L'INTERVISTA

«Il mercato a caccia di esperti cacciatori di dati»

Fabio Zamparelli, in qualità di responsabile Security–Ict Incident Monitoring di **Telecom Italia**, ha un punto di vista privilegiato sulle competenze di cyber security necessarie per operare in ambienti complessi.

Zamparelli, che mestiere fa il security manager?

Il termine indica figure diverse e un range molto ampio di attività, svolte a vari livelli. Si va dai tecnici specializzati in sicurezza informatica a ruoli più elevati, fino ad arrivare ai Chief Information Security Officer. Sono tutti security manager: la differenza sta nel livello di responsabilità e maggiore "esperienza organizzativa".

Cioè?

Tutti i security manager partono da un indispensabile bagaglio tecnico, ma evolvono grazie all'esperienza maturata nei contesti organizzativi. Si inizia con ruoli più tecnici e gestionali, ma con il tempo si apprende come dialogare e negoziare con le diverse aree di un'impresa fino ad assumere ruoli di coordinamento di altre persone o di raccordo con i vertici aziendali.

Quali le leve più importanti per questo lavoro?

In primo luogo un bagaglio formativo importante di tipo tecnologico, poi una particolare forma mentis e altissima curiosità. Alla base del mestiere c'è il piacere di scoprire e di approfondire le novità.

Contano più le competenze sulle soluzioni di mercato o di "tecnica pura"?

Fino a 10 anni fa il security manager era un esperto di prodotti e soluzioni. Questo perché la sicurezza era concentrata molto sul perimetro. Oggi serve una conoscenza profonda delle tecniche, ma anche del

Fabio Zamparelli
responsabile Security-Ict Incident Monitoring di Telecom Italia

business e delle operations più tipiche dell'azienda per cui si lavora. In Telecom Italia, per esempio, i security expert non hanno soltanto competenze standard, ma anche legate al mercato di riferimento, per esempio in materia di sicurezza dei router di un backbone o di altre tecnologie di Tlc.

Le caratteristiche, invece, di un buon capo?

Un buon team leader in ambito security deve avere ottime doti di comunicazione interna, saper far lavorare le persone in gruppo, non come solisti, e "schermare" le proprie risorse da eccessivi carichi organizzativi, lasciando loro la libertà di esprimere il proprio potenziale.

Com'è il mercato del lavoro per i security manager?

Sono figure ricercate, soprattutto se hanno esperienza. L'Italia in questo ambito non vede crisi, ma la mobilità è prevalentemente interna al settore. Diverso è in Europa, dove il mercato è aperto e spesso la domanda supera l'offerta.

Le tendenze sulle specializzazioni?

Cresce la richiesta di esperti di computer forensics e sicurezza in ambito mobility. C'è poi una terza tendenza piuttosto interessante: la necessità crescente di figure specializzate nella business intelligence per la cyber security. Si tratta di esperti "cacciatori", che setacciano i dati cercando anomalie e interpretazioni che nessuna macchina sarà mai in grado di offrire. ■

Job-ict Osservatorio sulle competenze digitali

Sguardo al futuro

Internet delle cose nel CV del security manager

Anche cloud e computer forensics fra le «competenze» innovative richieste ai professionisti della sicurezza informatica, il cui ruolo viene ritenuto sempre più strategico dalle aziende

Dario Banfi

«La superficie di attacco complessivamente esposta dalla nostra civiltà digitale cresce più velocemente della nostra capacità di proteggerla»: si apre così il Rapporto Clusit 2015 sulla Sicurezza Ict in Italia. Non c'è molto spazio per le interpretazioni: i difensori non riescono ad essere abbastanza efficaci.

A fronte di crescenti investimenti in sicurezza informatica, il numero e la gravità degli attacchi continuano ad aumentare. Si stima perfino che due terzi degli incidenti non vengano nemmeno rilevati dalle vittime. In questo scenario, poco rassicurante, la figura del security manager assume un ruolo sempre più strategico. È uno specialista IT noto alle grandi aziende del settore hi-tech e nei Soc (Security Operation Center), ma ancora poco valorizzato nei contesti con minore cultura della prevenzione, piccole imprese e PA. "È un ruolo che viene spesso ricoperto degli IT manager - spiega **Claudio Telmon**, consigliere **Clusit** e consulente di sicurezza informatica - ma che in realtà svolge compiti molto specifici, non di generica amministrazione dei sistemi. Deve infatti garantire la sicurezza del business, le tecnologie impiegate, il rispetto delle norme, la definizione di regole per la protezione degli asset e il monitoraggio degli incidenti in fase di esercizio"

Sebbene il tema della sicurezza tocchi vari ambiti dei sistemi informativi, l'approccio richiede competenze specialistiche. "Molto spesso ci si rifà a prodotti e servizi di mercato, ma ciò che fa la differenza è la corretta mentalità: serve una visione complessiva, coinvolgimento delle funzioni aziendali, un certo modo di pensare da giurista, fortissima preparazione tecnica e la convinzione che l'intelligenza di contrasto deve essere, come le minacce stesse, evolutiva e aggiornata".

La formazione gioca la sua parte, ma soltanto il tempo e l'esperienza migliorano le competenze operative. Tra le certificazioni professionali consigliabili per svolgere al meglio il mestiere, considerate tra le migliori dagli stessi esperti di cyber security, ci sono Cism e Cissp, oppure le quelle più "istituzionali" come Iso 27001, Itil o Cisa per l'audit dei sistemi o quelle più vicine alla cultura hacker come Ceh-Certified Ethical Hacker.

Com'è il mercato del lavoro per queste figure? "Tutto sommato buono", racconta **Davide Del Vecchio**, IS Security Coordinator presso il Soc di **Fastweb**. "Offre retribuzioni in linea con altre

Piccole imprese e PA ancora indietro: il ruolo viene spesso ricoperto dall'IT manager ma non basta

figure del settore, ma patisce una generale scarsa cultura aziendale in tema di sicurezza. È difficile, infatti, trovare occupazione come Information Security Manager: il ruolo è spesso assegnato all'IT manager, ma è percepito comunque come una funzione necessaria. Lo spazio di crescita si trova nelle grandi imprese, soprattutto là dove si supera la cultura dello 'smanettone' per inquadrare la funzione in maniera corretta".

Sotto il profilo della carriera è difficile che un security manager arrivi a coprire una ruolo da dirigente in azienda, ma ha responsabilità crescenti e giocherà in futuro sicuramente un ruolo chiave. "Inizialmente viene inteso soprattutto come un tecnico, che deve saper fare un po' di tutto, dal penetration testing all'audit sul codice, dalla malware analysis al monitoraggio di rete, ma la sua naturale evoluzione è quella di superare l'approccio puramente tattico, per definire strategie più ampie di prevenzione. Questo sarà sempre più richiesto in futuro nelle aziende di ogni dimensione". Le nicchie specialistiche che registrano già oggi un'impennata nella domanda di security manager sono quelle legate all'e-commerce, alla monetica e alla mobility. I fronti aperti che vedranno una crescita di richieste nei prossimi anni sono legati, invece, all'Internet of Things, ai servizi cloud e alla computer forensics.

Dal punto di vista del valore di mercato, secondo il più recente Osservatorio Competenze Digitali realizzato da **Agid**, Assintel e **Assinform** l'Ict Security Specialist ha registrato nel 2014 quotazioni retributive medie di 52.200 euro lordi all'anno se inquadrato con la qualifica di quadro e 32.600 euro lordi come impiegato. La Ral aumenta se si opera nella grande azienda (54.000 euro come quadro, 34.800 come impiegato); si ha un'età anagrafica sopra i 50 anni (56.800 euro come quadro, 40.200 come impiegato); sono stati raggiunti i cinque anni d'anzianità professionale (54.100 euro come quadro, 35.300 come impiegato). Non vi è distinzione di salario tra uomini e donne. Cambia, invece, lo scenario tra imprese Ict e non. Le seconde pagano i security manager, in media, 3.000 euro lordi in più all'anno. Al di là dei costi professionali, ogni security manager, è concorde comunque nel sostenere che il vero prezzo a cui prestare attenzione è quello da pagare in termini operativi, economici e di immagine in caso di scarsa prevenzione e sottovalutazione delle minacce reali. ■