Seconda Edizione del Corso di Formazione per Digital Security Manager

SCHEDA TECNICA

Le finalità del corso

La Fondazione ICSA propone al mondo delle piccole e medie imprese (PMI), in particolare a quelle inserite nella supply chain delle holding e dei principali gruppi industriali Italiani, nonché ai singoli professionisti aziendali, la *Seconda edizione del Corso per Digital Security Manager*, che si pone l'obiettivo di trasferire ai partecipanti le conoscenze e le competenze professionali di base per gestire le problematiche di sicurezza informatica.

Al termine dell'iter formativo i frequentatori del corso saranno in grado di individuare e comprendere i rischi di sicurezza informatica per la propria organizzazione (anche in merito alle relazioni con il proprio committente principale) nonché di organizzare le procedure e gli strumenti più efficaci per la loro prevenzione, mitigazione e riduzione.

In sintesi, il corso fornirà ai partecipanti un kit di risposta rapida a fronte del verificarsi di un evento critico di sicurezza cibernetica, che consentirà loro, fin dall'insorgere dell'attacco informatico, di predisporre le prime misure operative in grado di assicurare la continuità aziendale.

Questo corso intende rispondere alle esigenze del mondo delle imprese che derivano non solo dai sempre più frequenti casi di crimini informatici, ma anche da recenti disposizioni legislative quali il D.lgs. 65/2018 contenente misure per innalzare la sicurezza della rete e dei sistemi informativi, e il Decreto-legge 105/2019 (convertito dalla Legge 133/2019), che istituisce il perimetro di sicurezza nazionale cibernetica, che riguarda reti, sistemi informativi e servizi informatici.

Il D.lgs. 65/2018 si rivolge agli operatori di servizi essenziali (energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali, motori di ricerca, servizi cloud e piattaforme di commercio elettronico), prevedendo a loro carico obblighi di adozione di misure tecnico-organizzative "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici.

Anche il D.L. 105/2019 prevede l'adozione di misure (indicate dai competenti Ministeri) obbligatorie per le grandi imprese dei settori strategici (difesa, tlc, reti), e le Pmi della filiera, finalizzate a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici. Tali misure riguardano la struttura organizzativa preposta alla gestione della sicurezza e sono relative alle politiche di sicurezza e alla gestione del rischio; alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza; alla protezione fisica e

logica e dei dati; all'integrità delle reti e dei sistemi informativi; alla gestione operativa, compresa la continuità del servizio; al monitoraggio, test e controllo; alla formazione e consapevolezza.
Questa nuova disciplina interessa quindi molte aziende, le quali, per continuare a svolgere la loro attività, ed in particolare per mantenere i rapporti di fornitura, devono garantire il rispetto delle disposizioni sopra ricordate in materia di sicurezza informatica, relativamente a reti, sistemi informativi e servizi informatici.

I destinatari del corso

I destinatari del corso sono i responsabili delle aree IT, dell'organizzazione aziendale, e del personale delle imprese operanti nei settori dei servizi essenziali (ex D.lgs. 65/2018) e strategici (ex D.L. 105/2019), o in loro assenza, i titolari delle imprese interessate questi provvedimenti, che hanno l'esigenza di acquisire una piena consapevolezza dei potenziali problemi di sicurezza informatica e delle modalità per farvi fronte, nonché la capacità di intervenire, selezionando e incaricando le società specializzate o i professionisti, in grado di organizzare il sistema di sicurezza informatica e risolvere le eventuali criticità.
Per la partecipazione al corso sono richieste le seguenti competenze:

- Navigazione su PC e Internet;
- Concetti di base su sistemi Microsoft Windows e GNU/Linux;
- Concetti di rete di base;
- Conoscenza dei concetti di programmazione di base.

Le materie del corso

- Introduzione alla sicurezza informatica delle Pmi (4 ore)
- L'analisi del rischio informatico nelle Pmi (4 ore)
- La valutazione dell'efficacia dei sistemi di protezione informatica (2 ore)
- Introduzione agli strumenti e alle tecnologie di sicurezza informatica (Blockchain, IOT, Big Data, AI e Deep Learning) (2 ore)
- Le sfide derivanti dalla sicurezza informatica per le Pmi: business continuity e disaster recovery (2 ore)
- Digital Forensics (4 ore)
- Il quadro normativo in materia di sicurezza informatica (4 ore)
- ISO/IEC 27001 in materia di requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (ISMS - Information Security Management System) (4 ore)
- Il Computer Emergency Response Team (CERT) (2 ore)
- L'open Source Intelligence (OSINT) (2 ore)
- Sicurezza Offensiva (2 ore)

- Sicurezza Difensiva I: (Asset Inventory, Asset Monitoring, Sicurezza Perimetrale, HIDS, NIDS, WAF) (2 ore)
- Sicurezza Difensiva II: il Security Operation Center (2 ore)
- Cyber landscape: lo scenario delle nuove minacce. Il mercato della sicurezza (2 ore)
- Evoluzione del 5G: Cybersecurity, sicurezza e integrità dei dati e proprietà delle reti (4 ore)
- Problematiche inerenti protezione e standardizzazione del segmento spaziale (2 ore)
- La cyber resilienza dei prodotti e del servizio (2 ore)
- L'assicurazione del rischio cibernetico (2 ore)
- L'Incident Management (2 ore)
- Le scelte organizzative in materia di sicurezza informatica (outsourcing vs insourcing) (2 ore)
- La gestione delle risorse umane ai fini della sicurezza informatica (2 ore)
- Ottimizzazione dell'organigramma ai fini della sicurezza informatica e gestione dei contratti con clienti e fornitori (2 ore)

La metodologia del corso

Il corso si basa su un modello formativo, messo a punto dalla Fondazione ICSA, che prevede:
1) il trasferimento delle conoscenze finalizzate a rappresentare lo stato dell'arte sui vari argomenti;
2) la presenza dei rappresentanti più qualificati delle Istituzioni e delle società operanti nel settore della cybersecurity;
3) l'approfondimento delle tematiche più importanti con l'illustrazione di case history presentati da professionisti operanti nel settore della cyber security.

I contenuti del corso, così come i curriculum dei docenti, sono verificati dal Comitato scientifico della Fondazione ICSA, attraverso la supervisione del Presidente e del Direttore della Fondazione ICSA.
Il percorso formativo consentirà ai partecipanti di leggere il contesto strategico generale della sicurezza informatica, analizzare l'evoluzione degli scenari nazionali e internazionali, individuare e valutare i rischi della propria organizzazione sul piano della sicurezza informativa, costruire strategie, piani, policy e procedure di prevenzione volti alla loro mitigazione o riduzione, individuare i soggetti che possono realizzare le misure di sicurezza informativa previste, e valutare il risultato del loro operato.

Il Corpo docente

Il percorso formativo combina *contenuti di eccellenza* nell'ambito della cybersicurezza ed un *corpo docenti* composto dai consiglieri scientifici e responsabili dell'Area cybersecurity della Fondazione ICSA, nonché da esperti di comprovata professionalità provenienti dalle istituzioni e dalle principali holding e gruppi industriali nazionali, tra i quali:

Gianfranco Ciccarella

Ingegnere, ha lavorato in diverse società del Gruppo Telecom Italia con responsabilità tecniche e manageriali. Attualmente è un consulente nel settore ICT (Information and Communication Technology). Nel Gruppo Telecom ha ricoperto i seguenti ruoli: membro di Consigli di Amministrazione, Amministratore Delegato e Presidente di Società del Gruppo Telecom, Corporate Chief Technical Officer per Telecom Argentina e TIM Brasil, Vice President Next Generation Access Networks (NGAN) and Partnerships in the Strategy Department of Telecom Italia, Chief Information and Technical Officer di Telecom Italia Sparkle e Direttore della Scuola Superiore Guglielmo Reiss Romoli. Ha anche svolto attività di ricerca e insegnamento presso la Facoltà di Ingegneria dell'Università di L'Aquila (Professore Associato) e Polytechnic University di New York (dove è stato Adjunct Associate Professor).

Gerardo Costabile

CEO di DeepCyber, specializzata in Advanced Cyber Threat Intelligence, Protection e Antifrode. È stato Chief Security Officer di British Telecom e Fastweb spa, Executive Director della practice "Forensic Techonology and Discovery Services" per l'Europa dell'Ovest, Chief Information Security Officer del Gruppo Poste Italiane ed investigatore nel Gruppo Repressione Frodi della Guardia di Finanza di Milano.

Luisa Franchina

Ingegnere, partner e senior analyst Hermes Bay e presidente dell'Associazione Italiana esperti in Infrastrutture Critiche. Consigliere scientifico della Fondazione ICSA, fa parte dello Stakeholders Cybersecurity Certification Group (SCCG) della Commissione Europea. Esperto di protezione delle infrastrutture critiche e di strategie di sicurezza delle reti e dell'informazione, già Direttore Generale del Nucleo Operativo per gli attentati NBCR (nucleari, biologici, chimici e radiologici) presso la PDCM, nonché Capo della Segreteria Tecnica del "Tavolo PIC", in seno alla PDCM, per il coordinamento interministeriale delle attività riguardanti le infrastrutture critiche.

Emanuele Gentili

Founder, SVP of Threat Intelligence TS-WAY, Co-Direttore dell'area Cybersecurity della Fondazione Icsa. Esperto di Sicurezza Offensiva e Cyber Threat Intelligence. In possesso di un significativo background tecnico, ha maturato una lunga esperienza nell'analisi dei livelli di sicurezza delle infrastrutture e delle applicazioni ed è Cyber Threat Intelligence advisor per diverse realtà pubbliche e private. Parte integrante del Nucleo di Analisi Nazionale nell'esercitazione di guerra cibernetica NATO Locked Shields, svolge attività di ricerca per la produzione di algoritmi predittivi e metodologie di detection finalizzate all'identificazione di minacce cibernetiche complesse. Ricercatore accreditato nel campo della sicurezza offensiva, è trainer accreditato per i corsi di certificazione Offensive Security Certified Professional

(OSCP). E' stato coordinatore europeo fino al 2013 del progetto "BackTrack Linux", il sistema operativo leader nel campo delle verifiche di sicurezza. È' Co-fondatore del progetto "The Exploit Database", che si occupa di trattare informazioni confidenziali circa vulnerabilità 0day (non ancora pubbliche). Ha ricevuto crediti per le sue attività di security advisory da Google, Microsoft, Apple, Facebook, Symantec ed altri crediti per aver segnalato in "responsible disclosure" (rivelazione responsabile) problemi di sicurezza imponenti in applicativi e servizi.

Le regole del corso

Il Corso, della durata di 56 ore, si terrà a online a partire dal 26 aprile 2023 e si concluderà nel mese di giugno 2023.

Esso è articolato in 14 giornate da 4 ore, dalle ore 14 alle ore 18, due volte a settimana. Queste si terranno con la modalità della didattica a distanza.

Per l'iscrizione al Corso è necessario compilare la Scheda Amministrativa in tutte le sue parti.

La quota individuale di partecipazione è di € 1.500,00 (millecinquecento/00) + IVA. Il pagamento dovrà essere effettuato, in un'unica soluzione, prima dell'inizio del Corso tramite bonifico bancario sul conto corrente.

L'attestazione delle competenze e delle conoscenze acquisite durante il Corso avverrà attraverso un esame finale a cura della Direzione del Corso, a seguito del quale, in caso di esito positivo, verrà rilasciato un **Attestato della Fondazione ICSA**.