CONFINDUSTRIA DIGITALE

AUDIZIONE INFORMALE DI CONFINDUSTRIA DIGITALE

IX COMMISSIONE CAMERA DEI DEPUTATI

Posizione su Atto di Governo 177

(Schema di decreto del Presidente del Consiglio dei ministri in materia di Perimetro di sicurezza nazionale Cibernetica)

Premessa

Il decreto-legge 105/2019 ha istituito il perimetro di sicurezza nazionale cibernetica (Perimetro), con il fine di assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, o dall'utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Il decreto 105/2019 intende integrare le diverse previsioni di sicurezza reti e sistemi vigenti, a partire dalla Direttiva NIS, che è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 2018, con riferimento anche alla disciplina Golden Power e per la sicurezza delle reti di telecomunicazioni e detta la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi.

La Direttiva NIS definisce le categorie di soggetti che possono essere considerati Operatori di Servizi Essenziali OSE e Fornitori di Servizi Digitali FSD, indicando che questi devono essere identificati e soggetti al controllo di autorità competenti, definendo quindi la disciplina di gestione degli eventi di sicurezza tra OSE /FSD, CSIRT nazionale ed autorità competenti.

I soggetti identificati come OSE / FSD sono 465, mentre sono state definite Autorità competenti NIS, i ministeri: Sviluppo economico, per i settori energia, infrastrutture digitali e per gli FSD; Infrastrutture e trasporti, per il settore trasporti; Economia e finanze, per i settori bancario e infrastrutture dei mercati finanziari, in collaborazione

con Banca d'Italia e Consob; Salute e Ambiente. Per alcuni ambiti – come la salute e la fornitura e distribuzione di acqua potabile – sono autorità competenti le Regioni e Province autonome di Trento e Bolzano.

La disciplina sul Golden Power si applica anche alle operazioni relative alle reti 5G la normativa sulla sicurezza della continuità di servizio delle reti di telecomunicazioni è dettata dal Decreto Ministeriale dello Sviluppo Economico del dicembre 2018.

Il decreto 105/2019 definisce un quadro normativo che vede soggetti pubblici e privati, da cui, pur non configurandosi questi come OSE o FSD, può dipendere la prestazione di un servizio dalla cui assenza o uso improprio potrebbe derivare un pregiudizio per la sicurezza nazionale.

Tali soggetti dovranno essere soggetti ad una disciplina di gestione degli eventi di sicurezza e a forme di controllo analoghe a quelle della NIS e definite all'interno del decreto stesso.

I soggetti NIS (OSE e FSD) sono secretati e, sulla base di un emendamento già introdotto su indicazione del CISR (Comitato interministeriale per la sicurezza della Repubblica) anche i soggetti facenti parte del Perimetro nazionale di sicurezza cibernetica saranno definiti con un atto amministrativo della PCM, escluso da accesso e pubblicazione, poiché si ritiene che la conoscenza di tale lista presenti particolari profili di sensibilità sotto il profilo della sicurezza in quanto consentirebbe di ricostruire il quadro complessivo degli enti pubblici e privati critici per il funzionamento del Paese.

Alla luce dell'ampio ambito applicativo del DL 105/2019, si riporteranno nel seguito considerazioni di ordine generale e si rimanda ad un focus specifico (documento allegato) relativo alla peculiare situazione degli operatori di telecomunicazioni, esposta da Assotelecomunicazioni-Asstel.

Commenti generali

1. L'implementazione del decreto 105/2019 si realizza attraverso diverse fasi (2 DPCM e 1 Regolamento) e lo schema di DPCM in esame realizza solo la prima di queste fasi provvedendo a:
   - definire le modalità e i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge

- definire i criteri con i quali i soggetti inclusi nel Perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica

E' importante che tali criteri siano facilmente modificabili per essere coerenti con la rapidità dell'innovazione del settore ICT ed evitare situazioni ben note in cui beni o servizi vengono ordinati secondo capitolati di gara ampiamente superati.

A questo fine potrebbe essere utile l'istituzione un tavolo di confronto permanente tra fornitori di soluzioni tecnologiche e soggetti appartenenti al Perimetro, con la partecipazione di CVCN. Il tavolo avrebbe l'obiettivo di analizzare le evidenze di mercato, concordandone significato e rilevanza nel contesto, e facilitare ed accelerare la piena comprensione delle esigenze dei soggetti stessi.

2. I soggetti inclusi nel Perimetro appartengono (art.3), in via prioritaria e salvo modifiche ed estensioni, ai seguenti settori di attività: governativo, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche (prodotti a duplice uso, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cibersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie, enti previdenziali / lavoro.

I soggetti appartenenti a questi settori saranno inclusi nel Perimetro se:

- hanno compiti rivolti ad assicurare la continuità di funzioni essenziali dello Stato
- svolgono attività necessarie per una varia serie di compiti critici, ma anche semplicemente se rilevanti ai fini della competitività e dello sviluppo del sistema economico nazionale

La seconda formulazione consente quindi ampio spazio per includere nel perimetro qualunque filiera si ritenga rilevante, anche solo per proteggere il know-how o le quote di mercato dell'industria nazionale.

Consideriamo corretta questa definizione in considerazione della progressiva maggiore rilevanza dei servizi digitali per la continuità del sistema socio-economico nazionale.

Sarebbe forse opportuno, anche alla luce della recente emergenza Covid-19, evidenziare esplicitamente tra i settori inclusi nel Perimetro:

- *healthcare (specificando che anche il settore privato deve essere incluso nel Perimetro e non solo la sanità pubblica, includendo in tale allargamento anche la supply chain, cioè le industrie farmaceutiche, i produttori di dispositivi medicali, i laboratori di analisi e di ricerca, ecc.),*
- *agroalimentare e sua supply chain (v. implementazione NIS in F e D)*
- *sistema idrico e sua supply chain (v. recenti attacchi in Israele)*

3. I soggetti configurano un perimetro molto esteso poiché potranno includere anche Amministrazioni locali e PMI.

Consideriamo corretto questo allargamento poiché consente di includere, a titolo d'esempio, le filiere / catene di fornitura sulle quali si basano servizi considerati essenziali. L'interconnessione digitale delle supply chain crea certamente sia un ampliamento della superficie d'attacco sia l'opportunità di una rapida perturbazione dei processi di erogazione, soprattutto quando diverse aziende concorrono all'erogazione di servizi digitali, ed è corretto richiedere all'intera supply chain un comportamento omogeneo dal punto di vista della sicurezza cibernetica. Questa corretta posizione deve però tenere conto delle difficoltà che le PMI incontrano nel dotarsi di competenze e servizi di sicurezza a costi e condizioni adatte per e loro caratteristiche dimensionali e di business. E' quindi necessario che si dedichi attenzione alle modalità con cui il Perimetro potrà essere effettivamente implementato, collaborando con le aziende provider di sicurezza, sfruttando anche le strutture private e pubbliche 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).

4. Questi soggetti dovranno sottoporsi all'obbligo di aggiornamento periodico degli elenchi delle reti, dei sistemi informativi e dei servizi informatici (art. 7) nonché di protezione delle stesse e di notifica degli incidenti.

I soggetti del Perimetro ampliano notevolmente la platea dei possibili fruitori di servizi di sicurezza (o di servizi digitali sicuri) erogati dalle imprese che forniscono servizi di sicurezza; 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 che si proceda in modo ottimale e tempestivo anche alle fasi successive dell'implementazione del Decreto 105/2019.

5. Il decreto prevede che gli "elenchi dei beni ICT" e di "architettura e componentistica" inclusi nel Perimetro (art. 7.2.b) siano definiti secondo un criterio di analisi del rischio e di gradualità (inizialmente quelli che comprometterebbero in modo irreparabile il servizio essenziale o ne comprometterebbero la riservatezza in modo irreversibile e successivamente i beni a minore livello di rischio). Di tale elenco viene richiesto un aggiornamento almeno annuale.

Riconosciamo l'importanza di un approccio graduale e il fatto che un aggiornamento periodico (almeno annuale) consenta di verificare in modo continuativo l'ottemperanza dei soggetti alle richieste del Decreto; in alcuni casi l'unione di una sola periodicità fissa con un approccio risk-based potrebbe essere poco coerente e rendere opportuno implementare una modalità di aggiornamento semplice che consenta di effettuare modifiche alla lista dei Beni ICT ogni qual volta sia necessario. Se il parametro guida per la definizione dei beni inclusi nel Perimetro è il rischio, l'aggiornamento dovrebbe essere effettuato a fronte di una variazione del rischio stesso e non con cadenza fissa. Non si può peraltro pensare che non si richieda un aggiornamento dall'analisi del rischio ad un soggetto incluso nel Perimetro che effettui una variazione significativa di un sistema ICT o di un'architettura o di componentistica inclusi nel Perimetro (es. spostamento di applicazioni o storage in cloud o viceversa).

L'analisi dovrebbe, come già richiamato precedentemente, per uniformità di comportamento e trattamento, essere basata su criteri condivisi ed omogenei (standard ISO/IEC 27001:2013, ISO/IEC 27005:2018, ISO/IEC 31000:2018 e ISO/IEC 31010:2019). Ciò consentirebbe anche ai provider di servizi di sicurezza cibernetica e di servizi ICT sicuri di predisporre cataloghi omogenei di servizi erogabili e sfruttare economie di scala e scopo, con un beneficio sia lato domanda che lato offerta.

6. La modalità con cui sono descritte le azioni che i soggetti facenti parte del Perimetro devono compiere (identificazione beni ICT, comunicazione elenchi, utilizzo di un modello di architettura e comunicazione della stessa mediante una piattaforma online, …) sembrano configurare una situazione in cui ciascun soggetto viene

considerato come a sé stante, ma poi viene chiesto nell'art. 7 al punto 2.a.2 di indicare eventuali dipendenze con altre reti, sistemi e servizi ICT di altri soggetti. La dipendenza di per sé potrebbe non essere critica e quindi si dovrebbe valutare il profilo di rischio dei soggetti sulla base di come sono realizzate le architetture interconnesse o le catene del valore servite.

Suggeriamo di evidenziare la necessità di applicare criteri omogenei di descrizione delle architetture, dei componenti e servizi e delle configurazioni di sicurezza per consentire all'organo preposto alla verifica delle stesse di poter effettuare analisi anche automatiche o semi-automatiche delle interdipendenze.

Ai fini delle interdipendenze sarebbe utile che ciascun soggetto del Perimetro potesse indicare a quale altro soggetto del Perimetro è legato in una catena del valore fisica o digitale, ma tale possibilità è preclusa dal fatto che la lista dei soggetti appartenenti al Perimetro è esclusa da accesso e pubblicazione.

Sarebbe opportuno che l'ente tecnico preposto ipotizzasse una modalità con cui gestire analizzare e, ove necessario, approfondire le interdipendenze citate.

7. Il focus del decreto è rivolto fondamentalmente alle reti ed ai sistemi informatici, introducendo vincoli informativi e gestionali su architetture e componentistica relativa ai beni ICT.

E' necessario dare il giusto spazio anche al fattore umano, indispensabile per rendere il Perimetro più robusto, con particolare enfasi a quanto attiene alla consapevolezza ed ai processi. Se è stato infatti dimostrato che infrastrutture non connesse possono essere compromesse, è anche vero che la compromissione è possibile solo grazie ad una mancanza di adeguate regole e consapevolezza sui rischi, che supportino gli operatori nel fare la cosa giusta al momento giusto nell'utilizzo dei sistemi digitali.