DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

Agenzia nazionale sulla Cybersicurezza

Audizione di Paolo de Rosa, CTO del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri

1. Scenario

Grazie Presidente,

Onorevoli Deputate e Deputati,

Nel mio intervento, per quanto di mia competenza, cercherò di evidenziare i rischi informatici più insidiosi che il sistema paese deve attrezzarsi a fronteggiare e ad individuare l'approccio più lungimirante per affrontarli, anche guardando alle strategie di Cyber Security adottate da altri Paesi. Con riferimento alla proposta legislativa in esame mi concentrerò sulla introduzione della nuova Agenzia per la Cyber Security Nazionale (art. 5) e sulle sue competenze (art. 7).

Entrando nel merito della questione, la grande sfida che ci attende negli anni a venire sarà quella di governare la trasformazione digitale pervasiva della società, elaborando meccanismi di tutela idonei a fronteggiare le nuove minacce alla sicurezza nazionale, che non deriveranno più esclusivamente da attori stranieri.

Senza sottovalutare l'attività cibernetica statuale, che può rappresentare certamente una delle minacce più dannose per i nostri interessi nazionali, occorre pensare anche alla minaccia rappresentata dalla criminalità informatica, sempre più capillarmente diffusa.

Per la stragrande maggioranza dei cittadini e delle imprese del nostro paese, e quindi -anche- per la stragrande maggioranza dei fornitori di infrastrutture

critiche e dei fornitori di servizi pubblici, la minaccia principale è rappresentata da attacchi informatici diffusi e particolarmente insidiosi come ad esempio i **ransomware**.

E l'effetto cumulativo di una potenziale incapacità di gestire questo tipo di rischio è particolarmente preoccupante, come recentemente reso più evidente durante l'emergenza pandemica da covid-19: quando le attività di un intero paese sono necessariamente interconnesse (telelavoro, didattica a distanza, servizi pubblici e assistenza sanitaria erogati on line, etc.) tanti piccoli danni possono equivalere ad un rischio cumulativo di importanza nazionale.

Questo è il rischio per la sicurezza informatica più insidioso: non la minaccia da, ma la minaccia per; e - quindi - non la perdita di dati, ma l'impatto sulle operazioni, grandi e piccole, che impedisce a persone e aziende di vivere la propria vita quotidiana. Il volume totale rende questo tipo di minaccia quella di maggior impatto che dobbiamo affrontare. Ed abbiamo visto che può colpire il sistema sanitario come avvenuto in Irlanda con il ransomware CONTI, che ha impedito al sistema sanitario di funzionare con gravi conseguenze per la salute pubblica.

Il ransomware è stato storicamente appannaggio di gruppi di criminalità informatica di fascia alta con accesso a capacità e competenze tecniche avanzate, con sede in giurisdizioni terze che chiudono un occhio o in ogni caso non riescono ad agire per perseguire questi gruppi.

Ma l'ecosistema si sta evolvendo attraverso quello che chiamiamo Ransomware as a Service (RaaS) ovvero un modello di business "As a Service" che consente agli attori meno esperti nel ransomware di acquisire strumenti per condurre i propri attacchi.

Per rispondere efficacemente a questo nuovo tipo di minacce occorre creare una consapevolezza diffusa che consenta di sviluppare una vera e propria Cyber Resilienza non solo delle infrastrutture nazionali critiche ma anche delle imprese e della società civile: l'industria, il mondo accademico, gli operatori privati, le istituzioni pubbliche hanno tutti un ruolo da svolgere in questa battaglia. Ma perché questo sia possibile occorre avere una regia unica capace

di assicurare il necessario coordinamento interno per l'elaborazione e l'attuazione di una strategia nazionale di cybersicurezza.

2. Perché un'agenzia nazionale per la cybersecurity

Alla luce dello scenario appena tratteggiato risulta evidente l'importanza di disporre di un'Agenzia Nazionale per la Cybersecurity, di cui del resto si sono già dotati altri paesi (Francia, Germania e UK). L'esempio del Regno Unito risulta a mio avviso illuminante. A partire dall'istituzione del National Cyber Security Centre (NCSC) nel 2016 attraverso un partenariato tra Governo, forze dell'ordine, Intelligence e settore privato, il Regno Unito è riuscito ad imprimere una svolta lungimirante alla lotta ai cyber attack. Sono riusciti ad aumentare la resilienza in tutti i settori della loro infrastruttura nazionale critica, costruendo intese con aziende, enti e istituzioni per sviluppare strumenti e consigli di sicurezza informatica accessibili e utilizzabili da cittadini ed imprese. A livello UE, abbiamo potuto riscontrare, nelle nostre interlocuzioni per i progetti in corso, che in questa stessa direzione, si sono mossi quasi tutti gli Stati Membri. In Francia, ad esempio, nel 2009 è stata istituita l'ANSSI, posta alle dirette dipendenze del Segretario generale per la difesa e la sicurezza nazionale, che se ne avvale per l'esercizio delle proprie attribuzioni nel campo della sicurezza cibernetica, tese anche a supportare il Primo ministro ai fini dell'adozione delle politiche del Governo in materia.

In Germania è stato istituito nel 1991 il BSI, l'ufficio federale per la sicurezza informatica. Anche la Romania (che ospita il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca) sta al momento provvedendo alla disciplina normativa della propria Autorità di cybersicurezza che prevede di assumere circa 1200 persone entro il 2030.

Nei tavoli tecnici e nei confronti aperti per la definizione della strategia Cloud nazionale abbiamo potuto constatare direttamente come queste Agenzie svolgano un ruolo chiave per i Governi nazionali, garantendo un supporto tecnico di altissimo livello e assicurando una costante capacità di coordinamento anche con le corrispondenti Agenzie degli altri Stati Membri.

Pertanto non possiamo che salutare con favore l'istituzione dell'**Agenzia per la cybersicurezza nazionale** prevista all'art. 5 del testo in esame, che consentirà anche al nostro paese di dotarsi di un'Autorità unica, capace di accentrare le

competenze in materia, finora esercitate in modo frammentato da diverse istituzioni.

3. I vantaggi di una governance unificata

L'art. 7 del testo in esame definisce le funzioni dell'istituenda Agenzia per la cybersicurezza nazionale, assicurando una gestione unitaria delle diverse competenze sino ad oggi esercitate da altre istituzioni, secondo una logica di razionalizzazione certamente auspicabile, e in particolare con riferimento agli ambiti:

- della sicurezza delle reti e dei sistemi informativi (NIS)
- del perimetro di sicurezza nazionale cibernetica (PERIMETRO)
- della sicurezza delle comunicazioni elettroniche (TELCO)
- della sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture digitali delle pubbliche amministrazioni anche in relazione ai servizi cloud
- delle certificazioni di cybersicurezza

Sul punto c'è da dire che sono stati proprio gli operatori coinvolti ad invocare una unicità di indirizzo e di azione, in questa materia, sia in relazione alla definizione delle misure di sicurezza cui attenersi, sia in relazione all'esercizio delle funzioni ispettive, accertative e sanzionatorie.

Per quanto di diretta competenza del Dipartimento per la trasformazione digitale mi preme osservare che l'Agenzia per la cybersicurezza nazionale assumerà anche tutte le funzioni in materia di cybersicurezza già attribuite ad Agid dalle disposizioni vigenti e, in particolare, quelle previste all'articolo 51 del Codice dell'Amministrazione Digitale, nonché in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 dello stesso CAD.

L'Agenzia assumerà anche i compiti di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 già attribuiti all'Agenzia per l'Italia digitale e, pertanto, con proprio regolamento definirà:

- i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione (private cloud);
- le caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione (public cloud);
- i termini e le modalità con cui le pubbliche amministrazioni devono effettuare le migrazioni dei loro CED e dei relativi sistemi informatici privi dei requisiti fissati con il suddetto regolamento.

L'Auspicio è che nella stessa logica di razionalizzazione e accentramento delle competenza che caratterizza il presente intervento normativo, alla nascente Agenzia sia affidato anche il processo di qualificazione dei Cloud service provider sulla base dei criteri di cui al già citato regolamento, nell'ambito del c.d. Cloud della pubblica amministrazione.

All'Agenzia è altresì attribuita una funzione di supporto allo sviluppo di capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza, in un'ottica di autonomia strategica nazionale ed europea nel settore, con un forte impulso al partenariato pubblico-privato, alla creazione di spin-off di settore e al rafforzamento delle piccole-medie imprese, assicurando anche un coordinamento europeo con enti omologhi. Questa è sicuramente una funzione di massimo rilievo, poiché solo la capacità di produrre alcune soluzioni tecnologiche autoctone o europee ci consentirà di raggiungere quel livello necessario di autonomia strategica che caratterizzerà l'indipendenza di un paese nel prossimo futuro.

Sarà demandata all'Agenzia anche l'attuazione del PNRR, deliberato dal Consiglio dei ministri lo scorso 29 aprile 2021 e che come è noto prevede apposite progettualità nell'ambito della cybersicurezza e della architettura nazionale di sicurezza cibernetica quale fattore necessario per assicurare lo sviluppo e la crescita dell'economia e dell'industria nazionale, ponendo la cybersicurezza a fondamento della trasformazione digitale.

All'Agenzia sarà inoltre affidata la gestione coordinata, con i diversi attori coinvolti nazionali e europei, delle attività di prevenzione, preparazione e

mitigazione a situazioni di crisi, anche mediante la costituzione, nell'ambito della stessa agenzia, del Nucleo per la cybersicurezza.

Nella prospettiva della Cyber Resilienza e di un approccio globale e lungimirante al problema degli attacchi cyber credo sia importante sottolineare i compiti di "*svolgere attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia*" e di "*promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati*".

In conclusione, stanti anche gli ingenti investimenti previsti dal PNRR per la cybersicurezza, il presente intervento normativo pone finalmente le basi per imprimere anche nel nostro paese una significativa svolta nella lotta alle minacce cyber. La cybersicurezza deve diventare una questione di sicurezza nazionale e una questione di politica pubblica, così che il cyberspazio diventi principalmente un dominio di interazione civica e commerciale che consenta la crescita economica e benefici sociali più ampi per tutti e che, per questo, rimanga libero aperto pacifico e sicuro.