Master Specialistico

MASTER in CYBERSECURITY MANAGEMENT

Sicurezza informatica, Sicurezza delle informazioni, Governance e visione strategica della cybersecurity, processi di conformità, analisi dei rischi e delle minacce, business continuity, perimetro nazionale di sicurezza cibernetica

On Demand

ON DEMAND - Programma Dettagliato delle Lezioni

CYBERSECURITY & COMPLIANCE SECURITY MANAGEMENT

Sicurezza informatica, Sicurezza delle informazioni, Governance e visione strategica della cybersecurity, processi di conformità, analisi dei rischi e delle minacce, business continuity, perimetro nazionale di sicurezza cibernetica

Lezione 1

Fondamenti di Cybersecurity: Information Security Governance

- Missione dell'information security: Triade CIA
- Information Security Governance
  - Ruoli, Responsabilità metriche di Governance
  - Information Security Strategy
- Overview – Information Risk e Compliance
  - Determinare lo stato di maturità dell'Information security
  - Sviluppo di una strategia
- Sviluppo di un programma di information security
  - Obiettivi di programma e scelta di un framework
  - Definizione di una roadmap e implementazione
- Gestione di incidenti di information security
  - Risorse, obiettivi e indicatori
  - Business Continuity e Disaster Recovery
- Esercitazione:
  - Verifica di un programma di Information Security

Lezione 2

Cybersecurity Risk Assessment: Nozioni tecniche di base e Open-sources threat analysis

- Nozioni base di architettura dei sistemi
- Threats
  - Internal and External
  - Advanced Persistent Threat and Emerging Threats
  - MITRE att&ck, SANS
- Vulnerabilities
  - National Vulnerability Database
  - Open Web Application Security Project (OWASP)
- Esercitazione:
  - Password cracking

Lezione 3

Laboratorio di cyber security: Malicious cybersecurity activities e tecniche di business continuity

- Situazione degli attacchi riusciti nel mondo e in Italia suddivisi per tipologia d'attacco, vittime, luoghi e tecniche. (presentazione rapporto Clusit)
  - Esempi di attacchi riusciti
- Principali tecniche d'attacco
  - DOS e DDOS
  - Data exfiltration

        - phishing
        - defacement
        - malaware -> ransomware
    - Tecniche di difesa
        - Business continuity
        - Disaster Recovery
        - patch management

Lezione 4

Risk Assessment Cybersecurity: analisi e contestualizzazione delle minacce

- Analisi e trattamento del rischio cyber
- Episodi eclatanti di incidenti di sicurezza
- Evoluzione delle minacce e degli attori
- ENISA Threat Landscape,
- Panoramica delle principali minacce
- MITRE ATT&CK
- Metodologie di analisi OCTAVE, NIST, ISO31000
- Case study Risk Analysis

Lezione 5

Laboratorio di cyber security: Nozioni tecniche avanzate

- Sicurezza dei dati
- Cloud (vantaggi e nuovi problemi)
- Crittografia (cosa è e a cosa serve)
- Steganografia (cosa è e a cosa serve)
- Breve storia della crittografia
- Crittografia classica
    - simmetrica
    - asimmetrica
    - firma elettronica
- Cenni di crittografia avanzata

Lezione 6

Normative e Best practices di riferimento della cybersecurity

- Normative Cybersecurity UE ed ITA
- Perimetro Strategico Nazionale Cybersecurity
- Standards & Best Practices Cybersecurity
- Sistemi di gestione
- ISO/IEC 27001 e 27002
- ISO 22301 - Business Continuity
- Case study BIA
- Case Study DRP
- Standard USA (CSF, CIS, NIST SP800-53
- Case study NIS2 & DORA

Lezione 7

L’importanza della sicurezza fisica nella sicurezza informatica

- Fondamenti di Sicurezza Fisica e Security Convergence
- Analisi di dettaglio controlli di sicurezza fisica ISO 27001
- I controlli di sicurezza fisica nello Standard NIST SP800-53
- Sicurezza e sorveglianza nei Data Center
- Trasferimento delle responsabilità
- Cloud & Shared Reponsibility Model
- Case Study: Supernap & Google

Lezione 8

Cybersecurity risk management: Cybersecurity plan e Cybersecurity Management

- Progettazione e sviluppo di un Cybersecurity plan
  - Elementi essenziali
  - SWOT analysis e ROI del cybersecurity plan
- Processi del Sistema di gestione dell'Information security
  - Risk management
  - Incident and Change management
  - Internal audit, valutazione delle performance e processo di miglioramento

Lezione 9

Competenze e consapevolezza in materia di cybersecurity

- Concetti fondamentali
- Le competenze secondo la ISO/IEC 27021
- European Cybersecurity Skills Framework
- Panoramica formazione e certificazioni personali
- Programmi di formazione del cittadino ed aziendali
- Case study: "Secure The Humans!" tramite programma aziendale SAT
- AR-in-a-Box

Lezione 10

Fondamenti di Cybersecurity: Fondamenti Normativi

- Direttiva NIS 1 (Direttiva (UE) 2016/1148)
- Direttiva NIS 2 (Direttiva UE 2022/2555)
- EU-Cybersecurity Strategy
- EU-Cybersecurity Act – Regulation (EU) 2019/881 e il ruolo di:
  - European Network and Information Security Agency (ENISA);
  - Computer Emergency Response Team (CERT-EU);
  - Computer Security Incident Response Team (CSIRT);
- European Cyber Security Organisation (ECSO).
- Perimetro Cibernetico Nazionale
  - Decreto Legge 21 settembre 2019, n. 105
  - DPCM 131/2020 del 21 ottobre 2020
- Decreto legislativo 8 giugno 2001, n. 231 e i reati informatici

Lezione 11

Il contributo della Funzione Compliance nel processo di ICT Compliance

- Governo e organizzazione del sistema presidio della sicurezza informatica
  - Ruolo degli Organi Aziendali
  - Ruolo delle Funzioni Aziendali di Controllo
  - Ruolo della Funzione ICT e della Funzione di Sicurezza Informatica
  - Caso Partico: Organizzazione Cybersecurity di Avio SpA
  - Esercitazione "Attacco Ramsonwere" intervento degli Organi Aziendali e profili 231
  - Presidio delle Esternalizzazioni ICT
- Il contributo della Compliance per le tematiche di Compliance ICT
- Perimetro normativo di ICT Compliance

Per esigenze di natura organizzativa e didattica, la Scuola si riserva la facoltà di rinviare, di modificare, così come di spostare le date delle lezioni rispetto al calendario inizialmente prestabilito. Inoltre, si riserva il diritto di modificare in ogni momento i contenuti, dei programmi ed il corpo docente al fine di perseguire miglioramenti didattici in linea con i cambiamenti di mercato e le subentrate esigenze organizzative.