ASSOLOMBARDA

16 luglio 2024

Osservazioni allo schema di decreto legislativo di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

Premessa

Assolombarda è l'associazione più importante del Sistema Confindustria, con oltre 7.000 aziende associate che operano nella Città Metropolitana di Milano e nelle province di Lodi, Monza e Brianza, Pavia. Da sempre l'Associazione si è posta all'avanguardia rispetto all'approfondimento e alla costruzione di proposte tecniche nell'ambito della cybersicurezza, a partire dai lavori del Gruppo Tecnico Transizione Digitale e Innovazione tecnologica, che racchiude alcune delle più importante imprese, italiane e multinazionali, del comparto.

Osservazioni

In relazione allo schema di decreto legislativo in oggetto, e a seguito del confronto intercorso con i nostri Associati, abbiamo rilevato quattro principali osservazioni largamente condivise, e di seguito sinteticamente riportate.

1. Prendendo in considerazione l'approccio "propositivo" adottato dal Decreto, come previsto dall'Articolo 7, comma 1, saranno le imprese interessate a registrarsi o aggiornare la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS. Tale scenario delinea al momento forte incertezza, per quelle imprese che non fossero precedentemente contemplate nella Direttiva Nis I o nel Perimetro di Sicurezza Nazionale, rispetto alla necessità di una loro iscrizione ex novo. A titolo esemplificativo, numerose imprese non hanno un unico "settore di riferimento" come da allegato I, ma operano piuttosto su molteplici settori. Ciò estende il campo di applicazione, includendo un maggior numero di aziende considerate "delicate" per la sicurezza nazionale e l'economia.

Sarebbe quindi auspicabile, per il primo inserimento all'interno della piattaforma, che vi sia un input iniziale da parte dell'Autorità Competente verso l'azienda rispetto alla necessità di una sua iscrizione.

2. Da molte imprese è stata auspicata l'adozione di una gradualità nell'attuazione della norma per i soggetti "nativi NIS2", o della creazione di una finestra transitoria che possa dilatare in parte i tempi previsti per l'entrata in vigore di alcuni obblighi. Per molti di questi soggetti, al momento, risulterebbe infatti complicato portare a termine il piano di attuazione delle misure tecnico-organizzative previste dalla norma nei tempi richiesti, anche considerando l'attuale carenza di competenze e di offerta che caratterizza il mercato del lavoro

3. In considerazione dalla natura del provvedimento, in cui è presa in esame l'intera filiera, si chiede di considerare che i fornitori dei soggetti importanti o essenziali, in relazione al servizio/prodotto offerto, possano divenire soggetti importanti a loro volta. Tale riconoscimento dovrebbe essere eseguito in seguito ad un'analisi dei rischi che evidenzi quali siano i campi "critici" in cui un'eventuale compromissione potrebbe causare danni al soggetto essenziale o importante principale. Inoltre, si ritiene prioritario che i soggetti importanti ed essenziali siano responsabili del definire, attraverso un processo di analisi del rischio, quali sistemi aziendali debbano essere considerati ad alto impatto (come avviene, ad esempio, nell'ambito della certificazione iso27001). Attualmente, invece, la normativa considera l'intero sistema informativo.

4. In relazione all'articolo 11, in cui sono specificate le autorità di settore Nis, si ritiene importante dare vita ad un quadro normativo che indirizzi all'adozione di uno schema minimo di sicurezza di base omogeno per tutti i Ministeri e le autorità coinvolte. Partendo dal presupposto che molte delle imprese interessate mantengono simultaneamente rapporti di collaborazione con diverse istituzioni e autorità, appare evidente la criticità qualora, innanzi a un quadro disomogeneo, fosse loro richiesto di implementare differenti sistemi e strategie di sicurezza.