Il cybersecurity manager e il Ciso

La sicurezza informatica A causa della crescita continua degli attacchi informatici, molte aziende sono corse ai ripari e hanno iniziato a investire nella protezione delle infrastrutture digitali, delle reti informatiche e dei dati sensibili. Sottovalutare i cyber rischi e potrebbe causare gravi danni e comportare elevati costi da sostenere. Per questi motivi, sono sempre più richieste due figure professionali: il **cybersecurity manager** e il **Ciso** (*Chief Information Security Officer*).

I due ruoli Il cybersecurity manager ha un ruolo più operativo. Oltre a far **rispettare le policy di sicurezza** informatica aziendale, definisce la strategia e gli standard di sicurezza interni, contribuisce alla stesura delle **linee guida sulla sicurezza**, valuta rischi, minacce e possibili conseguenze di un attacco informatico; infine, stabilisce e gestisce il **piano di risposta agli incidenti**. Il Ciso ha invece compiti più manageriali, essendo la figura responsabile della gestione delle operazioni di sicurezza informatica e, in tale veste, verrà chiamato a scegliere come **investire il budget** che l'azienda gli mette a disposizione per migliorare la sicurezza informatica.

Il mercato del lavoro La **formazione** richiesta a un cybersecurity manager è di tipo tecnico, con laurea in **informatica** o ingegneria informatica e **nozioni giuridiche** relative alla protezione delle informazioni e alla criminalità informatica; Il Ciso deve avere una formazione altrettanto solida in **ambito IT** (teoria delle reti, programmazione, cybersecurity), a cui affiancare conoscenze e competenze in **campo manageriale, finanziario e amministrativo**. Nonostante l'importanza crescente di queste due figure in ambito aziendale, come emerge dall'ultimo report dell'Osservatorio cybersecurity e data protection del Politecnico di Milano: «Nel 53% delle imprese oggi è presente un Ciso. [Tuttavia], il 40% delle imprese non ha una figura che si occupi di sicurezza aziendale e le mansioni che dovrebbero essere svolte dal cybersecurity manager o dal Ciso vengono invece affidate ad altri membri del team IT».

In pratica

Luca P. è il cybersecurity manager della Sistemi Internazionali Spa, azienda leader nel settore della produzione di software per la nautica. Durante una normale giornata di lavoro, l'azienda subisce un **attacco informatico** e Luca si attiva immediatamente insieme al suo team per isolare i sistemi compromessi ed evitare la diffusione ad altri sistemi interni. Luca decide inoltre di riunire il suo team per **identificare la causa** e il **perimetro del danno**. Dall'analisi emerge che l'attacco è scaturito dall'imprudenza di un dipendente che ha ricevuto e aperto un'email con un allegato malevolo. Fortunatamente il pronto intervento ha impedito che venissero sottratti i dati di alcuni clienti presenti nel computer del dipendente.

Per sensibilizzare tutto il personale dell'azienda sull'importanza della sicurezza informatica, Luca organizza un corso nel quale vengono presentate le **tipologie di cyberattacchi** con le relative azioni da seguire. Tutto il personale viene periodicamente coinvolto in simulazioni di attacco a sorpresa e, in base alle reazioni individuali, sottoposto a nuovi **test sulla sicurezza**.