ASSOTELECOMUNICAZIONI
ASSTEL

ADERENTE A CONFINDUSTRIA E CONFINDUSTRIA DIGITALE

AUDIZIONE DI ASSOTELECOMUNICAZIONI-ASSTEL SU SCHEMA DI DPCM ATTUATIVO DEL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Camera dei Deputati – Commissioni riunite IX e XIV

Roma, 7 luglio 2020

Asstel è l'Associazione di categoria che, nel sistema di Confindustria, rappresenta la filiera delle telecomunicazioni costituita dalle imprese delle diverse aree merceologiche che le appartengono, tra le quali le imprese che gestiscono reti di telecomunicazioni fisse e radio-mobili e servizi digitali accessori, i produttori ed i fornitori di terminali-utente, i produttori ed i fornitori di infrastrutture di rete, di apparati e di servizi software per le telecomunicazioni, i gestori di servizi e di infrastrutture di rete, anche esternalizzati, i gestori di servizi di Customer Relationship Management e di Business Process Outsourcing. Asstel aderisce inoltre a Confindustria Digitale.

Si esprime un sentito ringraziamento per l'opportunità di intervenire su una materia così rilevante per la filiera delle telecomunicazioni.

Lo schema di DPCM in commento avvia il percorso delle norme attuative del perimetro di sicurezza nazionale cibernetica, che a sua volta sistematizza il quadro composito che emerge dalla direttiva NIS, dalle norme Golden Power e dalle norme per la sicurezza della continuità di servizio delle reti di telecomunicazioni (Decreto Ministero dello Sviluppo Economico 12 dicembre 2018, "decreto Telco"), per citare le più rilevanti.

E' necessario che si dedichi attenzione alle modalità con cui il Perimetro potrà essere effettivamente implementato, collaborando con gli attori di mercato, anche facendo perno sulle strutture (pubbliche e private) presenti sui territori (Digital Innovation Hub, Centri di Competenza, Punti Impresa Digitale, ecc.) ed adottando, come fatto per la NIS, strumenti comuni di valutazione ed intervento, ad esempio basati sul Framework Nazionale di Cyber Security e sugli standard internazionali (es. ISO/IEC 27001:2013, ISO/IEC 27005:2018, ISO/IEC 31000:2018 e ISO/IEC 31010:2019, EN/IEC 62443) oltre che sul quadro di Data Protection.

I criteri di sottoposizione al Perimetro ampliano notevolmente la platea dei possibili soggetti obbligati; per stabilire le corrette relazioni e costruire i necessari percorsi di analisi dei sistemi inclusi nel Perimetro, gestione della sicurezza / resilienza, gestione degli incidenti, è necessario procedere all'implementazione del Decreto 105/2019 in modo tale da definire un quadro normativo coerente in tutti i suoi aspetti "di filiera", che contemperi la necessità di un approccio graduale con quella di certezza delle regole in cui gli Operatori di mercato possono agire.

In questo senso, appare generalmente importante un primo elemento di chiarezza relativamente al fatto che l'obiettivo delle ispezioni dovrebbe essere ben identificato nella verifica dell'adempimento delle prescrizioni di legge e non nella garanzia dell'impenetrabilità dei sistemi (distinzione dell'ispezione ai fini di conformità degli adempimenti alle norme vs ai fini della tenuta dei sistemi di difesa).

Venendo al commento di quanto disposto dal DPCM oggetto di attenzione:

1. Lo schema di DPCM in commento definisce i criteri con cui individuare i soggetti obbligati, come previsto nella norma;
2. rimanda ad attività successive l'identificazione di funzioni e servizi essenziali (a cura dei Ministeri designati per i diversi settori: MiSe per telecomunicazioni) e la finalizzazione del modello per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e di servizi informatici. Questo sarà a cura del DIS, che predisporrà anche un sistema informativo per il caricamento dei dati e la messa a disposizione per attività ispettive. Questi aspetti sono di importanza fondamentale per consentire l'ordinata attuazione del perimetro, che dovrà avvenire tenendo costantemente attenzione alla coerenza complessiva del sistema.

3. Si segnalano come elementi di criticità interpretativa, nell'attuazione dei quali sarà necessaria una stretta interlocuzione con gli attori del mercato digitale,

    a. l'introduzione di definizioni di difficile interpretazione ("bene ICT" e "parte minimale di un bene ICT") e

b. l'assenza di riferimenti temporali precisi per le fasi transitorie e per le attività enunciate nello schema.

4. Inoltre, emergono una serie elementi che riteniamo opportuno segnalare:

   a. esigenza di introdurre riferimenti tecnico-operativi ed un linguaggio comune, possibilmente consistenti con standard e prassi internazionali (ETSI/3GPP/GSMA e ITU);

   b. necessità di avere un modello di analisi del rischio con una matrice di livelli con numerosità e definizione comuni;

   c. esigenza di definire architetture di riferimento comuni con componenti e relazioni/dipendenze ai quali associare livelli di criticità, con un opportuno livello di astrazione per evitare la complessità indotta dalla frammentazione nei dettagli

   d. importanza dell'attivazione del CVCN e dell'identificazione dei criteri di accreditamento dei laboratori esterni di supporto.

   e. esigenza di certezza e rapidità delle tempistiche di intervento a carico dei soggetti deputati (es. CVCN) con SLA impegnativi e clausole relative al diritto dell'operatore a procedere in assenza di riscontri utili nei termini temporali previsti dagli SLA

   f. <u>L'utilità di un percorso incrementale in continuità con decreto Telco (2018) e Golden Power 5G per procedimenti, convenzioni e misure già messe in campo.</u>

      Nell'ottica di adottare una soluzione che si ponga in continuità con quanto previsto dalle predette normative, segnaliamo l'opportunità di:

      - prevedere per i beni ICT le medesime misure di sicurezza indicate dall'art. 4 del decreto Telco o misure di livello equivalente, al fine di uniformare gli standard di sicurezza richiesti dalle divere normative e rendere più efficiente il sistema;
      - uniformare la procedura di notifica incidenti con quanto già previsto dall'art. 5 del "Decreto Telco";

- tenere in considerazione, sotto il profilo del rispetto degli obblighi posti dalle disposizioni attuative del Perimetro di Sicurezza cibernetica, gli esiti dei test condotti dagli operatori in ambito 5G per garantire i livelli di sicurezza richiesti dalla Golden Power, evitando duplicazioni nelle attività di test e verifica sugli stessi asset.

g. Con riferimento al ruolo degli operatori telco, tenere conto del limite di responsabilità degli operatori di telecomunicazioni nella catena ICT che indirizza obiettivi di sicurezza per servizi essenziali verticali. La responsabilità dell'operatore è fissata nei contratti con i clienti dei settori verticali e con misure guidate dall'analisi del rischio svolta dai clienti sui servizi essenziali di pertinenza.

h. esigenza di scongiurare l'imposizione di misure che insistano sul modello operativo e sull'organizzazione dei rapporti con i fornitori fino ad influenzare il modello di business (es. misure che vincolano la località fisica dei fornitori e la supervisione del loro operato)

5. Nella definizione dell'insieme dei provvedimenti attuativi del perimetro di sicurezza nazionale cibernetica, si dovrebbero tenere in conto le seguenti caratteristiche delle nuove reti e loro conseguenze:

   a. le nuove reti service-oriented e software defined (in particolare lo slicing 5G) mettono a disposizione la possibilità di indirizzare ambiti verticali con requisiti specifici (es. settore della Salute o settore dell'Energia): questa peculiarità dovrebbe essere considerata nell'indirizzare requisiti specifici di sicurezza dei diversi ambiti in modo mirato alle peculiarità delle categorie di utenze;

   b. la definizione delle misure e delle metriche che identificano gli "elevati di sicurezza" dovrebbe avvenire nell'ambito di un coordinamento a livello europeo, come avviene per la standardizzazione delle tecnologie, per scongiurare la frammentazione e non costringere i manifatturieri a ri-certificare i propri prodotti in ogni singolo stato membro. Da questo punto di vista sarebbe meglio ricondursi a standard internazionali riconosciuti.

6. Asstel ha l'ambizione di collaborare con gli interlocutori istituzionali per formulare proposte condivise dall'industry al fine di definire un modello di risk assessment ed un modello di riferimento per la descrizione dell'architettura di rete, al fine di contemperare in modo ottimale le esigenze di sicurezza nazionale cibernetica con le esigenze di sviluppo delle reti in un contesto operativamente ed economicamente sostenibile.