NetSec.co AG
Im alten Riet 125
9494 Schaan, Liechtenstein
+423 388 2777
info@netsec.co
https://netsec.co

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

27. September 2022/ThGu

Vernehmlassung betreffend Cybersicherheitsgesetz (CSG)

Sehr geehrte Damen und Herren

Gerne nehmen wir an der Vernehmlassung zum Cybersicherheitsgesetz (CSG) teil.

Wir haben den Gesetzesentwurf studiert und haben Anmerkungen zu einigen Artikeln.

Art. 1

Es sollte geprüft werden, ob Medienhäuser, die die Bevölkerung mit Informationen versorgt, nicht auch zu den wesentlichen Diensten gezählt werden sollten. In Krisenfällen sind sie ein wichtiges Standbein der Krisenbewältigung und sollten daher vor möglicher Manipulation ausreichend geschützt sein.

Art. 4 und 6

In den beiden Artikeln werden die Sicherheitsanforderungen für **Betreiber wesentlicher Dienste**, bzw. für **Anbieter digitaler Dienste** aufgeführt. Die Anforderungen sind nahezu identisch, wobei in Artikel 6 konkrete Aspekte aufgeführt sind (in Artikel 4 fehlen diese).

Wir schlagen vor zu prüfen, ob die beiden Artikel zusammengelegt werden können. Die Aufzählung der Aspekte könnte entweder so belassen werden, dass sie für beide Betreibergruppen gültig sind, oder sie könnte in die Verordnung verschoben werden.

Zitate

Art. 4

1) Betreiber wesentlicher Dienste ergreifen geeignete und verhältnismässige technische und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Massnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist.

Art. 6

1) Die Anbieter digitaler Dienste ergreifen geeignete und verhältnismässige technische und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung des digitalen Dienstes nutzen, zu bewältigen.

2) Diese Massnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, wobei den folgenden Aspekten Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen;

b) Bewältigung von Sicherheitsvorfällen;

c) Betriebskontinuitätsmanagement;

d) Überwachung, Überprüfung und Erprobung;

e) Einhaltung der internationalen Normen.

Art. 10

Hier schlagen wir vor, die **Förderung der allgemeinen Cyber-Sicherheit** als zusätzliche Aufgabe zu definieren.

Art. 11

1) a)

Hier schlagen wir vor, dass die Betreiber ihre Risikoanalyse, die die Bewertung der Risiken und die risikoreduzierenden Massnahmen enthält, ebenfalls offenlegen müssen.

Unserer Ansicht nach kann nur damit beurteilt werden, ob die Risiken realistisch beurteilt wurden und die getroffenen Sicherheitsmassnahmen zweckmässig und ausreichend sind.

2)

Hier schlagen wir vor, zu ergänzen, dass diese Daten in einem automatisch verarbeitbaren digitalen Format offengelegt werden müssen.

Ergänzung

Wir schlagen vor, diesen Artikel so zu ergänzen, dass die Betreiber auch verpflichten sind, Log Daten für eine bestimmte Zeit (z.B. 18 Monate) aufzubewahren, so dass diese bei Bedarf für forensische Analysen verwendet werden können.

Art. 15

Gemäss diesem Artikel muss die Stabsstelle Cyber-Sicherheit ein Computer-Notfallteam (CSIRT) einrichten und betreiben.

Unserer Ansicht nach ist Liechtenstein zu klein, um ein eigenes CSIRT zu betreiben. Dies aus folgenden Gründen:

- Ein CSIRT ist eine operative Einheit, die viel Erfahrung mit aktuellen Fällen benötigt; das Tätigkeitsgebiet Liechtenstein ist zu klein, um eine ausreichende Anzahl Fälle dafür zu haben.
- Ein CSIRT muss 7x24h operativ sein (darauf wird auch in den Erläuterungen hingewiesen). Wir erachten es daher nicht als zweckmässig, wenn der Betrieb nur zu Bürozeiten operativ ist und die restliche Zeit nur eine Triage durch einen externen Partner gemacht wird.
- CSIRTs werden in der Regel durch den Staat betrieben. Ob es zweckmässig ist, ein Liechtensteiner CSIRT mit Unterstützung externer Privatfirmen zu betreiben, sollte hinterfragt werden.

Aus den genannten Gründen schlagen wir vor zu prüfen, ob die Muss-Vorgabe in eine Kann-Vorgabe umformuliert und die Option, sich an ein bestehendes CSIRT eines anderen (idealerweise deutschsprachigen) Staates anzuschliessen, geschaffen werden kann.

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

Freundliche Grüsse

NetSec.co AG

Thomas Gusset

Geschäftsführer

Thomas Gusset, NetSec.co AG
Schaan, 27. September 2022
CEO
Unterschrift