La tutela della cybersicurezza e la difficile collaborazione tra pubblico e privato

di Luigi Previti - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 12 luglio 2023

La tutela della cybersicurezza costituisce una delle sfide più importanti dell'odierna Società digitale. Negli ultimi anni l'Italia si è dotata di un'articolata architettura istituzionale, volta a contrastare ed attenuare l'impatto delle sempre più frequenti minacce informatiche sulle reti, sui sistemi e sui servizi ICT di maggiore rilevanza. Tuttavia, per garantire un adeguato livello di resilienza cibernetica nel nostro ordinamento, è necessario incentivare e mantenere una duratura collaborazione tra istituzioni pubbliche competenti e operatori economici del settore, quali co-protagonisti e co-responsabili del complesso sistema di prevenzione e di gestione del rischio informatico.

L'instaurazione di un sincero e costruttivo rapporto tra pubblico e privato nel settore della cybersicurezza non costituisce affatto un obiettivo di agevole realizzazione.

Le principali ragioni che giustificano una situazione di reciproca diffidenza tra i diversi portatori di interesse sono ormai note. Se, da una parte, le autorità amministrative mani-fastano una certa riluttanza nel condividere all'esterno notizie riguardanti la propria sicu-rezza, dall'altra gli operatori economici del settore, ricevendo solo occasionalmente ade-guati incentivi per la collaborazione prestata, preferiscono non confidare informazioni, di natura riservata o personale, che li esporrebbero al rischio di subire azioni legali o di ledere la propria reputazione sul mercato. Tale circostanza è stata confermata anche dal report tematico dell'agosto 2018 del Gruppo di coordinamento sulla sicurezza cibernetica (GCSC) della Banca d'Italia e dell'Ivass, nel quale si sottolinea che, nonostante il valore strategico della condivisione delle informa-zioni relative alle minacce cyber, le imprese che hanno subito attacchi sono disposte a condividere i propri dati soltanto in contesti che garantiscono riservatezza e reciprocità.

Nel tentativo di superare tali criticità, negli ultimi anni le istituzioni dell'Unione hanno promosso, tramite istituti e modalità differenti, un più effettivo coinvolgimento delle im-prese che offrono prodotti e servizi tecnologici nell'ambito dei sistemi di sicurezza ciber-netica elaborati dai singoli Stati membri, come si evince dalla comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, La strategia dell'UE in materia di cybersicurezza per il decennio digitale (JOIN (2020) 18 final).

La strategia sovranazionale interviene, in primo luogo, per fissare due fondamentali principi, che si rivolgono agli operatori del settore in quanto co-protagonisti della qualità del livello di protezione assicurato alle infrastrutture e ai software del mercato unico.

In tal senso, i produttori e i fornitori delle ICT vengono obbligati, da un lato, a mettere in commercio esclusivamente beni e servizi che possiedono, fin dal momento della proget-tazione, determinati requisiti di sicurezza contro il rischio di incidenti e di attacchi ciber-netici (principio di sicurezza by design); dall'altro, gli stessi soggetti sono chiamati ad assumere, nei confronti degli utenti, un ruolo di interlocutori privilegiati durante l'intero ciclo di vita dei prodotti, collaborando con il settore pubblico nell'esercizio dell'attività di vigilanza (principio di responsabilità tecnologica).

Da qui la previsione di una serie di peculiari adempimenti, che si esplicano, tra gli altri: i) nell'effettuare verifiche periodiche di funzionamento dei dispositivi; ii) nel curare gli aggiornamenti e le revisioni necessari; iii) nell'eliminare con celerità le vulnerabilità in-formatiche segnalate dagli utenti; iv) nel garantire un corretto utilizzo dei dati personali trattati.

Se ne ricava l'introduzione di precisi oneri di diligenza rafforzata, tanto più stringenti quanto più elevati sono i rischi di manomissione delle applicazioni e dei sistemi tecnolo-gici offerti sul mercato.
L'obiettivo di costruire un'efficiente architettura multilivello in materia di cybersicurezza si traduce, in secondo luogo, nella definizione di modalità più strutturate e durature di cooperazione tra settore pubblico e settore privato, in grado di sfruttare adeguatamente le conoscenze e le capacità di analisi di quest'ultimo.
È sotto questa prospettiva che può essere compresa l'istituzione di alcune sedi privilegiate di raccordo di matrice europea, tra le quali: il Centro europeo di competenza indu-striale, tecnologica e di ricerca sulla cybersicurezza, che intende sviluppare le risorse e le competenze dell'Unione e ridurre la sua dipendenza da Paesi terzi, impegnando le energie dei Centri nazionali di coordinamento, del mondo dell'industria e delle università (sul punto, cfr. il regolamento UE 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021); l'Unità congiunta per il cyberspazio (Joint Cyber Unit), quale piat-taforma finalizzata a promuovere lo scambio di informazioni, buone pratiche e cono-scenze, nonché la cooperazione tra forze dell'ordine e della difesa, autorità civili e diplo-matiche e soggetti privati in caso di gravi attacchi o incidenti di natura transfrontaliera; la rete dei Centri operativi di sicurezza (Security Operations Center, SOC), quale network
finalizzato ad assicurare un monitoraggio costante, diffuso e in tempo reale delle intru-sioni e delle anomalie informatiche nelle reti e nei sistemi dei diversi stakeholders, anche attraverso il coinvolgimento delle PMI dell'Unione. Grazie a questa rete, in particolare, vengono potenziate le capacità di rilevamento, di analisi e di condivisione dei dati relativi agli attacchi cyber più pericolosi, consentendo ad autorità pubbliche e privati di segnalare tempestivamente minacce potenziali e in corso, prima che queste abbiano causato danni irreparabili su larga scala.
L'introduzione di questi organismi dimostra la maturata consapevolezza, da parte delle istituzioni europee, della necessità di predisporre una governance più partecipata per af-frontare al meglio le impegnative sfide per la sicurezza poste dalla diffusione del cyber-spazio.
E ciò in considerazione dei rilevanti benefici ricavabili dal contributo del mondo imprenditoriale, quantomeno, sotto una duplice prospettiva.
In primo luogo, un'interlocuzione costante tra attori pubblici e operatori privati in materia di cybersicurezza favorirebbe un proficuo scambio di conoscenze specialistiche e di so-luzioni operative.
Nel contesto in esame, infatti, la creazione di un sistema fortemente centralizzato e uni-laterale, in presenza di evidenti asimmetrie informative, è destinata a non essere efficace: da un lato, la capillarità delle minacce cyber e la complessità della tecnologia in commer-cio rendono le imprese del settore i soggetti più qualificati a comprendere le tattiche d'at-tacco degli hackers, a individuare le principali vulnerabilità nascoste nei software ed a suggerire alle autorità competenti le contromisure più opportune; dall'altro, la realizza-zione di un circuito di sorveglianza e di allerta distribuito (c.d. distributed surveillance), che si basa (anche) sulla continua attività di vigilanza svolta dagli operatori economici, può ridurre notevolmente le inefficienze e i costi amministrativi sopportati dagli Stati membri per la tutela della sicurezza cibernetica.
In secondo luogo, il coinvolgimento del settore imprenditoriale si rivelerebbe particolar-mente importante in sede di elaborazione e di aggiornamento dei protocolli, delle linee guida e degli standard di sicurezza comuni, specie nell'ambito della protezione delle infrastrutture e dei servizi considerati "critici", gestiti nella maggior parte dei casi da sog-getti privati.
In particolare, l'intervento di questi ultimi nel processo di determinazione delle politiche e delle misure vincolanti per tutti gli stakeholders offrirebbe certamente alle autorità com-petenti un valido supporto tecnico; tale forma di collaborazione consentirebbe, inoltre, di evitare il rischio di perseguire ambiziosi obiettivi di resilienza attraverso l'introduzione di oneri e requisiti

inidonei o eccessivi, non compatibili con il principio di proporzionalità e con la prospettiva liberale da preservare in materia. Come appare evidente, infatti, aziende ed enti differenti affrontano minacce, vulnerabilità e conseguenze diverse; per-tanto, un'effettiva inclusione di tali soggetti nelle sedi decisionali e consultive non po-trebbe che favorire la definizione di strumenti parametrati al concreto livello di rischio informatico, adeguati ai particolari contesti in cui operano le imprese e aggiornati rispetto alle innovazioni tecnologiche sopravvenute.
In altri termini, la promozione di forme più stabili e articolate di cooperazione tra attori pubblici e privati consentirebbe non solo una maggiore condivisione di informazioni, abi-lità e buone pratiche, ma anche un'auspicabile partecipazione "dal basso" al processo regolatorio, limitando il tradizionale approccio "command and control" per favorire forme di "enforced self-regulation".
Tali considerazioni inducono inevitabilmente a riflettere sul sistema italiano di tutela della sicurezza cibernetica, all'interno del quale il tentativo di riprodurre moduli orga-nizzativi e operativi propri del comparto intelligence (sulla falsariga del modello istitu-zionale di cui alla l. 3 agosto 2007, n. 124) ha determinato un chiaro deficit di partecipa-zione degli operatori economici del settore.
Una scelta legislativa che, a ben vedere, suscita numerose perplessità, anche in conside-razione della nota dipendenza delle pubbliche amministrazioni italiane dalle capacità e dalle esperienze in ambito tecnologico-informatico possedute dal settore privato. Dipen-denza che ha rappresentato, e rappresenta ancora, una delle principali cause dei ritardi registrati dal nostro Paese nel complessivo processo di transizione digitale (il tema è stato più volte analizzato nell'ambito di questo Osservatorio: in particolare, qui, qui e qui).
Ancora limitati e generici appaiono i riferimenti normativi che prendono in considera-zione il valore strategico della dinamica collaborativa tra settore pubblico e settore indu-striale.
Ci si riferisce, ad esempio, all'art. 7 del 14 giugno 2021, n. 82, conv. con mod. dalla l. 4 agosto 2021, n. 109, che affida all'Agenzia per la cybersicurezza nazionale (ACN) il compito di: «rendere effettive» le capacità nazionali di prevenzione, monitoraggio, rile-vamento, analisi e risposta agli attacchi informatici, anche attraverso il ricorso a iniziative di partenariato pubblico-privato (comma 1, lett. n); di supportare, mediante il coinvolgi-mento delle università e del sistema produttivo, lo sviluppo di competenze e capacità in-dustriali, tecnologiche e scientifiche (comma 1, lett. r), anche in qualità di Centro nazio-nale di coordinamento ai sensi del citato regolamento UE 2021/887; di costituire parte-nariati, consorzi, fondazioni o società, con soggetti pubblici e privati, per la migliore rea-lizzazione delle sue finalità istituzionali (comma 1, lett. z).
Pertanto, a differenza di quanto è avvenuto in altri Paesi, in Italia la collaborazione con i privati è stata, finora, di natura prevalentemente finanziaria e rivolta allo sviluppo di tec-nologie e infrastrutture digitali.
Il quadro normativo appena rappresentato conduce ad accogliere con particolare favore le interessanti proposte contenute nella Strategia nazionale sulla cybersicurezza 2022-2026 e nel relativo Piano di implementazione del maggio 2022 (segnalati qui e qui).
Per quanto più rileva in questa sede, occorre evidenziare che attraverso questi documenti l'Italia intende garantire, oltre ai necessari investimenti nella componente "Sviluppo", un più effettivo coinvolgimento del settore privato nel perseguimento degli obiettivi di "Pro-tezione", da un lato, e di "Risposta", dall'altro.
Nello specifico, con riferimento al primo obiettivo, la Strategia e il Piano di implementa-zione mirano a potenziare il sistema nazionale di "scrutinio tecnologico", che fa capo al Centro di Valutazione e Certificazione Nazionale (CVCN) istituito presso l'ACN e, negli ambiti di competenza, ai Centri di Valutazione (CV) presso i Ministeri dell'Interno e della Difesa (come è stato già segnalato qui).

Al riguardo viene prevista l'introduzione di una rete dei laboratori accreditati di prova (LAP), quali soggetti, di natura pubblica, privata o mista, chiamati a supportare le proce-dure di valutazione della qualità degli asset tecnologici e dell'affidabilità dei fornitori dei dispositivi digitali utilizzati dai soggetti inclusi nel Perimetro di Sicurezza Nazionale Ci-bernetica (PSNC), in conformità al DPCM n. 92/2022 e al d.lgs. 3 agosto 2022, n. 123. In tal modo, anche grazie all'utilizzo dei fondi dedicati in materia dal PNRR, le procedure di individuazione delle vulnerabilità presenti nei beni, sistemi e servizi ICT affidate dal CVCN potranno beneficiare dell'importante contributo, in termini di conoscenze specia-listiche e di buone pratiche, delle università, dei centri di ricerca e degli operatori del settore interessati ad aderire alla rete dei LAP.
Allo stesso tempo, i suddetti atti di indirizzo sottolineano la necessità di migliorare le capacità nazionali di identificazione e di risposta alle nuove insidie della dimensione ci-bernetica, prevedendo due diverse forme di collaborazione pubblico-privato.
La prima, di natura strutturale, riguarda l'istituzione di una rete di centri settoriali di analisi e di condivisione di informazioni (Information Sharing and Analysis Center, ISAC), chiamata a supportare gli uffici dell'ACN nel predisporre e nel diffondere buone pratiche, linee guida, avvisi di sicurezza e raccomandazioni all'interno del Paese.
La seconda, di natura occasionale, contempla il coinvolgimento diretto di aziende quali-ficate in materia di incident response nel supportare le attività istituzionali dello Com-puter Security Incident Response Team – Italia (CSIRT), analizzate in precedenza qui, nel caso in cui dovesse verificarsi «una moltitudine di incidenti cyber di natura siste-mica». Così facendo l'Italia mostra di voler implementare, accanto ad adeguate strategie di resilienza, efficaci tattiche di difesa attiva (active difense), con l'obiettivo di sviluppare, avvalendosi di una molteplicità di sorgenti di informazioni rilevanti e di attori responsa-bili, modalità tempestive di gestione delle crisi e di contrattacco.
Si auspica che tali novità siano ulteriormente implementate, in ragione dei rilevanti effetti dissuasivi e preventivi esercitati nei confronti delle operazioni di intrusione e di mano-missione poste in essere dai criminali informatici.
In definitiva, è chiaro che l'effettiva realizzazione di una solida e duratura cooperazione tra attori pubblici e privati richiederà dei costi non indifferenti; se, tuttavia, di fronte all'esponenziale aumento di attacchi a livello globale, la tutela della cybersicurezza passa anche attraverso la diffusione di meccanismi condivisi di responsabilità e di gestione del rischio, allora il non far niente avrebbe dei costi molto più alti.