la Repubblica.it

Cybersecurity, dal lavoro agli investimenti: ultima chiamata per l'Italia

Attacchi informatici in aumento, richiesta insoddisfatta di specialisti e regolamento europeo sulla privacy hanno portato il tema della sicurezza nell'agenda di aziende e PA. Le sfide sono tante e non ammettono temporeggiamenti. La chiave di volta è nel cambio di approccio: da problema a opportunità

di ANDREA FROLLA'

03 Novembre 2017

Potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati. E incentivazione della cooperazione tra istituzioni ed imprese nazionali. Sono questi alcuni indirizzi operativi del **Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali** che ha visto la luce a inizio anno e che non costituisce un mero aggiornamento del precedente piano, ma si pone l'obiettivo di imprimere un immediato impulso all'ulteriore fase di sviluppo dell'architettura nazionale cyber. Si tratta sicuramente di un passo importante da parte delle istituzioni governative verso la creazione di un **sistema integrato pubblico e pubblico-privato di difesa** contro le minacce del cybercrime, che però da solo non potrà reggere tutto il peso delle sfide odierne. I numeri dimostrano infatti che senza uno scatto di imprese e delle PA non si potrà andare lontano.

Il primo semestre dell'anno, rileva l'ultimo report del **Clusit**, ha infatti registrato una crescita degli attacchi dell'8% rispetto allo stesso periodo del 2016, con un dominio del cybercrime vero e proprio cioè delle attività mirate all'estorsione di denaro. Segno di un sistema che **fatica a fronteggiare l'avanzata del crimine informatico**, a causa di fattori diversi ma collegati fra loro. «Non si può negare che oggi ci sia un maggiore investimento di risorse e competenze tanto nel privato quanto nel pubblico. Dai numeri emerge un'insicurezza diffusissima su cui pesa l'evoluzione dell'informatica in cloud, del **mobile** e dell'Internet of Things che preoccupa, così come preoccupa l'aumento del numero di attacchi, dei soggetti bersagliati e delle offensive nei confronti delle infrastrutture critiche - spiega **Gabriele Faggioli**, ceo di Partners4Innovation, la società del Gruppo Digital360 che offre servizi di Advisory e Coaching per l'innovazione Digitale e imprenditoriale, oltre che **presidente del Clusit**, l'Associazione italiana per la sicurezza informatica - Su questo trend pesano i numeri sconfortanti della spesa in sicurezza informatica, che **non arriva al 2% della spesa Ict complessiva**. Così è **difficile creare un clima di fiducia**. Quanti salirebbero su una macchina sapendo che la casa automobilistica ha speso solo meno del 2% del budget per metterla in sicurezza? C'è un ritardo culturale accumulato nel corso degli anni. Ci si sta svegliando, **ma ad un ritmo ancora troppo lento**».

E chi deve necessariamente accelerare il risveglio dal letargo è il settore pubblico, storicamente indietro sul fronte digitale e per questo oggi esposto a rischi notevoli. «Il settore pubblico sembrerebbe scontare, in alcuni ambiti, una maggior arretratezza che si traduce comunque in situazioni diverse a seconda delle specifiche declinazioni. Fortunatamente **un aumento della sensibilità c'è stato, bisogna ora vedere se a questo incremento faranno seguito degli investimenti adeguati**. Tutte le iniziative di politica nazionale che mirano a favorire uno sviluppo di sinergie nazionali, internazionali e pubblico-private – sottolinea Faggioli - sicuramente aiutano. L'organicità del piano e l'approccio strategico sono da apprezzare perché **proseguono lungo una strada positiva di sistema** tracciata già da qualche anno». In questo contesto si inserisce il regolamento europeo in materia di privacy (**Gdpr**), che ha avuto il merito di portare il tema della sicurezza informatica all'attenzione del grande pubblico e delle imprese, spingendo quest'ultime ad attrezzarsi per evitare sanzioni estremamente rilevanti che potrebbero assumere, se applicate nei massimali, dimensioni disastrose per le aziende. «Il regolamento europeo sulla privacy **ha scosso le coscienze del mondo privato** – ricorda l'esperto di P4I - La prossima applicabilità e l'attenzione mediatica generata dai casi più eclatanti di cronaca hanno generato una **tempesta perfetta** che è necessario sfruttare. La leva normativa in particolare ha costretto le aziende a prestare un'attenzione elevatissima. Tutti ormai conoscono il tema e questo fa la differenza».

La cybersecurity si lega poi anche alla questione occupazionale. L'aumento degli attacchi e la loro gravità ha stimolato il mercato e in particolare una **domanda di esperti e professionisti che in Italia le aziende faticano non poco a trovare**. Anche se, sostiene Faggioli, il quadro sembra destinato a migliorare: «C'è una pressione occupazionale inedita in materia di cybersecurity. È sotto gli occhi di tutti il bisogno incredibile di competenze difficilissime da trovare nonostante le importanti prospettive remunerative e di carriera. Si tratta di un'occasione unica dalle grandissime potenzialità – avverte il presidente del Clusit - Le università si stanno attrezzano, fino a poco tempo fa gli esperti di sicurezza informatica arrivavano da studi più generalisti di informatica o da giovani appassionati. **La richiesta di professionisti sta diventando così evidente ed è lecito attendersi che il gap fra domanda e offerta si riduca nel tempo**. Un altro trend che merita attenzione riguarda la tendenza, anche e soprattutto normativa, a spingere le aziende, soprattutto Pmi professionisti e in parte Pa, all'esternalizzazione giustificata dal fatto che il costo sicurezza è così elevato che è bene affidarsi a chi fa cybersecurity di lavoro». Tutti questi temi saranno al

centro del **Cyber Security 360 Summit**, l’evento organizzato dal Gruppo Digital360 che andrà in scena il prossimo 14 novembre a Roma e che inquadrerà le sfide dei prossimi anni provando ad avanzare, grazie al confronto fra gli esperti, le migliori strategie per vincerle.