu verhindern.

unsere energie

Art. 21 (Bussen)
Die Höhe der Bussen kann trotz der gewählten Formulierung «bis zu» für KMU's zu einer sehr grosse Belastung werden. Hier würden wir anregen, eine Abstufung in Relation zur Unternehmensgrösse vorzunehmen.

Abschliessen weisen wir darauf hin, dass das Sicherheitsniveau der Stabsstelle Cyber-Sicherheit als zentrale Anlaufstelle und konzentrierter Datenhub entsprechend den sich stetig steigenden Risiken angemessen hochzuhalten ist. Insbesondere in technischen Belangen (hochprofessionelles Equipment, Schutz der erlangten Informationen etc.), die personellen Ressourcen betreffend (hochqualifiziertes spezialisiertes Personal, gilt auch für Dritte) aber auch in finanzieller Hinsicht (z.B. Haftpflichtversicherung im Schadensfall) müssen nicht unerhebliche Mittel bereitgestellt werden, um keine zusätzliche Angriffsfläche zu bieten und um die Cyber-Sicherheit im Land Liechtenstein gewährleisten zu können.

Für Fragen oder weitere Ausführungen stehen wir jederzeit sehr gerne zur Verfügung.

Freundliche Grüsse

Liechtensteinische Kraftwerke

Herbert Müller
Mitglied der Geschäftsleitung

Gerald Marxer
Vorsitzender der Geschäftsleitung

Liechtensteinische Kraftwerke Im alten Riet 17 9494 Schaan Telefon +423 236 01 11 Telefax +423 236 01 12 info@lkw.li www.lkw.li