QUALE FORMAZIONE (E CERTIFICAZIONE) PROFESSIONALE PER UN PROFESSIONISTA DELLA SICUREZZA DEL CLOUD COMPUTING?

Alberto Manfredi,
Presidente CSA

Spesso mi viene chiesto quali sono oggi, nel mercato della sicurezza informatica, i corsi e gli esami sia più completi dal punto di vista della base di conoscenza di riferimento (*knowledge base*) sia con più rilevanza e visibilità del brand o del cosiddetto "bollino" che è possibile acquisire e, soprattutto, esibire.
Una bella domanda, quasi una classica domanda da "un milione di dollari"! A parte la battuta, per poter rispondere correttamente dovremmo essere a conoscenza sia della cultura (diploma, laurea, ...) ed esperienze di base acquisite dal candidato sia degli obiettivi di carriera (tecnico, manageriali, ...) sia dagli interessi e gusti personali. Questi ultimi spesso possono essere determinanti per affrontare un percorso di studio, a volte complesso e dispendioso, che può richiedere sacrifici e compromessi su uno dei beni più preziosi che abbiamo ad oggi, il nostro *tempo* (peraltro già eroso da lavoro, famiglia, sport, ...).
Con questa premessa non voglio scoraggiare nessuno nell'intraprendere un giusto e doveroso percorso di certificazione professionale, ma come spesso l'esperienza e la vita insegnano, se si vogliono raggiungere buoni risultati con i giusti ritorni di investimento in denaro e tempo è necessario avere le idee chiare e soprattutto volontà di ferro.
La formazione professionale in ambito cyber security è oggi un mercato molto ricco di offerte formative[1]. Possiamo trovare, ad esempio:

- corsi offerti da istituti universitari (master, corsi di specializzazione),
- corsi offerti da ordini professionali e associazioni di categoria (in Italia),
- corsi offerti dai vendor di sicurezza, tipicamente volta a certificare le competenze nella configurazione di prodotto e quindi molto efficaci se si lavora o intende lavorare su determinati prodotti o sistemi,
- corsi offerti da associazioni professionali internazionali (CSA, SANS, ISC2, ISACA, EC Council, ...).

Ma se focalizzassimo la nostra ricerca ai corsi che forniscono una buona forma-

Alberto Manfredi è Presidente di CSA Italy dal 2011. Dottore in Scienze dell'Informazione e Dottore Magistrale in Informatica con pieni voti assoluti e lode, lavora da piu` di 20 anni nel settore ICT e Cyber Security. Attualmente lavora in Finmeccanica Spa come Business Development Manager nel Settore Elettronica e Sistemi di Difesa e Sicurezza. Detiene le certificazioni professionali CISA, CRISC, CISSP, GCFA, CCSK, Lead Auditor 27001, Certified CSA STAR Auditor. Cofondatore e Managing Director dell'associazione Club R2GS Europe nata per favorire lo scambio di esperienze e conoscenza nel campo Security Information and Event Management e Security Operation Centres.

CSA Italy è un'associazione no profit italiana nata nel 2011 come capitolo nazionale dell'associazione internazionale CSA (Cloud Security Alliance) a cui aderiscono le maggiori aziende del settore ICT ed Information Security che hanno scelto il Cloud Computing come parte rilevante del loro business. CSA coordina una community di professionisti che contribuiscono attivamente a sviluppare linee guida e buone pratiche per uno sviluppo ed utilizzo in sicurezza del Cloud.

zione cyber security anche o principalmente in ambito cloud computing le possibilità di scelta diminuirebbero drasticamente. Questo risultato è dovuto principalmente al fatto che si considera ancora il cloud computing come una particolare "architettura" e pertanto viene trattato nei corsi tradizionali (escludendo la formazione di prodotto offerta da vendor quali Vmware, RedHat, Oracle, ecc.) come uno dei possibili scenari con cui avrà a che fare un professionista della sicurezza informatica, sottovalutando quindi, dal mio punto di vista, la pervasività del paradigma cloud, dall'infrastruttura alle applicazioni, nelle modalità d'uso per l'utente, e della conseguente necessità di rivisitazione ed aggiornamento degli usuali paradigmi e soluzioni di sicurezza adottati.

Inoltre nel prossimo futuro il professionista di sicurezza si dovrà confrontare con clienti ed interlocutori che considereranno il cloud come una "prima scelta" (o il primo "problema") nell'utilizzo di infrastrutture e soluzioni ICT.

Sulla base del punto di osservazione ed esperienza dalla nostra associazione, per iniziare ad orientarsi possiamo identificare 3 tipologie di percorsi di formazione per un professionista nella sicurezza del cloud computing, ovvero:

1. percorso per Cloud Security Consultant
2. percorso per Cloud Security Architect
3. percorso per Cloud Security Auditor

Vediamo in seguito alcune brevi raccomandazioni su prerequisiti e corsi di formazione e certificazione attinenti a questi percorsi formativi suggeriti.

CLOUD SECURITY CONSULTANT

Questo percorso può essere di interesse per professionisti ICT con competenze di base in sicurezza informatica che intendono approfondire gli aspetti di sicurezza e governance del cloud computing. La nostra associazione, Cloud Security Alliance, è stata tra le prime a riconoscere e strutturare circa 6 anni fà questa nuova professionalità ed a proporre un percorso di certificazione professionale specifico e indipendente dai vendor sulla sicurezza cloud, il CCSK (Certificate of Cloud Security Knowledge)[2], oggi riconosciuta nelle prime 10 certificazioni professionali indipendenti sul Cloud Computing[3] e le prime 11 certificazioni su IaaS (Infrastructure as

1 CLUSIT (www.clusit.it) ha realizzato anche un apposito "Quaderno"
2 https://ccsk.cloudsecurityalliance.org/
3 http://www.cio.com/article/2369439/cloud-computing/129043-Top-10-Cloud-Computing-Certifications.html

a Service)[4]. Il CCSK, o corsi analoghi, possono essere un buon punto di partenza per costruire le fondamenta di una competenza professionale nella sicurezza del cloud che può essere consigliata sia a figure tecniche, e non solo in ambito IT (pensiamo ad esempio agli ambiti Legale o Acquisti) sia manageriali che dovranno occuparsi di cloud computing (ad esempio, Business Manager, CSO, CIO, ...)

CLOUD SECURITY ARCHITECT

Il percorso *Architect* può essere rivolto a professionisti che sono o saranno coinvolti prevalentemente nella progettazione e/o configurazione di infrastrutture e servizi cloud computing. In questo caso il professionista può scegliere di seguire un percorso di certificazione offerto da un vendor (ad es. RedHat, Vmware, IBM, ...) se dovrà progettare e configurare soluzioni cloud oppure, se ha già sufficienti o buone conoscenze sulle tecnologie, potrà rafforzare le sue competenze scegliendo un percorso di certificazione indipendente. Tra questi ultimi citiamo ad esempio il CCSP Certified Cloud Security Professional[5] di (ISC)2 e CSA, che è un percorso di certificazione in cui è necessario dimostrare sia una buona padronanza dei domini di conoscenza del CISSP[6], una delle certificazioni più impegnative e riconosciute in ambito Information Security, sia del CCSK (vedi sopra). Ci sono comunque percorsi analoghi proposti da ISACA (CRISC e CS-X), SANS (SEC524 Cloud Security Fundamentals), EC Council (CAST 618 Designing and Implementing Cloud Security), EXIN (Cloud Computing Foundation), per citarne alcuni.

CLOUD SECURITY AUDITOR

Il percorso Cloud Security Auditor può, in generale, essere consigliato a professionisti in attività di audit IT, con una buona co-

4 http://www.networkworld.com/article/3004365/public-cloud/11-top-iaas-cloud-computing-certifications.html
5 https://www.isc2.org/ccsp/default.aspx
6 https://www.isc2.org/cissp/default.aspx

noscenza della norma ISO 27001[7]. Sulla base del ruolo ricoperto, ovvero se auditor interno o auditor di terza parte può essere sufficiente una formazione analoga a quella del Cloud Security Consultant (ad es. su CCSK) oppure optare per un percorso di certificazione specifico. In quest'ultimo caso citiamo il percorso definito da CSA con la collaborazione di British Standard Institution (BSI) chiamato Certified STAR Auditor, rivolto a professionisti certificati Lead Auditor 27001, in cui vengono fornite le informazioni e gli strumenti di base per eseguire un audit di sicurezza di servizi ed infrastrutture cloud computing secondo lo schema di certificazione STAR[8] (Security Trust and Assurance Registry) di CSA.

CONCLUSIONI

Il tema della formazione professionale è piuttosto esteso e complesso. Non abbiamo ad esempio citato le attività in corso nell'ambito European e-Competence Framework[9] (e-CF), di schemi di formazione nazionali/regionali (ad es. il QRSP della Regione Lombardia[10]) oppure dell'interessante esperienza del Dipartimento di Difesa degli USA con la Direttiva 8570.1 ed altro ancora. Ho deciso quindi di dare semplici raccomandazioni supportate da esempi concreti sulla base delle domande sul tema che sono pervenute alla nostra associazione (e a me personalmente), ma anche su quanto si inizia ad intravedere come requisiti professionali nell'ambito di trattative pubbliche e private (ad es. bandi gara), sicuramente uno degli "stimoli" più interessanti per intraprendere un percorso di formazione e certificazione professionale sulla sicurezza del cloud.
Per la nostra associazione, a livello internazionale e nazionale, il tema della formazione professionale rimane uno dei cardini per assicurare un corretto sviluppo e uso in sicurezza di tutte le forme di computing. In particolare in Italia abbiamo deciso di attivare dallo scorso anno un'area di ricerca[11] dedita a strutturare della basi di conoscenza in ambito Cloud Security Governance, Cloud Privacy e Cloud Contratti sulla base delle esigenze formative rilevate nel mercato italiano e che vogliamo mettere a disposizione come complemento "cloud" ai corsi di formazione già presenti sul mercato. ■

7 http://www.iso.org/iso/iso27001
8 https://cloudsecurityalliance.org/star/certification/
9 http://www.ecompetences.eu/it/
10 http://www.ifl.servizirl.it/site
11 http://cloudsecurityalliance.it/ricerca/education/