Memoria scritta in relazione all'esame del disegno di legge C. 3161, di conversione del decreto-legge 14 giugno 2021 n. 82 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"

Presentazione dello scrivente

Netgroup, azienda da oltre 25 anni attiva nell'area dell'Information & Communication Technology, vanta significative esperienze nella ideazione, realizzazione e gestione di sistemi di comunicazione e soluzioni informatiche innovative nei mercati Pubblica Amministrazione e Industria. Il gruppo conta oggi più di 600 dipendenti distribuiti nelle sedi di Roma, Napoli, Firenze, Torino, Bari e Brighton (UK) oltre a presidi su tutto il territorio nazionale. Un centro R&D, due centri di formazione Netgroup Academy, impegnati nell'ambito della Formazione Professionale nel settore ICT.

Netgroup basa il suo modello aziendale sulla flessibilità, sul concetto di impresa "a rete" e sul coinvolgimento diretto di risorse altamente qualificate. È proprio la competitività, non solo sotto il profilo delle capacità professionali e di "offerta architetturale", ma anche sotto quello dei costi e dei margini, che consente oggi a Netgroup di presentarsi come un interlocutore qualificato in tutti i settori dei servizi ICT per il Cittadino e le Imprese. L'elevato know-how acquisito da Netgroup nel settore dell'ICT, sia nel campo della consulenza, dell'outsourcing, dello studio dei processi aziendali, che in quello del "solution management", della fornitura di applicazioni, di infrastrutture e di servizi, permette di offrire le soluzioni più innovative, rispondendo sempre in maniera immediata alle esigenze dei propri clienti, sia nel settore pubblico che in quello privato. Netgroup ha già maturato con successo esperienze per Clienti Pubblici e Privati: LEONARDO, TIM, Aeroporti Di Roma, RAI, Banca d'Italia, Regione Campania, SOGIN, US-Navy, NATO, Provincia di Napoli, Università degli Studi di Napoli "Federico II", Università di Salerno, etc. Netgroup dispone di competenze metodologiche e progettuali core e si avvale di partner per segmenti specifici del progetto. Conseguentemente, la struttura organizzativa di Netgroup è flessibile e basata sul modello delle competenze core, che sono di volta in volta allocate ai progetti e alle commesse. Questo modello operativo favorisce alta efficienza, a vantaggio anche del Cliente, promuovendo la specificità e l'efficacia delle soluzioni. La metodologia adottata da Netgroup le consente di proporsi come partner ideale per le imprese e le Pubbliche Amministrazioni, grazie a competenze strategiche che consentono di: intervenire nella reingegnerizzazione di processi e di organizzazioni, gestendo contestualmente il processo di cambiamento derivante; definire ed implementare architetture tecnologiche innovative; condurre globalmente progetti complessi ed articolati; garantire la continuità dell'erogazione del servizio; monitorare la qualità del servizio erogato ed intervenire in modalità attiva/proattiva dall'inizio del ciclo di progettazione.

Nell'ambito dei servizi legati alla cybersicurezza e alla conduzione di infrastrutture e sistemi, Netgroup eroga attività di analisi, progettazione, implementazione e gestione di infrastrutture e sistemi di sicurezza, servizi SOC in ambito Industriale OT e Enterprise IT, NOC per i servizi di monitoraggio infrastrutturale, SPOC per i servizi di IT fleet management. Netgroup propone attività di Information Security Assessment, con servizi di vulnerability assessment e remediation, Analisi dati del Surface, Deep e Dark web, servizi consulenziali con attività di Framework Assurance, Alta formazione e Consulenza anche grazie a un accordo di collaborazione con la Fondazione YMCA Italia e con l'International Istitute for Counter Terrorism che opera all'interno dell'istituto IDC di Tel Aviv, Israele.

NETGROUP
SOFTWARE & NETWORK ENGINEERING

Memoria scritta

Considerazioni sull'Agenzia Nazionale per la Cybersicurezza

L'attuale scenario nazionale e internazionale, di sempre maggiore digitalizzazione e informatizzazione delle attività, ha conosciuto una crescente escalation di episodi di cybercrime e di cyberwarfare tale da rendere indispensabile una presa di coscienza decisa in materia di cybersicurezza, che diviene perno centrale nella strategia implementativa della Transizione Digitale prevista nel PNRR.

La cybersicurezza assume oggi, inevitabilmente, rilevanza strategica per il sistema Paese e pertanto diviene oggetto di un'importante rivoluzione normativa e operativa.

Il DL 82/2021 evidenzia, in tal senso, la centralità della materia per la politica nazionale, espressa dalla volontà di identificare nell'Agenzia per la cybersicurezza nazionale l'autorità in materia di cybersicurezza, anche riunendo funzioni prima distribuite tra differenti Ministeri e Istituti Governativi, sotto la diretta responsabilità del Presidente del Consiglio dei Ministri.

L'Agenzia collaborerà con il Comitato Interministeriale e con le agenzie dei servizi di informazione, evidenziando il tal modo la **consapevolezza del Governo della natura trasversale della sicurezza cybernetica**, che **necessita di verticalizzazioni tematiche nei settori vitali del sistema Paese**, dalla pubblica amministrazione alla difesa nazionale, dall'università all'industria, dalla finanza alle infrastrutture critiche (rete elettrica, televisiva, di telecomunicazione, ferroviaria, stradale).

In considerazione del crescente rischio e dell'importanza vitale degli asset impattati, sarà fondamentale **definire e porre in sicurezza nel più breve tempo possibile il perimetro di sicurezza nazionale**, attività essenziale per garantire la **resilienza del Paese contro le cyber minacce**, con una **transizione rapida ed efficace** verso un assetto operativo dell'Agenzia che dovrà rapidamente concretizzare e indirizzare la recente copiosa produzione normativa in tema di cybersicurezza, operando non solo in logica reattiva, ma principalmente in modalità proattiva.

È indispensabile un ruolo centrale dell'Agenzia nella **definizione di linee guida nell'ambito della cybersicurezza sia per la Pubblica Amministrazione sia per il settore privato**, anche a carattere di cogenza, promuovendo ogni necessaria azione per l'applicazione diffusa delle stesse nonché per il **controllo dell'applicazione delle norme anche mediante procedimenti sanzionatori**, con particolare riferimento all'adesione ai dettami della **Direttiva NIS dell'Unione europea** da parte dei soggetti interessati.

In particolare, la definizione delle linee guida dovrà tener conto della specificità e strategicità di quegli **Enti che gestiscono le infrastrutture critiche del sistema Italia**, per le quali potranno essere definite **policy di sicurezza ad hoc maggiormente stringenti**,

promuovendo una collaborazione diretta fra queste e l'Agenzia mediante partnership improntate non solo allo sviluppo e trasferimento tecnologico tra mondo della ricerca e industriale, ma anche al controllo diretto dell'attuazione delle politiche di cybersicurezza nonché alla valutazione della postura di sicurezza di quei soggetti pubblici e privati considerati strategici per il Paese.

In tal senso, **sarebbe auspicabile la predisposizione di sedi territoriali dell'Agenzia**, in contesti specifici nei quali **sviluppare e gestire sia relazioni con Centri di Eccellenza nell'ambito della cybersicurezza, sia con i principali stakeholder**, portando ad una maggiore efficienza dei processi e a un più stretto coinvolgimento delle realtà direttamente interessate.

Il ruolo centrale dell'Agenzia non dovrà passare poi per la sola difesa del perimetro di sicurezza nazionale ma dovrà anche **focalizzarsi sullo sviluppo di tecnologie innovative e di buone pratiche a supporto della cybersicurezza**, mantenendo una forte focalizzazione su attività di ricerca e sviluppo con carattere di spiccata innovatività, coinvolgendo attivamente i principali Centri di Ricerca e Competence Center nazionali e internazionali, promuovendo processi di ricerca e industrializzazione di prodotti e servizi che rendano **il Paese** sempre più **indipendente da quei soggetti extra-europei** oggi principali fornitori mondiali di soluzioni di sicurezza.

Compito dell'Agenzia dovrà essere anche quello di **creare consapevolezza e competenza in materia di cybersicurezza** nel sistema Paese definendo, in collaborazione con gli enti formativi istituzionali, soggetti pubblici e privati, percorsi di upskilling e reskilling delle risorse, con particolare riferimento a profili quali **Cybersecurity Auditor, Digital Risk Manager, Cyber-Intelligence Analyst**, in linea con le norme e le politiche di sicurezza definite per ogni area tematica ritenuta sensibile nell'ambito della sicurezza nazionale.

L'Agenzia dovrà svolgere un ruolo consultivo di primo piano nei confronti di quei soggetti pubblici e privati di interesse rilevante per la sicurezza nazionale, secondo i principi del Golden Power, ruolo rivestito anche nei confronti del legislatore nazionale nell'attività di produzione di contenuti normativi. Tale ruolo assicurerà l'**attuazione del paradigma della 'Security by Design'** affinché i requisiti di sicurezza informatica, le **linee guida e le direttive europee** siano incorporate in tutti i progetti di trasformazione digitale sin dalla loro definizione iniziale, in particolar modo in quei progetti strategici di respiro europeo e internazionale quale il progetto GAIA-X, attraverso una partecipazione attiva nella definizione di regole chiare in termini di sicurezza e nelle attività volte all'implementazione dell'infrastruttura cloud federata.

Auspicabile la creazione, in seno all'Agenzia, di un Ufficio focalizzato nella **gestione dei rapporti e nel coordinamento delle attività con la rete di Centri nazionali europei** operanti nel campo della cybersicurezza. Il ruolo di tale Ufficio sarà fondamentale non solo per assicurare che le norme e le politiche di sicurezza nazionali vengano sviluppate in maniera armonica rispetto alle direttive e alle linee guida comunitarie, ma anche per porre in essere tutte le azioni congiunte necessarie per la **gestione proattiva e reattiva delle minacce cyber rispetto al perimetro europeo e nazionale**. Inoltre, sul modello dell'European Data Protection Board (EDPB), costituito dai rappresentanti delle Autorità di Protezione dei Dati di tutti i paesi membri dell'Unione, è auspicabile che venga istituito un **organismo sovranazionale** volto a coordinare l'attuazione delle previste misure tecnico-normative e a portare a fattor comune le migliori pratiche e le informazioni strategiche per il contrasto alle minacce cyber.

In definitiva, l'Agenzia per la cybersicurezza nazionale dovrà costituire da un lato il principale baluardo nei confronti della crescente pericolosità delle minacce cibernetiche, anche dal punto di vista formativo e informativo, dall'altro dovrà rappresentare il riferimento principale per quei soggetti pubblici e privati le cui attività costituiscono la spina dorsale del sistema Paese, mantenendo un ruolo di centralità nelle relazioni con i propri omologhi europei e con le corrispondenti Agenzie dei paesi alleati.

Roma, 30 Giugno 2021

NETGROUP

Il Presidente

Giuseppe Mocerino