DPCM 1° agosto 2015

Al Signor Ministro degli Affari Esteri e della Cooperazione internazionale
Al Signor Ministro dell'Interno
Al Signor Ministro della Difesa
Al Signor Ministro della Giustizia
Al Signor Ministro dell'Economia e delle Finanze
Al Signor Ministro dello Sviluppo Economico
Al Signor Sottosegretario di Stato alla Presidenza del Consiglio – Autorità delegata per la Sicurezza della Repubblica
Al Signor Direttore Generale dell'Agenzia per l'Italia Digitale
Al Signor Consigliere militare del Presidente del Consiglio dei ministri
Al Signor Direttore Generale del Dipartimento delle informazioni per la sicurezza
Al Signor Direttore dell'Agenzia informazioni e sicurezza esterna
Al Signor Direttore dell'Agenzia informazioni e sicurezza interna
Al Signor Ministro per la Semplificazione e la Pubblica Amministrazione

Premessa

L'Italia si è da alcuni anni dotata di un'architettura istituzionale con l'obiettivo di ricomporre e mettere a sistema i molteplici attori, pubblici e privati, che operano nel campo della sicurezza dello spazio cibernetico. È un primo passo, che è stato compiuto nell'ambito del quadro legislativo esistente e, doverosamente, nel rispetto delle attuali esigenze di finanza pubblica.

La definizione dei punti cardine del sistema ha consentito di approvare in breve tempo il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il correlato Piano nazionale, strumenti rivolti a porre il Paese in linea con i principali partner internazionali.

Occorre ora proseguire con determinazione nell'attuazione degli indirizzi strategici ed operativi identificati, ponendo in essere tutte le linee di azione necessarie sotto il profilo tecnico, organizzativo, procedurale e della collaborazione internazionale, che consentano di assicurare ai nostri cittadini uno spazio cibernetico in cui possano essere esercitate, in una cornice di sicurezza, diritti fondamentali e scambio di conoscenze, intraprese attività economiche ed intessute relazioni sociali, cogliendo così tutte le opportunità offerte dalle nuove tecnologie dell'informazione e della comunicazione.

Indirizzi generali

Per il raggiungimento di queste finalità, da una prima ricognizione sullo stato di attuazione degli indirizzi del Quadro strategico e del Piano nazionale, è emersa innanzitutto l'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi.

Sentito il CISR nella riunione del 19 maggio u.s., ritengo quindi opportuno fissare puntuali linee d'azione che tutti i soggetti coinvolti dovranno seguire per accelerare la realizzazione degli obiettivi indicati. Ciò deve determinare un allineamento degli assetti strategici agli standard internazionali, che consenta al nostro Paese di rapportarsi autorevolmente con i principali partner internazionali.

I principi fondamentali che devono guidare il percorso verso l'obiettivo indicato sono:

- un maggiore e più efficace coordinamento, nonché l'integrazione delle funzioni dei diversi soggetti pubblici, tenendo conto che il quadro di competenze rimane ancora frammentato sotto il profilo legislativo;

- lo sviluppo delle relazioni con il settore privato, realizzando un efficace e capillare partenariato con tutti gli operatori non pubblici a cui è affidato il controllo di infrastrutture informatiche e telematiche da cui dipendono ormai funzioni essenziali per il sistema-Paese e per la fruizione dei diritti fondamentali degli individui.

Misure rivolte alla amministrazione:

a. il potenziamento della capacità di reazione

Ogni singola Amministrazione ed Organo, componenti l'architettura nazionale di sicurezza, deve potenziare la capacità di reazione agli eventi cibernetici sotto il profilo tecnico, adottando e attenendosi a procedure improntate al massimo coordinamento sia interno che tra le Amministrazioni. A ciò si deve aggiungere l'impegno, nell'ambito di ciascuna Amministrazione, a provvedere affinché, nel quadro delle pianificazioni organizzative e finanziarie di competenza, siano destinate risorse umane e finanziarie adeguate agli assetti rivolti alla funzione della sicurezza cibernetica ed alla protezione informatica.

Tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici devono dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, l'Agenzia per l'Italia digitale dovrà rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

In questo quadro, in particolare, il Nucleo per la sicurezza cibernetica, il CERT nazionale ed il CERT della Pubblica Amministrazione dovranno adottare, in attuazione di quanto previsto dagli indirizzi operativi del Piano nazionale, le iniziative necessarie a potenziare l'operatività, pianificando quanto prima il pronto allineamento agli standard internazionali di riferimento.

b. il coordinamento interistituzionale

Nel contempo, deve essere da subito assicurato il raggiungimento dell'ottimale funzionamento del coordinamento interistituzionale, in un'ottica di massima integrazione della risposta all'evento, tenuto conto che ogni singolo evento può assumere natura sistemica.

Per questo fine, le SS.LL. impartiranno le necessarie disposizioni affinché ciascuna Amministrazione, anche in funzione della partecipazione al Nucleo per la sicurezza cibernetica, improntì la propria azione al raggiungimento dell'interesse generale del Paese a che le informazioni sugli attacchi e sugli altri eventi di rilievo in ambito cibernetico vengano immediatamente e puntualmente condivise, secondo le procedure concordate, contestualmente alle azioni messe in atto da ciascuna Amministrazione per la immediata tutela e il ripristino dei sistemi.

Il massimo coordinamento deve essere assicurato anche nell'ambito dell'attività degli Organismi di informazione per la sicurezza, in linea con il modello previsto dalla legge n. 124/2007 secondo cui il Presidente del Consiglio, e l'Autorità delegata ove istituita, si avvalgono del DIS per assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nelle analisi e nelle attività operative dei Servizi di informazione ed al DIS è affidato il compito di coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Nel quadro del coordinamento tra i diversi attori del sistema di reazione in caso di evento cibernetico, deve infine essere accelerata la predisposizione di una rete di comunicazione classificata, allo scopo di evitare ritardi o disfunzioni nella fase di gestione dell'evento, garantendo un continuo e sicuro scambio informativo tra le Amministrazioni interessate, i CERT ed il Nucleo per la Sicurezza Cibernetica.

Azioni per il partenariato pubblico-privato

L'innalzamento delle capacità in materia di sicurezza nel settore pubblico non è di per sé in grado di assicurare la sicurezza *tout court* dello spazio cibernetico di pertinenza del Paese, senza un efficace diffuso coinvolgimento degli operatori privati, a partire da quelli cui fanno capo segmenti importanti dell'infrastruttura cibernetica nazionale. La *best practice* internazionale individua, infatti, come momento fondamentale il partenariato pubblico-privato, posto che dalla funzionalità e resilienza dei sistemi e delle reti affidati a privati dipendono funzioni essenziali sia per il sistema-Paese, sia per la fruizione dei diritti fondamentali degli individui.

In tale contesto, l'opera di sensibilizzazione effettuata nei confronti degli operatori economici privati che gestiscono infrastrutture critiche e di altri soggetti di rilevanza strategica nazionale, già avviata in diversi settori di interesse primario, va estesa ad altri settori economici potenzialmente esposti ad attacchi cibernetici di portata sistemica.

Le modalità di individuazione degli operatori privati e lo sviluppo delle relazioni dovranno essere definite in modo coordinato nelle sedi individuate dall'architettura istituzionale e, in particolare, nell'ambito dell'Organo collegiale di supporto al CISR. Ciò al fine di evitare dannose sovrapposizioni e duplicazioni, suscettibili tra l'altro di ingenerare, presso gli operatori privati, confusione circa ruoli e competenze della parte pubblica. Deve, infatti, essere assolutamente garantito che gli operatori privati abbiano una visione unitaria dell'azione statuale e chiari i punti di riferimento istituzionali in materia di protezione cibernetica e sicurezza informatica.

La ricerca nazionale

Nel percorso di accrescimento delle capacità e potenzialità del Paese, inoltre, deve essere riconosciuto un fondamentale rilievo, attese le repentine evoluzioni tecnologiche cui è soggetta la materia, al settore della ricerca e sviluppo delle attività di sicurezza informatica e alla cooperazione, per queste finalità, con università e centri di ricerca anche privati.

Tale attività tanto più risulta cruciale per la sicurezza informatica nazionale quanto più va evidenziandosi l'esistenza e il possibile ulteriore sviluppo di strumenti di intrusione indebita negli apparati informatici dall'elevato potenziale invasivo, che si vanno sempre più configurando come una minaccia a livello sistemico.

Nella consapevolezza dell'esigenza di una compiuta regolamentazione di tali strumenti, anche nella prospettiva della salvaguardia dei diritti della persona, si rende intanto necessario che, grazie alle sinergie con gli enti di ricerca, le infrastrutture strategiche sviluppino strumenti di difesa e reazione il più possibile avanzati dal punto di vista tecnologico.

Anche nell'ambito di queste attività, le Amministrazioni e gli Organi che compongono l'architettura istituzionale, nella definizione di accordi e intese di collaborazione, dovranno improntare la propria azione, per le stesse considerazioni già espresse, ad un puntuale raccordo e coordinamento delle iniziative, evitando ogni iniziativa unilaterale e non previamente concordata nella sede collegiale dianzi richiamata.

La cooperazione internazionale

Il conseguimento degli obiettivi indicati rappresenta una condizione imprescindibile nel contesto della cooperazione internazionale: i rapporti bilaterali e multilaterali presuppongono, infatti, un comune livello di preparazione e di interoperabilità, senza il quale l'Italia non può partecipare a pieno titolo e quale partner di rango primario ai relativi consessi internazionali.

Per queste finalità è altresì necessario che le SS. LL. impartiscano disposizioni, ognuno nel proprio ambito di competenza, affinché, in particolare nei principali contesti multilaterali, NATO e UE, la partecipazione nazionale sia la risultante di un approccio di sistema e, in quanto tale, frutto di una preliminare attività di coordinamento-Paese. Ciò risulta indispensabile in fase sia ascendente (definizione della posizione nazionale) che discendente (governo degli obblighi conseguenti).

Disposizioni finali

Ritengo importante che le azioni necessarie in ciascuna Amministrazione per il perseguimento degli obiettivi indicati dalla presente direttiva siano svolte con la più ampia condivisione delle finalità tra coloro che saranno chiamati a darvi attuazione, essendo la consapevolezza e la motivazione da parte di ciascun responsabile o addetto, ai diversi livelli, cruciale per la buona riuscita di iniziative di carattere sistemico e di così ampia portata.

Sicuro della particolare sensibilità e della preziosa opera che le SS.LL. sapranno dispiegare perché possano essere attuate le indicazioni delle presente direttiva, confido perciò anche nella conseguente adozione di adeguate iniziative di comunicazione nell'ambito di ciascuna Amministrazione.

Il Sottosegretario di Stato, Autorità delegata per la sicurezza della Repubblica, e il Direttore generale del DIS sono incaricati di seguire l'attuazione delle linee di azione indicate, per gli aspetti di competenza, e di riferirmi con cadenza semestrale.

Il Presidente del Consiglio dei ministri
Matteo Renzi