Certificare il Security Manager

di Marco Misitano, CISSP, CISM

La sicurezza è fatta non solo di tecnologia. L'arte di preservare segretezza, disponibilità e integrità dei dati si avvale di molteplici aspetti, quello tecnologico è certamente uno molto importante, ma non per forza il più critico. Quello umano, e cioè di coloro i quali le tecnologie le scelgono, le implementano e le gestiscono, è tuttora trattato con relativamente poca importanza dal punto di vista della professionalità delle persone. La sempre costante difficoltà di avere garanzie di professionalità da parte dei responsabili della sicurezza dei sistemi informativi e dei responsabili dei sistemi informativi stessi si basa principalmente sull'esperienza delle persone e su una pletora di certificazioni di sicurezza che garantiscono, almeno in teoria, e con diversi livelli di attendibilità, la preparazione della persona a gestire, scegliere, implementare non solo tecnologie di security ma anche altri aspetti che concorrono alla sicurezza aziendale. Presa coscienza di quanto importante sia la mano del "guidatore" della tecnologia, si sta in questo momento assistendo ad un vero e proprio boom delle certificazioni di sicurezza. È vero, infatti, che anche le migliori tecnologie, se usate senza cognizione di causa, sono inefficaci, e che il miglior firewall, se configurato con scarsa accuratezza o senza profonda conoscenza rischia di essere efficace tanto quanto un cartello "attenti al cane" in una proprietà senza cani da guardia. Le prime realtà a muoversi sotto quest'aspetto sono stati i vendor di tecnologie che hanno rilasciato certificazioni riguardanti i propri prodotti. Sono nati quindi i Cisco Qualified Specialist (focalizzati su Firewall, IDS, VPN), la specializzazione Security dell'apprezzatissimo Cisco Certified Internetwork Expert (CCIE), i Checkpoint Security Administrator e Security Expert (CCSA, CCSE), le specializzazioni Security per le popolari Microsoft Certified Systems Engineer e Systems Administrator (MCSA, MCSE). Queste, assieme ad altre non menzionate, sono certificazioni rivolte a fornire alla persona le conoscenze necessarie alla migliore implementazione, configurazione e amministrazione *del prodotto*, o di una tecnologia circoscritta per forza di cose al singolo vendor. La Cisco CCIE Security ha una connotazione fortemente tecnica, ed è una delle poche certificazioni il cui esame presuppone anche una prova pratica. Garantisce approfondite conoscenze di networking da parte del certificato, sulle quali si appoggia una robusta e molto tecnica conoscenza delle problematiche di sicurezza delle reti e dei protocolli e meccanismi che ne regolano il funzionamento.Sempre Cisco, inoltre, ha affiancato un ulteriore livello di certificazione di sicurezza, il Cisco Certified Security Professional (CCSP), infatti, si pone ad un livello superiore ai già menzionati Qualified Specialist, e con competenze differenti rispetto al CCIE Security. Si tratta, infatti, di un professionista che conosce non solo molto bene le singole tecnologie, ma anche come implementarle, gestirle ed orchestrarle assieme in una rete, grazie ad un approccio modulare come suggerito dalla metodologia Cisco SAFE, che ha il pregio fra l'altro d'essere *vendor independent*, dando quindi al CCSP la capacità di considerare problematiche di Management, Monitoring, attacchi di vario genere, sicurezza applicativa e architetturale.

A essere pignoli, manca ancora qualcosa, e ci si riferisce esattamente al punto di partenza di quest'articolo. Se, con le certificazioni rilasciate dai vendor otteniamo professionisti profondi conoscitori di tecnologie e di diversi livelli di contorno a queste, esistono alcune certificazioni che prendono una diversa direzione. Una delle più note, è la Certified Information Systems Security Professional (CISSP) rilasciata da un ente indipendente come l'International Information Systems Security Certification Consortium (ISC²). Il

CISSP non è un profondo conoscitore di una tecnologia molto ristretta, piuttosto ha dimostrato conoscenze su una vasta serie di argomenti relativi ai molteplici aspetti della sicurezza (*"an inch deep and a mile wide"* si dice delle competenze del CISSP). Il percorso di studio per questa certificazione non parla di prodotto se non occasionalmente; di contro prende in considerazione la totalità degli aspetti relativi alla sicurezza. L'idea alla base della certificazione CISSP è di stabilire un fondamento di conoscenza comune (il *Common Body of Knowledge,* CBK) composto da dieci aree, o domini, per seguire la sua terminologia, che coprono:

- *Access Control Systems & Methodology*
- *Applications & Systems Development*
- *Business Continuity Planning*
- *Cryptography*
- *Law, Investigation & Ethics*
- *Operations Security*
- *Physical Security*
- *Security Architecture & Models*
- *Security Management Practices*
- *Telecommunications, Network & Internet Security*

Inoltre, a differenza di altre certificazioni, alla scadenza della validità del titolo, ISC² non prevede una ricertificazione con esame, ma piuttosto il mantenimento della credenziale attraverso attività inerenti la sicurezza informatica in una sua forma qualsiasi, compresa la diffusione della cultura della sicurezza stessa. A differenti attività sono associate differenti punteggi, e per mantenere la certificazione occorre, nell'arco di tre anni (quello della validità della certificazione) raggiungere un quorum di punti, pena la perdita del titolo. Come dire che il CISSP non solo dimostra superando l'esame di avere un'enciclopedica conoscenza sull'argomento sicurezza, ma, mantenendo la credenziale, anche di essere un *addetto ai lavori* (cosa peraltro già richiesta per sedersi a sostenere l'esame: quattro anni di esperienza professionale nel campo di uno qualsiasi dei dieci domini, e sottoscrizione di un codice etico). ISC², l'ente certificatore sostiene che CISSP è lo standard di riferimento per i professionisti della sicurezza informatica. Al di là delle interminabili discussioni che gravitano attorno a questa credenziale, probabilmente questa affermazione non si distacca molto dalla realtà. Un po' meno diffusa è la Certified Information Systems Auditor (CISA), rilasciata da un altro ente indipendente che è l'Information Systems Audit and Control Association (ISACA). A differenza della precedente, il CISA ha un bagaglio culturale mirato ai principi di auditing e specifico a sei domini di conoscenza legati all'auditing dei sistemi informativi. Pur con la consapevolezza di starne tralasciando diverse altre, fra le certificazioni indipendenti sono da non dimenticare anche Global Information Assurance Certification (GIAC) che, da un punto di vista indipendente dai vendor, certifica conoscenze tecniche in varie tecnologie specifiche (ad es. Firewalling, intrusion detection etc).

-

Se da un punto di vista di tecnologie per la sicurezza di rete la vastità della scelta è imbarazzante, per le certificazioni non è molto diverso. Inoltre l'efficacia della tecnologia messa in opera è strettamente legata alla competenza del professionista che la gestisce.

Esistono varie certificazioni che garantiscono diversi profili professionali e differenti competenze tecnologiche, e si è appena tracciato un profilo delle più importanti. Attenzione dunque alle certificazioni "improvvisate" e casalinghe, di scarso valore e contenuto, in genere create come veicolo di vendita di costosi corsi organizzati ad-hoc, e,

come sempre, con un pizzico di buon senso, è bene valutare obiettivamente i professionisti per la loro professionalità prima che per il tipo e numero di credenziali possedute.

Referenze:

https://isc2.org
International Information Systems Security Certification Consortium

http://cisco.com/go/ccsp
Cisco Systems Certified Security Professional

http://cisco.com/go/ccie/security
Cisco Certified Internetwork Expert Security

http://www.giac.org
Global Information Assurance Certification

http://www.certmag.com/articles/templates/cmag_feature.asp?articleid=170
Certification Magazine: Rating Certifications