Sicurezza del Sistema Paese, il punto della situazione con il Presidente del CO.PA.SI.R

intervista all'on. Lorenzo Guerini, Presidente CO.PA.SI.R | a cura di Raffaello Juvara

Alcune ricerche segnalano l'aumento dei reati informatici a danno della PA, mentre diminuiscono quelli nei confronti del settore privato, invertendo il quadro degli anni precedenti. A cosa è dovuta questa situazione?

La Relazione annuale sulla politica dell'informazione per la sicurezza, presentata al Parlamento nelle settimane scorse, ci dice che complessivamente il rischio è in crescita. Nel 2018 gli attacchi ai danni della pubblica amministrazione sono aumentati del 561% rispetto all'anno precedente, mentre sono più che triplicati quelli contro aziende e soggetti privati. In entrambi i settori si è quindi assistito a un incremento significativo.

Non c'è dubbio che l'aumento così importante nei confronti della pubblica amministrazione sia un dato che ci dice come la dimensione stessa dello Stato possa essere un obiettivo. Questo anche perché all'interno di una competizione globale, chi ha intenzioni criminali individua nelle diverse amministrazioni target di particolare interesse. La progressiva digitalizzazione delle strutture pubbliche, inoltre, espone ulteriormente a rischi.

Detto questo, possiamo però affermare che il nostro Paese si è nel tempo dotato di una serie di strumenti normativi e organizzativi che hanno cominciato ad affrontare il problema. Già nel 2013 è stato istituito il Nucleo per la sicurezza cibernetica ed è stato prevista la elaborazione di un Piano Nazionale per la protezione cibernetica e la sicurezza informatica, adottato nel maggio del 2017. Inoltre è stata affidata al DIS la regia della nuova architettura contro il cyber crimine, anche in attuazione di quanto prevede la c.d. Direttiva NIS (Network and Information Security), direttiva europea recepita in Italia nel 2018, che definisce le misure necessarie a conseguire un elevato livello

di sicurezza delle reti e dei sistemi informativi, attraverso procedure di cui vengono resi responsabili gli OSE (Operatori di Servizi Essenziali), soggetti pubblici o privati che forniscono servizi essenziali per la società e l'economia nei settori: sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

Accanto a questo, è ovviamente insostituibile il ruolo e la funzione dei nostri servizi di intelligence che, nel tempo, hanno dimostrato non solo la loro crescente efficienza e capacità di analisi, ma anche la loro decisiva opera di supporto all'azione dei governi, attraverso la raccolta di informazioni, l'opera di prevenzione, la tempestività nell'avvisare sui più rilevanti fattori di rischio e la puntualità e completezza delle analisi di situazione da porre a disposizione del decisore politico.

Quindi, in breve, sicuramente i rischi e gli attacchi sono aumentati in modo considerevole, ma il Paese è attrezzato

per poterli fronteggiare con efficacia, naturalmente ben sapendo che occorre tenere alta la guardia e continuare a progredire in termini di prevenzione e risposta.

Quali sono le iniziative in corso in questa Legislatura per elevare il livello di consapevolezza dei rischi informatici nelle diverse categorie del Paese?

Mi permetto inizialmente di citare il fatto che il Copasir sta svolgendo una indagine conoscitiva sui temi della cyber security, anche con riferimento alle reti 5G che, attraverso audizioni di soggetti competenti, sta consentendo di acquisire informazioni e di aumentare la conoscenza del tema, delle sue enormi potenzialità e anche dei suoi rischi. I risultati saranno poi consegnati al Parlamento in una relazione che non si limiterà all'analisi ma, speriamo, possa indicare proposte politiche e legislative. Penso di poter dire che anche questo lavoro istituzionale può essere utile per diffondere quella cultura della sicurezza che è opportuno coinvolga i cittadini. Vi è poi un dato che ritengo positivo, che riguarda il moltiplicarsi di occasioni di approfondimento dei temi che riguardano la sicurezza, non solo informatica, e che vedono protagonisti istituti universitari ed enti di formazione. Una sicurezza partecipata può essere un valore aggiunto che permetta a tutti una maggior consapevolezza anche dei rischi.

Le cronache degli ultimi tempi, d'altra parte, segnalano come i rischi anche per la privacy dei cittadini siano in aumento. Per questo appare anche fondamentale sviluppare una crescita e diffusione della cultura della sicurezza cyber, che riguardi e coinvolga i singoli cittadini, in quanto fruitori della tecnologia informatica e potenziali vittime di questo tipo di minaccia e, soprattutto, chi opera nei settori produttivi e industriali, non solo ad alto rischio.

Viene sollevato da più parti il problema della sicurezza delle persone, degli asset e delle informazioni delle imprese italiane che operano all'estero in teatri complessi, attualmente costrette ad avvalersi di organizzazioni straniere per la mancanza di una regolamentazione delle PMSC italiane. Ritiene possibile il superamento del problema in tempi brevi?

Quella della sicurezza delle imprese che operano in territori a rischio è una questione complicata alla quale dare la giusta attenzione. Una preoccupazione e un'esigenza comprensibili di chi opera economicamente all'estero.

L'opportunità di una regolamentazione complessiva va presa in considerazione. Senza dimenticare mai, naturalmente, l'azione fondamentale che svolgono i servizi di informazione esterna in quei territori a tutela della sicurezza delle persone e degli interessi nazionali.

Come valuta le richieste di elevare a sistema i responsabili della sicurezza delle aziende pubbliche e private che operano in settori sensibili, formalizzando il loro ruolo nel quadro complessivo della sicurezza partecipata?

Io penso che sia essenziale una circolazione di informazioni e uno spirito di collaborazione stretta tra i livelli di sicurezza istituzionale, i nostri servizi e le imprese che maggiormente sono esposte a rischi in quanto operanti in settori più sensibili. Questo già avviene ma, a un aumento del rischio, può e deve corrispondere una ancora più efficace cooperazione. In questo senso occorre diffondere dentro le aziende la consapevolezza della necessità di attrezzarsi su queste materie. Una strategia che la nostra intelligence sta già sviluppando. Più persone, anche con livelli di responsabilità, si specializzano su questi temi maggiore sarà la sicurezza per tutti.