PRIMO PIANO Il Sole 24 Ore lunedì 05 FEBBRAIO 2018

Verso il 25 maggio. Dai budget tagliati negli ultimi anni alle tecnologie obsolete

Pa e aziende pubbliche in ritardo e con pochi fondi

Se la situazione delle imprese, come documenta l'Osservatorio del Politecnico, registra un incremento degli investimenti nel campo della cybersicurezza, il mondo della pubblica amministrazione e dei suoi apparati informatici centrali e locali rischia di arrivare molto impreparato. Informazioni in banche dati e piattaforme strategiche per la sicurezza e gli interessi nazionali che si scontrano con budget scarsi. Una situazione da corto circuito. Anche per questo motivo la Pa potrebbe incontrare forti difficoltà nell'adeguarsi agli obblighi del Gdpr.

La conferma arriva da Carlo Mauceli, national digital officer di Microsoft Italia, il cui team interviene sia nel pubblico sia nel privato. «Dalla nostra esperienza nel rapporto con numerose aziende pubbliche la valutazione dell'iter è partita - spiega - ma ora occorre dare un'accelerazione forte verso la compliance. Fatta eccezione per i principali Ministeri e per qualche Regione, in moltissimi casi occorre ancora iniziare un valido processo di valutazione».

Se si può dare per conclamato un potenziale ritardo della Pa nel trattamento dei dati personali secondo il nuovo modello, la situazione non migliora quando si analizza il livello di sicurezza It di Comuni, aziende sanitarie e municipalizzate. «È piuttosto scarsa perché molte realtà utilizzano sistemi obsoleti e di conseguenza sono esposte a gravi rischi - avverte il top manager -. D'ora in poi sarà importante aumentare le competenze tecnologiche dei responsabili e dei team It in tema di sicurezza, perché spesso non sono in linea con i tempi. È così che purtroppo in Italia si incorre in molte negligenze relative alla messa in sicurezza delle infrastrutture digitali».

Per il prossimo esecutivo è un campanello d'allarme che continua a squillare. Il pensiero corre alla primavera 2016 quando la Farnesina e le sedi estere subirono un attacco che fu scoperto oltre quattro mesi dopo. Seguirono le rituali smentite sulle reali conseguenze dell'intrusione, ma del resto la spending review e i tagli ai budget destinati alle piattaforme Ict hanno le loro conseguenze. «Secondo la nostra esperienza, le misure minime di sicurezza varate dall'Agid ad oggi non sono nel complesso rispettate: molti enti della Pa lamentano la mancanza di investimenti e questo implica che ci sia un ritardo rispetto all'adeguamento alle misure, a volte considerate anche di difficile implementazione» segnala Mauceli.

Logica conseguenza sarebbe un piano straordinario governativo finalizzato al rinnovo delle piattaforme critiche, quanto meno le più obsolete, con la messa in sicurezza delle infrastrutture e secondo un'ottica di lungo periodo. «Nel caso si potrebbe varare una collaborazione pubblico-privato nell'ambito di un percorso di trasformazione digitale con un focus incentrato sulla sicurezza» suggerisce il national digital officer di Microsoft Italia.

Se per la Pa è difficile ipotizzare un budget che permetta di avere un livello minimo di difesa cyber, una via potrebbe essere il ricorso alle piattaforme e ai servizi cloud. Ma soprattutto una visione strategica di lungo termine che a quanto pare finora non si è vista. «Gli attacchi informatici che personalmente ho dovuto gestire sono figli di questa mancanza di lungimiranza - conclude Mauceli -. Basterebbe ricominciare ad investire nelle infrastrutture».