L’accelerazione sulle questioni di sicurezza informatica

La rivoluzione digitale, se da un lato ha migliorato lavita degli individui, dall’altro ha posto l’accentosulle questioni legate alla sicurezza e alla vulnerabilità deisistemi informatici. È ormai noto che unattacco cibernetico potrebbe causare gli stessi danni di unattacco armato, e in caso si verificassecontro uno dei Paesi membri dell’Alleanza Atlantica potrebbedeterminare misure di difesa collettiva invirtùdell’Art. 5 del Trattato di Washington.

Ad aumentare la consapevolezza di quanto siaimportante dotarsi di sistemi di sicurezza adeguatialle sfide del momento ha contribuito anche lapandemia 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 lafornitura e la gestione dei dati, come denunciava loscorso giugno il Ministro per l’Innovazionetecnologica e la transizione digitale, Vittorio Colao.

La storia degli attacchi informatici più famosi aidanni 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 minaccecybernetiche, anche da parte di governi lontanidalle nostre democrazie, hanno contribuito a sottolinearel’importanza della cybersecurity e della cyberdefense, rendendole questioni cruciali nelleagenda di chiunque abbia bisogno di mantenere riservate informazioni, dati e strategie, che sianoesse politiche, economiche o militari.

La sicurezza e la resilienza digitale sono un puntochiave anche per il PNRR. All’interno del Piano di Ripresa uno dei capitoli fondamentali è infattidestinato proprio alla transizione digitale dellaPubblica Amministrazione, al quale sono riservati620 milioni di Euro.

Secondo il Rapporto Clusit nel triennio 2018 – 2020gli 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, ilprimo 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