Milano, 19/07/2024

Al Presidente della Commissione
Affari Costituzionali

Oggetto: Osservazioni in merito al recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica al regolamento (UE) 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

PREMESSO

che l'Associazione Italiana dei Professionisti della Security Aziendale, AIPSA-ETS, è una rete associativa di oltre 800 professionisti di security e più di 200 società, rappresentative dei più rilevanti gruppi industriali nazionali e dei servizi essenziali di pubblica utilità, nonché gestori di infrastrutture critiche nazionali,

che al suo interno, l'associazione conta diversi gruppi di lavoro impegnati nello studio delle materie tecniche, funzionali, giuridiche e legislative in materia di security aziendale,

che nell'ambito dell'esame dell' Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (cd. NIS2) è stata richiesta ad AIPSA una memoria scritta da lasciare agli atti delle Commissioni al fine di acquisire utili elementi di conoscenza e di valutazione.

CONSIDERATO

che il confronto intercorso con i nostri associati, le argomentazioni e analisi istruttorie a valle di una ricognizione ragionata dei requisiti previsti dal testo della direttiva europea, ivi incluso rispetto all'ecosistema normativo europeo di recente produzione, hanno rilevato alcuni profili di attenzione rispetto al tempestivo ed efficace recepimento della direttiva Direttiva (UE) 2022/2555 in Italia,

con la presente memoria si producono le seguenti considerazioni ed osservazioni di seguito sinteticamente riportate e suddivise in sei aree tematiche:

OSSERVAZIONI

1) **<u>Sull'ambito di applicazione</u>**
   1. Si auspica l'armonizzazione tra la strategia nazionale per la resilienza dei soggetti critici e la strategia nazionale per la cybersecurity. In particolare, si osserva la necessità di una strutturata coerenza normativa tra la Direttiva NIS 2 e la Direttiva CER, che attribuisca alla NIS 2 pertinenza e competenza in ambito cybersecurity, favorendo altresì coordinamento, omogeneità e integrazione in termini di approcci, metodi e contenuti con la direttiva CER, ispirati dai principi della sicurezza olistica ed approcci multirischio, da criteri di efficientamento e snellimento burocratico nonché da logiche sinergiche di collaborazione pubblico-privato.

2) **Sull' analisi dei rischi**

2. Si osserva la necessità di integrare l'approccio multirischio in NIS 2 con i framework e i metodi di analisi del rischio già recentemente formalizzati (ad esempio, rispetto alla normativa in ambito PSNC).
3. Si auspica il recepimento da parte dell'ACN del Framework Nazionale per la Cybersecurity e la Data Protection (nella sua ultima versione v2.0 attualmente in vigore).
4. Si auspica la promozione e valorizzazione di approcci multidisciplinari integrati alla gestione del rischio, che consentano, per i rispettivi ambiti di pertinenza e applicazione delle diverse norme in materia di security e resilienza, di integrare e armonizzare criteri, soglie, livelli e funzioni di calcolo del rischio, valorizzando i riferimenti alla necessità di trattare minacce sempre più ibride secondo approcci integrati multirischio (di cui al punto 1) della presente memoria).

3) **Sulle misure di sicurezza e la gestione degli incidenti**

5. Si auspica l' implementazione di dettagliati criteri di adeguatezza e proporzionalità nelle misure di sicurezza, sia in funzione del livello di rischio analizzato, sia rispetto alla esposizione e tipologia del soggetto identificato (differenziando quindi tra soggetti importanti ed essenziali), sia rispetto alla valutazione di impatto sui sistemi informativi e di rete.
6. Si osserva la necessità di rafforzare il reporting periodico in ambito cybersecurity al board, per finalità di monitoraggio e indirizzo delle priorità strategiche cyber.
7. Si richiede di uniformare le procedure per la segnalazione degli incidenti tra NIS 2, PSNC e CER.
8. Si auspica un chiarimento sulla gerarchia delle norme, qualora il soggetto rientri nel perimetro della NIS 2, ma abbia anche conferito Beni in ambito PSNC, con particolare riferimento al trattamento degli asset "fuori perimetro".

4) **Sui criteri di individuazione, il programma di adeguamento e le responsabilità**

9. Si auspica che il piano di adeguamento normativo sia definito secondo principi di proporzionalità e gradualità, in coerenza con il livello di maturità di partenza del soggetto e con particolare riferimento alle iscrizioni ex novo.
10. Si richiede maggiore chiarezza sulle tempistiche di applicazione della norma, con particolare riferimento alle modalità specifiche e i tempi graduali di implementazione differenziati in relazione alla categorizzazione di cui all'art. 40 comma 2 e sulle tempistiche di ricorrenza della valutazione rispetto alla categoria di rilevanza, di cui all'art.30 comma 1.
11. Si auspica che gli aspetti tecnici riguardanti le modalità di attuazione della norma, ivi incluso il dettaglio sulle procedure di registrazione, non risiedano nella legge di recepimento ma vengano definiti in determine del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (ACN).
12. Si osserva altresì la necessità che il soggetto, nelle more della responsabilità di dare attuazione al programma di attività comunicato, comunichi e giustifichi esaurientemente eventuali variazioni di tempistiche al medesimo piano.
13. Si auspica che alcuni criteri di attribuzione delle soglie di inclusione per le società possano essere definiti dalle Autorità di settore con il coinvolgimento dei soggetti critici in perimetro.

5) **<u>Sulle terze parti</u>**

14. Si auspica che i fornitori dei soggetti importanti ed essenziali, laddove non già in perimetro NIS 2, siano automaticamente inquadrati come soggetti "NIS 2 relevant" (ed almeno importanti) ai sensi del decreto. Si osserva la necessità di enfatizzare l'importanza di questo rilievo, dacché il solo fatto che siano previste nei contratti clausole di security in riferimento agli adempimenti in materia di valutazione del rischio, misure di sicurezza e segnalazione degli incidenti, appare non sufficiente a garantire l'efficacia e l'efficienza della sicurezza della supply chain. Si osserva la necessità di implementare registri di security degli accordi contrattuali.
15. Si osserva la necessità di fornire elementi di indirizzo rispetto alla definizione e implementazione di framework per la gestione dei rischi connessi alle terze parti, che prevedano anche il coinvolgimento di associazioni di categoria già attive nell'ambito specifico.

6) **Sulla formazione**

16. Si auspica anche il supporto da parte ACN nella condivisione di linee guida, nell'attivazione di corsi di formazione per dipendenti di soggetti importanti ed essenziali e nello svolgimento di esercitazioni su scenari di particolare criticità e rilevanza.