Prima 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 *Prima 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.

I contenuti del corso

Il corso si articola in 4 moduli per complessive 56 ore, così articolate:

Modulo 1 - Introduzione alla sicurezza informatica delle Pmi

- Lo scenario attuale delle minacce informatiche verso le Pmi
- La "Cyber Kill Chain" e le tecniche e tattiche di attacco informatico
- Gli avversari cibernetici (statuali e sponsorizzati da stati, cybercriminali e hacktivisti)
- Le minacce di tipo "Ransomware"
- I tradizionali punti deboli delle reti e dei sistemi informatici delle Pmi;
- L'impatto dello smart working, dell'uso di smartphone, di reti wireless, e dei clouds sulla sicurezza informatica delle Pmi;
- L'analisi del rischio informatico nelle Pmi:
  a) Differenze tra risks e threats e vunerabilities;
  b) Modelli di valutazione del rischio (analisi quantitativa, analisi semi-quantitativa, analisi qualitativa);
  c) Identificazione delle minacce e categorie di minacce;
  d) Identificazione delle vulnerabilità e categorie di vulnerabilità;
  e) Tools di risks assessment;
- La valutazione dell'efficacia dei sistemi di protezione informatica;
- Introduzione agli strumenti e alle tecnologie di sicurezza informatica (Blockchain, IOT, Big Data, AI e DeepLearning);
- Le sfide derivanti dalla sicurezza informatica per le Pmi: business continuity e disaster recovery.

Modulo 2 - Il quadro normativo in materia di sicurezza informatica

- Il D.L. 105/2019, e i relativi decreti ministeriali, in materia di perimetro di sicurezza nazionale cibernetica;
- Il D.Lgs. 65/2018, attuativo della direttiva Ue 1148/2016 (cd. Direttiva Nis), recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Ue;
- Il D.Lgs. 196/2003, come modificato dal Reg Ue 2016/679 (GDPR), sui doveri delle

imprese in materia di tutela della privacy e il ruolo del Garante della Privacy;

- Il Piano nazionale per la protezione cibernetica e la sicurezza informatica del marzo 2017;
- ISO/IEC 27001 in materia di requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (ISMS - Information Security Management System);
- L'impatto della normativa sulle Pmi relativamente a:
  a) monitoraggio della sicurezza delle comunicazioni dei lavoratori (smartphone, computers, altri dispositivi mobili aziendali, reti);
  b) tutela dei dati dei lavoratori e dei terzi (clienti, fornitori).

Modulo 3 - Gli strumenti per la sicurezza informatica delle Pmi

- La Cybersecurity IT (Information Technology) e la Cybersecurity OT (Operation Technology) e il suo ruolo nel sistema di Security Management;
- Il quadro istituzionale della Cyber Security (l'Agenzia per la Cybersicurezza Nazionale e la Polizia Postale e delle Comunicazioni);
- I diversi sistemi di sicurezza informatica difensiva:
  a) Sicurezza Difensiva I: (Asset Inventory, Asset Monitoring, Sicurezza Perimetrale, HIDS, NIDS, WAF);
  b) Sicurezza Difensiva II: il Security Operation Center;
  c) Sicurezza Difensiva III: il Computer Emergency Response Team;
- I diversi sistemi di sicurezza informatica offensiva (Vulnerability Assessment, Penetration Test, Red Teaming);
- La crittografia;
- L'Incident Management:
  a) la classificazione degli incidenti;
  b) le fasi dell'Incident Management;
  c) le attività dell'Incident Management (rilevazione, investigazione, contrasto);
  d) i fattori chiave per la gestione degli incidenti;
  e) il piano di Incident Management;
- Il Disaster recovery
- La Cyber Threat Intelligence e l'information sharing;
- L'Open Source INTelligence (OSINT);

- Le certificazioni e gli standard di cybersecurity per le Pmi;
- L'assicurazione del rischio cibernetico;
- La Digital Forensics nel sistema giudiziario italiano;
- Testimonanze e case studies in materia di cyber security.

Modulo 4 - L'organizzazione aziendale ai fini della sicurezza informatica

- La governance del sistema informatico di una Pmi mediante i KPI (Key Performance Indicators) e i SLA (Service Level Agreements);
- Le scelte organizzative in materia di sicurezza informatica (outsourcing vs insourcing);
- La gestione delle risorse umane ai fini della sicurezza informatica;
- L'ottimizzazione dell'organigramma ai fini della sicurezza informatica;
- L'impostazione e gestione dei contratti con clienti e fornitori.

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.

Le regole del corso

Il Corso, della durata di 56 ore, si terrà a online a partire dal 27 aprile 2022 e si concluderà il 22 luglio 2022.

Esso è articolato in 14 giornate da 4 ore, che 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**.