Ecco le certificazioni professionali che qualificano i CISO

INDICE DEGLI ARGOMENTI

Questi professionisti hanno molti compiti, tra i quali stabilire politiche di sicurezza a livello aziendale, sviluppare piani di resilienza alla violazione dei dati, supervisionare le comunicazioni di aggiornamento del sistema e gestire i dati finanziari della sicurezza delle informazioni.
l crescente numero di organizzazioni che affrontano la transizione digitale richiede un correlato aumento di professionisti della sicurezza informatica capaci di proteggere questi sistemi. Il **Chief Information Security Officer (CISO) è un professionista IT e della sicurezza informatica la cui responsabilità è necessaria alle aziende** ad istruire opportune misure di sicurezza finalizzate a prevenire e proteggere le reti e i sistemi digitali dalle minacce informatiche.

Il CISO possiede spesso una laurea in informatica, diversi anni di esperienza nel campo della cyber security e una o più certificazioni professionali che richiedono una formazione professionale continua per essere mantenute. Vediamo quante e quali sono le attestazioni che certificano l'esperienza acquisita.

1 LA PROFESSIONALITÀ DEL CHIEF INFORMATION SECURITY OFFICER (CISO)

I CISO lavorano a fianco di decisori aziendali, manager, responsabili IT e team operativi di sicurezza informatica al fine di monitorare e mantenere in modo efficace la sicurezza delle applicazioni, dei database, dei computer e dei siti Web di una organizzazione.
Hanno inoltre il compito di stabilire politiche di sicurezza a livello aziendale, sviluppare piani di resilienza alla violazione dei dati, supervisionare le comunicazioni di aggiornamento del sistema e gestire i dati finanziari della sicurezza delle informazioni.
La professionalità di un CISO è legata anche alla capacità di comprendere le trasformazioni del core business aziendale e adeguare ad esso i controlli di sicurezza attuali e quelli necessari per una futura evoluzione.
Un CISO deve quindi preparare sé stesso e i dipendenti di una organizzazione con strumenti, competenze, processi, procedure per sviluppare capacità adeguate alla protezione dai rischi di sicurezza delle informazioni digitali.
L'efficacia ed efficienza delle azioni di un CISO risiede nella comprensione di come operano le altre discipline aziendali come finanza, risorse umane, acquisti, marketing etc, per adeguare le prassi di protezione all'operatività di ogni giorno senza ingessare l'azienda: quindi conoscere le operazioni e delle funzioni della propria organizzazione per prendere decisioni efficaci e proteggersi dai rischi di sicurezza informatica.

2

LA PREPARAZIONE FORMATIVA DI UN CISO

La formazione universitaria di un aspirante CISO dovrebbe partire da una laurea in sicurezza informatica o informatica (avendo cura in quest'ultimo caso di scegliere il maggior numero di esami legati alla sicurezza informatica).
Ma se si è in possesso di un diploma tecnico l'esperienza accumulata in anni di professione nella sicurezza può costituire un valido bagaglio.
Quello che conta in ognuno dei due percorsi è il raggiungimento di un metodo di lavoro appropriato e strutturato per la pianificazione strategica e il correlato piano tattico implementativo per avviare ogni iniziativa che rientra nei compiti e nelle responsabilità del CISO.
Nelle maggiori città italiane esistono università con indirizzi tecnici nella sicurezza che offrono lauree magistrali o triennali, master di I e II livello, dottorati di ricerca e le maggiori sono elencate alla pagina dedicata alla formazione del laboratorio nazionale per la Cyber security.
Oltre alla preparazione scolastica e quella universitaria è buona regola studiare per ottenere una o più certificazioni professionali che ampliano ulteriormente le conoscenze e permettono di essere considerato un candidato distintivo per future opportunità di lavoro.
Secondo il D.lgs. 13/2013 nato per definire regole di formazione non formale finalizzata all'aggiornamento continuo per tutte le professioni, non organizzate in albi e ruoli, la norma di certificazione per le professioni in ambito informatico a livello nazionale è la UNI 11506, successivamente arricchita dalle norme 11621 parte 1,2,3,4,5.

Proprio la UNI 11621-4 riguarda i profili professionali relative alla sicurezza delle informazioni ovvero definisce i requisiti relativi all'attività professionale soggetti operanti nell'ambito della sicurezza delle informazioni; A 10 anni dalla legge 4/2013 la stessa UNI ha pubblicato un bilancio dell'attuazione e della portata sul mercato valutando il numero di adesioni volontarie alle certificazioni UNI.
In tema di certificazioni per i CISO la Western Governor University (WGU) ne suggerisce diverse: Professionista certificato della sicurezza nel cloud (CCSP), Professionista certificato in sicurezza dei sistemi (SSCP), Specialista certificato in crittografia (Consiglio CE ECES), una o più certificazioni **COMPTIA** (A+, Certificazione di analista di sicurezza informatica CySA, Professionista della valutazione della vulnerabilità della rete, Professionista della sicurezza di rete, Professionista dell'analisi della sicurezza, Specialista delle operazioni IT, sicurezza, progetto, PenTest).
Altre certificazioni utili al day-by-day del CISO possono essere quelle offerte da **ISACA**: Responsabile certificato della sicurezza delle informazioni (CISM), Revisore dei sistemi informativi certificato (CISA), Certificato in Controllo dei Rischi e dei Sistemi Informativi (CRISC).
Ulteriormente utili possono essere la **International Information Systems Security Certification Consortium (ISC)2**, quella del professionista certificato di sicurezza offensiva (**OSCP**) e del Professionista certificato della sicurezza dei sistemi informativi (CISSP), la certificazione da Hacker etico (**CEH**) dell'EC-Council. Non da meno la **SANS.org** che ne indica due: la **GIAC Law of Data Security & Investigations** (GLEG) e la **GIAC Strategic Planning, Policy, and Leadership** (GSTRT).
Esistono infine certificazioni che riconoscono l'esperienza accumulata come la certificazione Associate C|CISO e **C|CISO dell'EC-Council**.

3

IL VALORE DELL'ESPERIENZA

Il programma formativo C|CISO riconosce l'esperienza nel mondo reale. Essenzialmente, C|CISO mira a colmare il divario tra la conoscenza del management esecutivo di cui hanno bisogno i CISO e le conoscenze tecniche di cui dispongono molti aspiranti CISO.
I partecipanti al corso analizzano una combinazione di argomenti fra 5 domini della sicurezza (governance e gestione del rischio, controlli sulla sicurezza delle informazioni, conformità e gestione degli audit, gestione e operazioni dei programmi di sicurezza, competenze chiave sulla sicurezza delle informazioni, pianificazione strategica, finanza, approvvigionamenti e gestione dei fornitori).
Se il richiedente si forma secondo lo schema dell'EC-Council non è prevista alcuna tassa di iscrizione e sono richiesti solo cinque anni di esperienza in tre dei cinque settori (ma attenzione l''esperienza richiesta deve essere acquisita mentre il candidato mantiene la certificazione di tipo Associate C|CISO che è quindi propedeutica).
Se invece il richiedente tenta l'esame senza frequentare la formazione autorizzata dall'EC-Council, sono richiesti cinque anni di esperienza ognuno dei cinque domini della security anche sovrapposti oltre ad una tassa di iscrizione (100 dollari).

4

SAPER COMUNICARE È DECISIVO

Al pari della preparazione tecnica (cosiddette hard skill) **è opportuno prepararsi anche nelle competenze soft ed in particolare quelle legate alla comunicazione efficace, alla guida dei team e anche alla presa di decisioni strategiche e leadership:** è quindi raccomandabile considerare anche la possibilità di una formazione manageriale.
Infine, la formazione continua dovrebbe essere un'abitudine periodica ricorrente per aggiornarsi sul panorama della minaccia, sulle prassi di protezione, sui rischi, sulla evoluzione tecnologica e correlata applicazione della sicurezza.
Nonostante l'alta operatività che contraddistingue ogni giornata tipo di un CISO ritagliare dello spazio per la formazione e per competenze e conoscenze aggiornate è cruciale. Per questo motivo il mantenimento della maggior parte delle certificazioni oltre al pagamento annuale richiede un numero prefissato di crediti formativi in un arco temporale limitato verificando i singoli certificati di frequenza.
Ai fini dell'aggiornamento professionale è fondamentale anche essere membro di associazioni di categoria dedite alla sicurezza come ad esempio l'**AIPSA**, o **ASSOCISO** e di organizzazioni di formazione competenti in materia di sicurezza delle informazioni come ad esempio il **CLUSIT** o l'**ISACA**.

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ