Cybersecurity, il rischio più grande è il personale inesperto

Data: Invalid Date | Autore: Redazione

I cybercriminali, certo. E poi la maggiore sofisticazione e pericolosità delle minacce, che trova breccia in sistemi per la sicurezza spesso e volentieri inadeguati e non aggiornati. La violazione di dati sensibili e infrastrutture critiche all'interno di un'azienda ha sempre una spiegazione e - il dato è sorprendente fino a un certo punto - per l'87% delle grandi organizzazioni è il personale inesperto il principale «cyber risk».

Il dato, particolarmente preoccupante se consideriamo che la formazione degli addetti è tra i fattori che progrediscono più lentamente in relazione agli attacchi informatici, emerge dal rapporto «The Cyber Security Imperative» elaborato da Esi ThoughtLab (la divisione di Econsult Solutions che si occupa di thought leadership) in collaborazione con Willis Towers Watson e altre aziende specializzate in sicurezza e gestione del rischio.

Le aziende definite come "leader", nello specifico, tendono a concentrarsi di più sui cosiddetti "hacktivist" (voce espressa nel 52% dei casi) e su minacce interne dolose (40%), mentre il 42% delle "principianti" è maggiormente preoccupato da azioni dolose esterne (al 42%) riconducibili a partner e fornitori.

I manager che appartengono alla prima categoria investono di più in cyber-resilience (procedure da attuare a valle di incidenti informatici) rispetto a quelli della seconda. E ancora. Il 91% dei "leader" sostiene che gli investimenti effettuati finora siano adeguati a soddisfare i bisogni di sicurezza

dell’azienda mentre tale percentuale scende al 33% nel caso dei principianti. L’80% delle organizzazioni censite, in generale, destina almeno un piccolo budget per l'acquisto di un'assicurazione cyber, e la cifra stanziata è maggiore nelle aziende farmaceutiche (in media 16,4 milioni di dollari di capitale assicurato) e minore nelle manifatturiere (in media 8,6 milioni).

Tornando allo studio, Corrado Zana, responsabile Cyber Risk Solutions di Willis Towers Watson per l’Europa Continentale, ha ricordato come la maggior parte degli incidenti di cyber security derivi da comportamenti errati del personale e da errori umani. «All’interno delle aziende – ha precisato in una nota - i leader investono ingenti risorse nella protezione dei sistemi informatici e nella gestione del rischio contro le minacce esterne, ma la formazione del personale, così come la cultura aziendale, giocano un ruolo di primaria importanza, più di quanto molti pensino. Per questo motivo, oltre a mitigare le minacce attraverso la tecnologia e il trasferimento del rischio, devono adottare una strategia di valutazione continua del rischio cyber». Una valutazione che deve considerare persone, processi e tecnologia.

Fonte: Il Sole 24 Ore - Articolo di Gianni Rusconi