LA REPUBBLICA - AFFARI & FINANZA – 14 OTTOBRE 2024

Cyber sicurezza ecco le nuove regole

di Alessandro Longo

«Ma chi vuoi che mi attacchi? Sono piccolo, io; non ho niente di valore». Questa frase, detta da molte piccole aziende italiane, «era sbagliata già vent'anni fa», dice Claudio Telmon, dell'associazione sicurezza informatica del Clusit. Adesso, in un'era in cui i cyber criminali attaccano tutti, anzi soprattutto i più piccoli perché più vulnerabili, «pensarlo è follia pura. Parlano chiaro i numeri degli attacchi alle aziende italiane, sempre più terribili anno dopo anno, come si vede nel report 2024 del Clusit », aggiunge. Non c'è settore merceologico che sia esente dal problema; nel 2023 gli attacchi in Italia sono cresciuti del 64 per cento, cinque volte la media globale. I criminali hanno capito che siamo facili prede.

Le imprese hanno difficoltà a imparare la lezione. Così, dopo vent'anni di allarmi e tentativi di sensibilizzarle, adesso scattano le norme. Per guidarle – volenti o no – verso pratiche migliori di sicurezza. Dal 16 ottobre entra in vigore in Italia la direttiva Nis 2, alla luce del recente decreto di recepimento. L'idea dell'Europa, prima con la direttiva Nis e ora la sua versione bis, è che bisogna obbligare le aziende più importanti a misure di sicurezza preventive. Nell'interesse loro e, insieme, di tutti. Chi non si adegua rischia sanzioni fino a 10 milioni o al 2 per cento del fatturato.

Il principio di fondo è che nella cyber ci si salva o ci si perde tutti assieme. Se è colpita un'azienda che offre servizi di importanza critica per la sicurezza, l'economia o i cittadini, il danno è a cascata. Quei servizi – bancari o di trasporto, ad esempio – rischiano di essere interrotti. Dati preziosi vengono trafugati, come quelli personali dei cittadini detenuti dall'azienda in questione. Idem per segreti industriali o militari, importanti perl'economia o la sicurezza del Paese. Un'azienda piccola "bucata" dai criminali può inoltre diventare testa di ponte per attaccare un suo cliente, che magari è una azienda grossa e importante; e così via.

Ecco perché la Nis 2 amplia, rispetto alla Nis, il ventaglio delle aziende tenute a adottare "misure tecniche e organizzative" adeguate al rischio cyber. La norma si applica principalmente alle grandi aziende, ossia almeno 250 dipendenti e fatturato annuo superiore a 50 milioni di euro o asset a bilancio per più di 43 milioni di euro. Anche le aziende di dimensioni più piccole possono essere soggette, se operano in settori particolarmente critici: energia, trasporti, bancario e finanziario, sanità, acqua potabile e acque reflue, infrastrutture digitali, pubblica amministrazione, fornitura e distribuzione di alimenti, servizi postali e di corriere, gestione dei rifiuti, fornitori di servizi digitali, telecomunicazioni. L'Italia è stato il solo Paese ad aggiungere il settore della cultura all'elenco.

Chi è soggetto alla Nis 2 deve fare una valutazione dei rischi associati ai sistemi informativi, adottare misure per prevenire e mitigare gli impatti di questi rischi, e assicurare la capacità di rilevare e

rispondere agli eventi di sicurezza. E anche garantire la continuità operativa dei servizi essenziali in caso di incidenti, attraverso un aggiornamento regolare delle misure di sicurezza adottate.
In caso di incidenti significativi che impattano sulla continuità dei servizi essenziali, le aziende devono segnalare tempestivamente l'incidente agli organi competenti. La notifica iniziale essere inviata entro 24 ore dalla scoperta dell'incidente, con successivi aggiornamenti man mano che emergono nuovi dettagli. La direttiva impone anche obblighi di responsabilità, chiedendo alle aziende di integrare la gestione della sicurezza informatica nella governance aziendale. Ciò significa che i dirigenti devono essere direttamente responsabili per la sicurezza informatica, e i dipendenti devono ricevere un'adeguata formazione sui rischi e sulla sicurezza informatica.
Le aziende devono dimostrare la loro conformità ai requisiti della Nis 2, anche attraverso audit e verifiche condotte dagli organi competenti.
«Il timore è ovviamente legato ai costi dell'adeguamento, soprattutto per le imprese che prima non erano incluse nella Nis», dice Pierluigi Perri, professore di sicurezza informatica all'università degli Studi di Milano e collaboratore dello studio legale Chiomenti. «Tuttavia, la gradualità delle misure previste dal decreto nazionale dovrebbe essere pensata proprio per andare incontro alle esigenze delle imprese con dimensioni più ridotte", aggiunge. "Ora inoltre dovrà intervenire l'ente attuatore della Nis – ossia l'Agenzia per la cibersicurezza nazionale – per dare maggiore concretezza ai principi previsi nel decreto", continua Pierri.
Una stima della società di consulenza Pwc a Repubblica indica circa 200 mila costi iniziali di adeguamento per una tipica pmi italiana (200 dipendenti, 100 milioni di fatturato).