Cybersecurity: lo scenario normativo tra Italia e Unione Europea

L’accelerazione sulle questioni di sicurezza informatica

La rivoluzione digitale, se da un lato ha migliorato la vita degli individui, dall’altro ha posto l’accento sulle questioni legate alla sicurezza e alla vulnerabilità dei sistemi informatici. È ormai noto che un attacco cibernetico potrebbe causare gli stessi danni di un attacco armato, e in caso si verificasse contro uno dei Paesi membri dell’Alleanza Atlantica potrebbe determinare misure di difesa collettiva in virtù dell’Art. 5 del Trattato di Washington.

Ad aumentare la consapevolezza di quanto sia importante dotarsi di sistemi di sicurezza adeguati alle sfide del momento ha contribuito anche la pandemia di Covid-19, a causa della quale si è reso necessario un massiccio ricorso allo smart working. Ciò ha dimostrato la scarsa sicurezza e affidabilità dei servizi informatici, soprattutto riguardo la fornitura e la gestione dei dati, come denunciava lo scorso giugno il Ministro per l’Innovazione tecnologica e la transizione digitale, Vittorio Colao.

La storia degli attacchi informatici più famosi ai danni di multinazionali, governi e privati cittadini dimostra che nell’era di Internet niente e nessuno può dirsi al sicuro. L’aumento degli attacchi informatici e l’accresciuta esposizione alle minacce cybernetiche, anche da parte di governi lontani dalle nostre democrazie, hanno contribuito a sottolineare l’importanza della cybersecurity e della cyberdefense, rendendole questioni cruciali nelle agenda di chiunque abbia bisogno di mantenere riservate informazioni, dati e strategie, che siano esse politiche, economiche o militari.

La sicurezza e la resilienza digitale sono un punto chiave anche per il PNRR. All’interno del Piano di Ripresa uno dei capitoli fondamentali è infatti destinato proprio alla transizione digitale della Pubblica Amministrazione, al quale sono riservati 620 milioni di Euro.

Secondo il Rapporto Clusit nel trienno 2018 – 2020 gli attacchi informatici sono aumentati del 20%, e nel solo 2020 “gli attacchi rilevati e andati a buon fine hanno avuto nel 56% dei casi un impatto “alto” e “critico”; il 44% è stato di gravità “media”. Questo significa che non si è registrato solo un aumento nella quantità, ma anche nella qualità dell’attacco.

Cybersicurezza : Italia a che punto siamo?

L’ultima novità in tema di sicurezza informatica in Italia è il Decreto Legge n° 82 del 14 giugno 2021 convertito nella Legge n. 109 del 4 agosto 2021 recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale». Quest’ultima norma modifica il DPCM n° 131 del 30 Luglio 2020, il primo dei quattro decreti con i quali si intendeva attuare il perimetro di sicurezza cibernetica modificato in parte dal Decreto Legge n°162 del 2019.

Con la nuova normativa di giugno 2021 si definisce l’architettura nazionale per la sicurezza informatica, che prevede, oltre all’Agenzia per la cybersicurezza, anche il Comitato interministeriale per la cybersicurezza, il quale assolve alle funzioni di consulenza, proposta e vigilanza nel settore, e il Nucleo per la cybersicurezza, che si occupa di prevenire e preparare la risposta in caso di eventuali crisi e di attivare le procedure d’allerta. Presso la nuova Agenzia saranno trasferiti anche la sezione italiana del Csirt (Computer security incident response team) e il Centro di valutazione e certificazione nazionale.

“L’alta direzione e la responsabilità generale delle politiche di cybersicurezza” dell’AgenziaCsirt spetta al Presidente del Consiglio dei Ministri, il quale nomina e revoca il direttore generale e il suo vice. Attualmente, a capo dell’Agenzia per la sicurezza informatica è stato nominato Roberto Baldoni, ex vicedirettore del Dipartimento per le informazioni e la sicurezza, professore ordinario di Sistemi Distribuiti presso il Dipartimento di Ingegneria informatica, automatica e gestionale della Facoltà di Ingegneria dell’informazione, informatica e statistica – Università La Sapienza.

Le principali funzioni del nuovo ente che avrà personalità giuridica di diritto pubblico e autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria sono: coordinare la sicurezza informatica nazionale, prevenire, rilevare e monitorare le cyber minacce mitigandone gli effetti, innalzare la sicurezza delle tecnologie ICT (Information and communications technology), supportare e promuovere progetti per l’innovazione, lo sviluppo e la crescita della sicurezza digitale, che possano stimolare il potenziamento e l’accrescimento di competenze industriali, tecnologiche e scientifiche. L’Agenzia sarà inoltre l’unico interlocutore nazionale, sia per i soggetti pubblici che privati, in tema di cybersecurity, avrà il compito di predisporre le strategie di sicurezza digitale a livello nazionale e, infine, sarà l’autorità nazionale di certificazioni per la cybersicurezza.

E la sicurezza digitale in Europa?

Il primo atto europeo che avrebbe dovuto garantire un comune livello di sicurezza informatica in tutti gli Stati Membri è la Direttiva Nis – Networok and Information Security – del 2016 sulla sicurezza delle reti e dell’informazione, la quale però si è rivelata poco efficace a causa della difficile attuazione da parte di ogni singolo Stato. La Direttiva è stata recepita dal Governo italiano con il D. Lgs n° 65 del 18 Maggio 2018, ma a livello europeo ha dimostrato un basso grado di resilienza informatica delle aziende che operano in UE, un’eccessiva frammentazione nella sua applicazione e di conseguenza una scarsa capacità di agire congiuntamente in caso di attacco cibernetico, condividendo conoscenze e informazioni. Alla luce di queste considerazioni si è resa necessaria la proposta di una nuova Direttiva Nis, la Nis –2 appunto, che abrogherà la Nis –1 e si allineerà meglio a quanto già previsto dal GDPR – Regolamento Generale sulla Protezione dei dati.

Contemporaneamente alla proposta di una Direttiva Nis –2, la Commissione Europea ha pubblicato una nuova strategia per la cybersicurezza che contiene norme innovative per rendere più resilienti i soggetti critici fisici e digitali.

Accanto alla Direttiva Nis –1 c'è poi il Cybersecutity Act del 2019 con il quale la Commissione Europea ha adottato un sistema di norme di certificazione per la sicurezza informatica europea e ha definito il quadro normativo entro il quale si muove l'ENISA – l'Agenzia dell'Unione Europea per la sicurezza informatica, nata già nel 2004.

Secondo gli obiettivi che l'Unione Europea si prepara a perseguire, muovendosi nella direzione di uno spazio comune che possa essere resiliente, verde e digitale, la sicurezza informatica dei cittadini, dei governi e delle aziende, riveste un ruolo fondamentale come sottolineato nel comunicato stampa del marzo di quest'anno, diramato a conclusione del Consiglio Europeo.

Un fronte comune contro le cyber minacce è dunque estremamente necessario data l'importanza che gli strumenti informatici e digitali rivestono nella vita dei cittadini, nell'organizzazione delle Pubbliche Amministrazioni e nell'azione di multinazionali e Governi.

Read More