PUNTO DI VISTA

Bruno Frattasi

G7 – Un nuovo capitolo per la cybersicurezza

Il 16 maggio 2024 Roma è stata il palcoscenico della prima riunione del gruppo di lavoro G7 sulla sicurezza cibernetica, un evento voluto e costruito dalla presidenza italiana. Riproponiamo in questo numero di Gnosis la dichiarazione integrale del prefetto Bruno Frattasi, direttore generale dell'Agenzia per la cybersicurezza nazionale (Acn) in qualità di presidente del nuovo gruppo di lavoro G7.

«Oggi, a Roma, per la prima volta in ambito G7 e su iniziativa della Presidenza italiana, si è riunito il Gruppo di lavoro cybersicurezza del G7 nel formato policy makers di alto livello insieme alle agenzie e centri per la sicurezza e resilienza dello spazio cibernetico. Ringrazio il Ministero degli Esteri e della Cooperazione Internazionale per averci ospitato. Ho presieduto un incontro nel quale abbiamo interagito come una comunità, aperta al confronto ed alla condivisione delle politiche di sicurezza cibernetica. Nei mesi scorsi abbiamo costruito con le altre delegazioni le condizioni per dare avvio a questa cooperazione che vogliamo sia permanente d'ora in avanti.
Nei miei incontri con i Capi delle altre agenzie, nei mesi scorsi, ho presentato la proposta italiana. Insieme ai miei collaboratori l'abbiamo via via affinata, riscuotendo adesioni convinte. La nostra iniziativa punta ad una stretta collaborazione internazionale per la resilienza dello spazio cibernetico. È stata menzionata nel comunicato della Ministeriale esteri G7 di Capri (19 aprile) perché complementare agli sforzi da tempo intrapresi dai Paesi G7 a favore di uno spazio cibernetico sicuro, affidabile, aperto, retto dai principi e dalle norme del diritto internazionale.

Tutte le agenzie dei Paesi G7 e l'UE hanno partecipato ai lavori, insieme ai vice consiglieri per la sicurezza nazionale di Stati Uniti e Giappone e al direttore Sicurezza del Foreign Office britannico.
Ai colleghi intervenuti va il mio ringraziamento per il loro impegno e contributo alla discussione e per aver dato vita alla comunità delle agenzie cyber del G7. Proseguiremo in questo formato il nostro dialogo per operare insieme al meglio delle nostre capacità nell'affrontare le numerose e complesse sfide su temi centrali e prioritari di politica di sicurezza e resilienza dell'ecosistema digitale.
Nella prima sessione di lavoro si è parlato dell'interdipendenza tra cybersicurezza e intelligenza artificiale (IA). L'IA è il tema centrale della Presidenza italiana del G7.
Ne abbiamo discusso ampiamente, facendo seguito alle interlocuzioni dello scorso anno avvenute nel contesto del Processo di Hiroshima. È una nostra responsabilità comprendere meglio e monitorare gli impieghi attuali e quelli potenziali dei sistemi di IA (compresi i cd. Large Language Models, LLM). Sistemi e modelli possono essere utilizzati per fini malevoli, ma consentono anche di monitorare le minacce ed abbattere i rischi connessi a tali impieghi. L'obiettivo è duplice: conoscere le opportunità che questa tecnologia offre nel settore della cybersicurezza e, al contempo, governare il rischio che possa derivare da utilizzi imprudenti o malevoli. Tutti noi condividiamo l'importanza che i sistemi di IA vengano concepiti, sviluppati e distribuiti in modo sicuro e responsabile, come previsto dalle Linee guida, a cui abbiamo aderito lo scorso novembre, per uno sviluppo sicuro dei sistemi IA, secondo il principio di "sicurezza by design".
Nel corso della seconda sessione abbiamo discusso sulle opzioni di policy per rafforzare la sicurezza e la resilienza dell'ecosistema digitale di fronte a crescenti minacce informatiche, tra cui il ransomware. Un fenomeno criminale che interessa un'ampia gamma di organizzazioni e settori, incluso quello sanitario, e che ha un significativo impatto economico e sociale, e solleva profili di sicurezza nazionale. Nel riconoscere che la prevenzione e il contrasto agli attacchi ransomware richiedono l'adozione di misure multidisciplinari, il Gruppo ha sottolineato l'importanza di promuovere policy e azioni volte a disarticolare il modello di impresa criminale che caratterizza questi attacchi, rendendoli economicamente sempre meno vantaggiosi.
In questo senso, il Gruppo ha richiamato l'importanza che i Paesi disincentivino il pagamento dei riscatti e sostengano i principi di trasparenza, affidabilità e sicurezza dell'utilizzo di valute virtuali. Inoltre, di fronte ad una minaccia crescente e mutevole, il Gruppo ha espresso la volontà di supportare l'adozione di policy e meccanismi volti a rendere sicura e resiliente l'innovazione tecnologica e digitale. Tali meccanismi comprendono la certificazione di cybersicurezza di prodotti, dispositivi e servizi digitali, compreso l'Internet delle Cose. Il Gruppo ha riaffermato l'importanza di distribuire prodotti dell'Internet delle Cose affidabili e ha convenuto di discutere le modalità per gestire i rischi alla catena di approvvigionamento al fine di raggiungere tale obiettivo. Si tratta di un fondamentale strumento per la salvaguardia degli utenti, del mercato digitale e della sicurezza dei Paesi G7.

La terza ed ultima sessione è stata dedicata alla collaborazione tra di noi, per rafforzare la sicurezza informatica delle infrastrutture in settori critici per la società e l'economia, incluso quello energetico. Il Gruppo ha discusso di come operare per favorire insieme agli operatori delle infrastrutture critiche la sicurezza dell'intera catena di approvvigionamento, per ridurre fortemente il rischio che componenti tecnologiche possano diventare veicolo per la diffusione di un attacco alle reti infrastrutturali. Un settore in cui è importante applicare il principio di security-by-design attraverso l'acquisizione di componenti che rispondano ad alti standard di sicurezza.
Coopereremo sempre meglio e ci consulteremo tutte le volte che ne avremo la necessità. Questo è l'impegno che abbiamo assunto insieme. Scambieremo informazioni sulle principali minacce cyber che riguardano le infrastrutture critiche, sugli incidenti, nonché sulle misure di sicurezza che possono essere adottate dagli operatori critici per farvi fronte.
Crediamo tutti molto nel coordinamento con il settore privato. In questo senso la nostra Agenzia, forte dell'esperienza della Legge Perimetro ha una naturale propensione a sviluppare l'interazione con il mondo delle imprese e quello della ricerca.
La riunione di oggi ci dice che siamo sulla giusta strada. Il dialogo permanente e la cooperazione tra i centri e le agenzie che si occupano di sicurezza e resilienza dell'ecosistema cyber e digitale contribuiscono a rafforzare la sicurezza nazionale e collettiva dei Paesi G7. Per essere efficace la cooperazione richiede continuità e ci siamo impegnati in questo senso. Siamo determinati a plasmare insieme una collaborazione dinamica, basata sulla condivisione di orientamenti ed esperienze nazionali e sulla definizione di soluzioni di policy e operative.
Il Sottosegretario Mantovano, che ringrazio per aver condiviso con le delegazioni riunite il pensiero del Governo sulla nostra iniziativa e sul ruolo che agenzie e centri di cybersicurezza svolgono, ha dato atto al nostro Gruppo di essere uno stimolo e un sostegno al dialogo politico G7 sulla sicurezza e sulla resilienza cyber, con l'obiettivo di rafforzare la sicurezza nazionale e collettiva dei Paesi G7 e dell'Unione europea».