Cyber security

Docenti: Barbara Indovina, Michele Slocovich

Lingua

Italiano

Descrizione del corso e obiettivi

Nell'era dell'interconnessione è sempre più difficile mettere al sicuro dati e informazioni. La trasformazione del modo di comunicare ha posto l'attenzione sulla necessità di proteggere adeguatamente i flussi di dati e i sistemi interconnessi. Al crescere della complessità delle architetture informatiche cresce da pari passo la complessità nel controllo manageriale sulle informazioni, sulle persone e sui mezzi predisposti per il loro trattamento. Le aziende sono esposte a gravi rischi spesso ignorati. Il corso vuole fornire agli studenti una panoramica sul contesto operativo della cyber security e sulla normativa Europea e Italiana relativa alla sicurezza dei dati e delle informazioni, fornendo gli strumenti necessari per comprendere il processo di governo della sicurezza e compliance aziendale alla normativa.

Gli obiettivi del corso sono di fornire agli studenti un approccio pratico e concreto al processo di governo e compliance all'IT security partendo dai concetti di sicurezza dei dati e delle informazioni attraverso una lettura completa e critica delle normative in tema di sicurezza dei dati e del loro trattamento.
Nell'ultima lezione del corso gli studenti parteciperanno all'analisi di un caso pratico di gestione di un incidente di sicurezza all'interno dell'azienda.

Alla fine del corso, i partecipanti saranno in grado di:

- Comprendere quali sono le principali minacce informatiche
- Comprendere come è possibile mitigare i rischi di un attacco informatico
- Comprendere le interdipendenze internazionali delle attività cyber
- Comprendere quali risorse aziendali sono necessarie nel processo di innalzamento del livello di sicurezza informatica
- Comprendere l'importanza della computer forensics per conservare le tracce di un incidente informatico (Forensics Readiness)

Destinatari

Il corso è aperto a tutti gli studenti Bocconi. In particolare si rivolge a tutti coloro che sono interessati a comprendere il contesto giuridico e tecnologico e l'approccio in materia di compliance aziendale, sia dal punto di vista normativo che da quello

tecnologico. Per la natura degli argomenti trattati, è particolarmente indicato per gli studenti del CLMG e dei Corsi di Laurea Magistrale, in particolare del CLELI.

Prerequisiti

Nessuno. Si consiglia tuttavia di aver superato un esame di informatica come Computer science o Informatica per giurisprudenza, o di possedere le competenze equivalenti.

Regolamento

Iscrizione:
Le iscrizioni ai corsi possono essere effettuate esclusivamente tramite l'agenda dello studente yoU@B, nel box "Adesione attività varie".
È possibile annullare la propria iscrizione esclusivamente tramite agenda **entro e NON oltre** il termine delle iscrizioni al corso stesso. Non sono consentite altre modalità di cancellazione.
L'iscrizione verrà confermata qualche giorno prima dell'inizio del corso attraverso un messaggio nell'agenda yoU@B.

Frequenza:

- Frequenza pari o superiore al 75% delle lezioni: ottenimento dell'Open Badge
- Frequenza inferiore al 25% delle ore di lezione: inserimento in blacklist

Modalità didattica

Sarà possibile partecipare al corso esclusivamente in maniera presenziale.

Durata

10 ore

Calendario

Lezione	Data	Ora	Aula
1	lun 08/04/2024	18.15 - 19.45	N32
2	mar 09/04/2024	18.15 - 19.45	N32
3	lun 15/04/2024	18.15 - 19.45	N32
4	mar 16/04/2024	18.15 - 19.45	N32
5	lun 22/04/2024	18.15 - 19.45	N32

Programma delle lezioni

Lezione	Argomenti
1	**La sicurezza informatica** - Definizioni (sicurezza dei dati e sicurezza delle informazioni) - Cyber security come gestione del rischio - I tipi di rischio: intrusion, furto di identità, interruzione di servizio - Le tecniche: phishing, intrusion, DDoS ecc. - I principali framework di riferimento per la Cyber security
2	**La sicurezza in azienda** - Compliance aziendale - La normativa europea (ENISA, Direttive NIS) - Information warfare (la guerra delle informazioni) - Il GDPR - Policy e procedure - La gestione dell'incident (data breach) - Esempi pratici: le CEO Fraud

3	**Il rischio cyber: difesa della superficie d'attacco**
	- Mitigazione del rischio: approccio e misura
	- Misure Tecniche:
	  o perimetrale, interna, preventiva, reattiva
	  o monitoraggio
	- Sistemi di rilevazione degli incidenti di sicurezza e importanza del monitoraggio: SIEM, IoA e IoC, sistemi antifrode, VA ecc.
	- Velocità di ripristino vs. necessità di investigazione
	- Incident responding: identificazione del perimetro di intervento
	- Anonimizzazione e tracciabilità

Lezione	Argomenti
4	**Attacchi e prevenzioni** - Misure Organizzative: o Il fattore umano: Training, consapevolezza o I ruoli aziendali coinvolti: DPO, CISO, CRO - Identificazione del problema, intervento, ripristino, notifica del breach - Unità di crisi multifunzionale - Acquisizione forense delle evidenze, ripristino dei sistemi - Digital Forensics: investigazione con valore probatorio delle risultanze - Riferimenti normativi - La Forensic Readiness
5	**Analisi di un caso pratico** - Partendo da casi di cyber attacchi realmente accaduti, verrà analizzata la gestione della cyber crisis sotto il profilo tecnico, legale ed organizzativo. - Attività di debriefing del caso e analisi delle possibili soluzioni

Bibliografia suggerita

Materiali prodotti dai docenti

Posti disponibili

Questa attività è a numero chiuso quindi l'iscrizione non sarà possibile oltre **110 posti** o dopo la chiusura del periodo di iscrizione.
E' possibile annullare l'iscrizione esclusivamente tramite agenda yoU@B entro e NON oltre il termine delle iscrizioni al corso stesso.