Università degli Studi di Cagliari

CORSO VALORE PA 2021

CYBERINTELLIGENCE, DIGITAL INVESTIGATION E REATI INFORMATICI

(Corso di primo livello in materia di “Cyberintelligence digital investigation & social media intelligence; Intercettazioni, tecnologie, utilizzo e quadro normativo-giuridico - Reati e crimini finanziari – reati e crimini informatici - Analisi del comportamento e psicologia criminale”)

PROGRAMMA DETTAGLIATO

MODULO 1, DURATA 6 ORE: La Cyberintelligence

Obiettivi: Analizzare i concetti di base in materia di Cyberintelligence, investigazioni digitali, sicurezza e vulnerabilità delle infrastrutture critiche

Argomenti:

- Concetti generali di Cyber Intelligence
- Analisi del contesto e dei target di riferimento
- Classificazione dell'informazione: basi del Social engineering, Phishing e cyber-esche, esposizione delle informazioni
- L'importanza dei Social media per il reperimento delle informazioni
- Aspetti economici della insicurezza
- Investigazioni e tecniche di ingegneria sociale
- Social network: geotag, e-mail tracking
- Contesti di rete ignoti: Deep and dark web Exploitation
- Industrial Espionage: vulnerabilità delle infrastrutture critiche
- Profilazione degli utenti: ricerche di persone e società
- Data breach and Data leakage

MODULO 2, DURATA 6 ORE: Acquisizione e produzione in giudizio delle prove digitali - Aspetti giuridici

Obiettivi: consentire di comprendere le regole procedimentali che governano l'acquisizione, la produzione e l'utilizzabilità delle prove digitali nella fase delle indagini preliminari e nel giudizio; i limiti, le garanzie dei diritti dei soggetti coinvolti (imputato ovvero vittima del reato) ovvero dei terzi estranei nonché il ruolo affidato alla polizia giudiziaria, al pubblico ministero ed al giudice. Si illustreranno infine le investigazioni del difensore e l' accesso delle parti private alle nuove tecnologie in materia di prova.

Argomenti:

- Le prove tipiche e le prove atipiche
- I mezzi di prova e i mezzi di ricerca della prova
- Intercettazioni di conversazioni e comunicazioni (con particolare riguardo alle intercettazioni di comunicazioni informatiche e telematiche nonché all'impiego del captatore informatico)
- Ispezioni informatiche
- Perquisizioni informatiche
- Sequestro informatico
- Acquisizione dei tabulati telefonici
- Pedinamento satellitare mediante GPS
- Geolocalizzazione
- Videoriprese di immagini non comunicative in luoghi riservati
- Videoriprese di immagini in luoghi pubblici
- I software di polizia predittiva
- L'attività investigativa difensiva: limiti e operatività

MODULO 3, DURATA 6 ORE: Acquisire elementi digitali come prove legali - Digital Forensics

Obiettivi: Presentare le diverse modalità di investigazione "digitale" e le tecniche di indagine informatica, investigazione difensiva nel campo dei crimini informatici e dei crimini comuni la cui prova sia costituita da

dati digitali o veicolati da sistemi informatici. Prospettare un quadro complessivo dei problemi tecnici legati alla forensics in connessione con le problematiche giuridiche che sottendono a tali tipi di indagini. Illustrare in particolare le " best-practices" da utilizzare sul campo per acquisizione, conservazione, analisi e produzione dei dati digitali rinvenuti nei computer e dei flussi telematici per la loro utilizzabilità nell'ambito giudiziale. Fornire le conoscenze giuridiche e tecnologiche in materia di intercettazioni digitali, anche con riguardo ai c.d. "trojan di stato".

Argomenti:

- Concetti generali della Digital Forensics
- Importanza dell'approccio nella scena del crimine: la metodologia e la tecnica
- Le varie fasi della D.F.: Identificazione, Preservazione, Estrazione, Analisi, Report, Catena di custodia
- Il contesto di analisi: Live Analysis, Dead Analysis
- Altri campi della Digital Forensics
- Strumenti, hardware e software da utilizzare; best practices e standard di riferimento
- Le intercettazioni digitali: profili generali, tecnologie e quadro normativo
- I "trojan" destinati alle intercettazioni: funzionamento, potenzialità e disciplina giuridica

MODULO 4, DURATA 6 ORE: Data investigation, social media intelligence e informazioni ricavabili dalle fonti aperte (OSINT)

Obiettivi: fornire un'approfondita conoscenza della disciplina giuridico-normativa e delle tecnologie correlate al mondo dell'Intelligence e della Digital Investigation, focalizzandosi sui metodi di analisi delle fonti aperte e sulla loro applicazione pratica nelle fasi di ricerca di informazioni attraverso particolari strumenti e metodologie.

Argomenti:

- Il target: cosa e dove cercare, la geolocalizzazione, file e matadata
- Social networks e relazioni correlate
- Uso dei motori di ricerca standard: metodologie, strumenti, tecniche
- Motori di ricerca non standard; tor
- Le Fonti: standard e non standard, verifica e validazione delle fonti e delle informazioni
- Analisi delle immagini: tante informazioni che non si vedono
- OSINT tools; strumenti on-line e programmi dedicati
- Documentazione delle evidenze: creazione di report con logiche degli eventi

MODULO 5, DURATA 6 ORE: Crimini e criminalità informatica

Obiettivi: fornire conoscenze di taglio penalistico-sostanziale e criminologico in materia di reati informatici e finanziari

Argomenti:

- Computer Crimes: analisi della normativa rilevante; Reati posti a tutela dell'inviolabilità del domicilio – III.2 Reati posti a tutela dell'inviolabilità dei segreti – III.3 Delitto contro il patrimonio mediante frode – III.4 Illeciti penali in ambito protezione dei dati personali;
- Cyber Crimes nella pubblica amministrazione: analisi del quadro normativo applicabile alle pubbliche amministrazioni; dalla convenzione di budapest alla direttiva 2016/148/ce;
- I reati finanziari nei nuovi scenari digitali
- Analisi del comportamento e psicologia del criminale informatico
- introduzione alla psicologia giuridica e criminologia
- psicologia investigativa
- psicologia giudiziaria e forense
- psicologia del criminale informatico e tecniche di profiling/digital profiling

MODULO 6, DURATA 6 ORE: Sicurezza e resilienza dei sistemi tecnologici (Parte prima)

Obiettivi: fornire conoscenze e competenze in materia di sicurezza informatica, cybersecurity, infrastrutture critiche, ricognizione e prevenzione delle minacce e attacchi che minano la sicurezza delle informazioni, Best Practices internazionali e obblighi normativi. Il ruolo centrale delle strategie di difesa all'interno delle organizzazioni. L'infrastruttura cyber-resiliente in grado di adattarsi ai differenti contesti potenzialmente esposti a condizioni di rischio. Le misure minime di sicurezza ICT emanate dall'AgID. La valutazione e il miglioramento del livello di sicurezza informatica delle organizzazioni e delle pubbliche amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

Argomenti:

- Argomenti: Concetti generali di Information e Cybersecurity
- La gestione dell'infrastruttura tecnologica e dei sistemi informativi
- Autenticazione e accesso alle risorse: utilizzo e gestione delle credenziali di accesso, abilitazione dei sistemi MFA
- Vulnerabilità dei sistemi e contromisure
- Le misure minime di sicurezza ICT: NIST CIS
- L'implementazione delle politiche di sicurezza
- Standard, procedure e documentazione
- Gestione degli incidenti: definizione del processo
- Monitoraggio e controllo: i log degli eventi, aspetti di performance e di sicurezza
- Concetti generali; concetti di Information security e Cyber security
- Analisi del contesto di riferimento: il perimetro di riferimento, individuazione dei targets
- Le vulnerabilità: il ciclo di vita del processo di gestione
- Le risorse informatiche: gestione e controllo
- La formazione: importanza della consapevolezza e della comunicazione
- Le procedure: Standard di riferimento, importanza delle procedure e della documentazione

MODULO 7, DURATA 6 ORE: Sicurezza e resilienza dei sistemi tecnologici (Parte seconda)

Obiettivi: fornire conoscenze e competenze in materia di sicurezza informatica, cybersecurity, infrastrutture critiche, ricognizione e prevenzione delle minacce e attacchi che minano la sicurezza delle informazioni, Best Practices internazionali e obblighi normativi. Il ruolo centrale delle strategie di difesa all'interno delle organizzazioni. L'infrastruttura cyber-resiliente in grado di adattarsi ai differenti contesti potenzialmente esposti a condizioni di rischio. Le misure minime di sicurezza ICT emanate dall'AgID. La valutazione e il miglioramento del livello di sicurezza informatica delle organizzazioni e delle pubbliche amministrazioni, al fine di contrastare le minacce informatiche più frequenti, al fine di contrastare le minacce informatiche più frequenti.

Argomenti:

- Cybersecurity delle infrastrutture critiche: Le origini e le caratteristiche delle infrastrutture critiche; Presidential Decision Directive 62 e 63 degli Stati Uniti; La Direttiva 2008/114/CE e il Decreto Legislativo 61/2011; La Direttiva 2013/40/UE; Punti di contatto tra disciplina delle infrastrutture critiche, la Direttiva NIS e il GDPR.
- Sicurezza e Resilienza rispetto alle minacce: Sicurezza fisica e logica
- Identificazione del perimetro: identificazione dei targets
- Minacce informatiche: mitigare l'Impatto delle minacce, stratificare la sicurezza sul contesto tecnologico
- Aspetti generali sull'Internet delle cose (IoT):vSmart City e Smart Industry
- Standard e linee guida di riferimento
- Aspetti generali della Data Protection: La disciplina privacy nei rapporti di lavoro pubblici in rapporto al Reg. UE 2016/679; I controlli a distanza sull'attività del lavoratore e riforma dell'art. 4 dopo il Jobs act: videosorveglianza, Geolocalizzazione, dispositivi di riconoscimento biometrico; Le soluzioni biometriche per il controllo accesso e per la rilevazione presenze nella PA: analisi del Decreto c.d. Concretezza ed il parere del Garante per la protezione dei dati personali
- Le figure e i ruoli richiesti nel Piano Triennale per l'Informatica nella Pubblica Amministrazione
- Diritti e doveri delle quattro figure cardine della digitalizzazione: RTD, DPO, Resp. della Conservazione, Amministratore di Sistema
- Definizione di un modello di Information Security Governance
- Contromisure ispirate alla Defense in Depth e Maturity Model
- Requisiti e Policy per la Sicurezza delle Informazioni
- Strumenti SW a supporto delle conformità di legge
- Vulnerability Management, Exposures, Remediation Plan
- Ruoli e responsabilità nella Business Continuity

QUESTIONARIO FINALE DI VALUTAZIONE, durata 2 ore.