SUPSI

MAS ICT Systems, Security and Cybercrime

Master of Advanced Studies

Presentazione

La sicurezza informatica è tra i settori che hanno visto gli sviluppi più vertiginosi degli ultimi decenni, trasformandosi da scienza emergente puramente tecnologica negli anni ‘70 e ‘80 in una dimensione olistica che include oggi tecnologia, psicologia, sociologia, studi comportamentali e analisi dell’emotività e della suscettibilità umana.Le tecnologie informatiche e le insidie alla sicurezza celate dai nuovi media (e soprattutto dal nostro modo di interpretarli e di farne uso) hanno pervaso tutta la nostra esistenza, sia di privati cittadini, sia di organizzazioni, sia di aziende, sia di governi, sia di genitori.

Il contesto risulta essere molto complesso, le necessità in termini di controllo e di sicurezza sempre più elevate.

Obiettivi

Obiettivo della formazione è quello di rispondere alle nuove sfide poste dagli sviluppi tecnologici e sociali in termini di sicurezza e delle tendenze in atto nell’approcciare la sicurezza nell’era cibernetica in modo olistico.

Destinatari

Il Master of Advanced Studies SUPSI in ICT Systems, Security and Cybercrime è un'offerta di formazione continua destinata ai professionisti dell'informatica e dei sistemi collaborativi di informazione che hanno, o intendono avere, una posizione di guida nell'ambito dell'organizzazione, dell'erogazione e della gestione dei servizi IT.

Requisiti

Professionisti con conoscenze di gestione dei sistemi informativi e di fondamenti di sicurezza e delle minacce del mondo digitale.

Certificato

Master of Advanced Studies Master of Advanced Studies SUPSI in ICT System, Security and Cybercrime, subordinato al superamento di tutti gli esami previsti.

Crediti di studio ECTS

67 ECTS

Programma

Fondamenti di sicurezza dei sistemi e delle reti
- Sicurezza e vulnerabilità dei sistemi, delle reti e delle soluzioni distribuite
- Laboratorio: di sicurezza dei sistemi e delle reti, fondamenti di penetration testing
- Laboratorio di Business Continuity
- La crittografia moderna e le sue applicazioni alle reti di comunicazione
- Advanced Storage Architectures
- Streaming e multicasting, VoIP e integrazione nelle reti VPN
- Analisi criminologica del cyberspazio: cybercrime, quo vadis?
- Open Source Security Testing Methodology (OWASP, OPST, OPSA)
- Cloud security: i benefici e le insidie dei sistemi altamente integrati che fanno uso di cloud computing
- Social engineering, user profiling, il fattore umano e cyber-security

Approfondimenti: sicurezza di applicazioni e servizi; strategie difensive contro le minacce tecnologiche
- Standard e metodologie per lo sviluppo di dispositivi, sistemi e software sicuri. Security by design, Privacy by design
- Architetture dei sistemi IoT; la loro sicurezza; vulnerability assessment
- La sicurezza dei sistemi industriali e delle infrastrutture critiche
- Fondamenti di Computer e Network Forensic: procedure, strumenti, limiti
- La sicurezza nei dispositivi mobili: vulnerabilità dei sistemi, insidie della proximity communication (ad es. NFC), rischi correlati, tecniche di protezione
- La sicurezza e le insidie dei framework web e di collaborazione
- L'evoluzione delle tecniche di attacco e delle famiglie di malware
- Tecniche di hacking del software e delle infrastrutture
- Hacking everything 1 – la fragilità dei sistemi concepiti senza prestare le dovute attenzioni alla sicurezza
- Hacking everything 2 – human vulnerability assessment (HVA): human hacking, attacchi non convenzionali tramite la componente umana
- La mia rete è infetta? Gestione della sicurezza e dei sistemi di monitoraggio del traffico aziendale
- Laboratorio: i sistemi di difesa e di monitoraggio della sicurezza
- Analisi delle principali tecniche di attacco: virus, botnets, DDoS, spam, phishing,
spear phishing, MITM, DNS Poisoning, CSS, data sniffing, intrusion systems, …
- Cyber Threat Intelligence
- Laboratorio tecnologie di Networking: aspetti di convergenza delle tecnologie, qualità dei servizi, reti P2P e tecniche di virtualizzazione
- La sicurezza dei sistemi operativi, dei server e dei data center
- Big Data e Machine Learning
- Preparazione alla certificazione CISM
- Network Evolution - Next generation networks. Next generation security architectures

Strumenti di management
- Business continuity management
- Aspetti giuridici della sicurezza informatica
- Mind mapping e sicurezza informatica. Teoria dei sistemi complessi
- Le diverse policies e documenti per la gestione della sicurezza in azienda
- Security Operations Centers
- Risk management e incident response; dalla gestione del rischio alla nascita di un CSIRT
- Metodologie per la protezione dei dati, il GDPR e le sue implicazioni

Durata

688 ore-lezione

Responsabile/i

Angelo Consoli, ricercatore SUPSI

Relatore/i

Professionisti e docenti con esperienze significative nel proprio ambito di insegnamento

Date

L'inizio delle lezioni è previsto al 11 dicembre 2019. Il calendario dei corsi è disponibile all'indirizzo:
www.supsi.ch/fc/offerta-formativa/advanced-studies/mas/ict-systems-security-cybercrime

Orari

17.30-21.00

Luogo

SUPSI, Dipartimento tecnologie innovative, Manno

Costo

Il costo complessivo della formazione è di CHF 21’000.– (CHF 7'000.– per anno accademico), più CHF 1'000.-- quale quota per l'esame finale.
È previsto uno sconto del 10% per i membri individuali dell'Associazione Ticinese Elaborazione Dati (ATED) e Swiss Engineering (ATS).

Tali costi comprendono la documentazione didattica, gli esami alla fine di ogni modulo e il rilascio dei certificati.

Informazioni

SUPSI, Dipartimento tecnologie innovative, Galleria 2, 6928 Manno
tel.+41 (0)58 666 66 84
fax +41 (0)58 666 65 71
dti.fc@supsi.ch
www.supsi.ch/fc/offerta-formativa/advanced-studies/mas/ict-systems-security-cybercrime

Termine d'iscrizione

Entro il 22 novembre 2019

Link per le iscrizioni

https://fc-catalogo.app.supsi.ch/Course/Details/1000002750

Condizioni generali

Iscrizioni e ammissione
Per partecipare a un corso l'iscrizione è obbligatoria e vincolante per il partecipante. L'ammissione ai corsi di lunga durata è tuttavia subordinata alla verifica dei requisiti richiesti dal percorso formativo. Per garantire un buon livello qualitativo, SUPSI può fissare un numero minimo e massimo di partecipanti.

Quota d'iscrizione
Se il corso è a pagamento, la quota di iscrizione è da versare sul conto bancario della Scuola universitaria professionale della Svizzera italiana (SUPSI):
- Dalla Svizzera, prima dell'inizio del corso, tramite la polizza che verrà inviata con la conferma di iscrizione
- Dall'estero, dopo la conferma d'iscrizione, con bonifico bancario intestato a SUPSI presso la Banca dello Stato del Cantone Ticino, CH-6501 Bellinzona
IBAN CH05 0076 4190 8678 C000C
Swift Code BIC: BSCTCH 22
Clearing 764
Causale: Titolo del corso

Obbligo di pagamento della quota di iscrizione
Il pagamento della quota di iscrizione è da effettuarsi entro 30 giorni dalla data della fattura. La conferma di iscrizione e la fattura sono trasmesse al partecipante dopo il termine di iscrizione al corso. In casi particolari è possibile richiedere una rateazione della quota d'iscrizione; la richiesta scritta va inoltrata alla segreteria competente entro il termine di iscrizione. Verso la SUPSI il debitore del pagamento della quota è il partecipante, che attraverso l'iscrizione al corso, riconosce espressamente il proprio debito ai sensi della LEF, nonché l'obbligo di pagamento e si impegna al versamento dell'importo dovuto. Se la formazione è finanziata dal datore di lavoro o da un terzo, il partecipante rimane comunque debitore verso la SUPSI fino ad effettivo pagamento della quota da parte del datore di lavoro o del terzo indicato. Al riguardo il partecipante si impegna e si obbliga verso la SUPSI ad assumere il pagamento della quota di iscrizione, nel caso in cui il datore di lavoro o il terzo indicato, non dovesse corrispondere l'importo dovuto. Le disposizioni relative all'obbligo di pagamento non si applicano se i corsi non prevedono il versamento di una tassa.

Annullamenti e rinunce
Nel caso in cui il numero di partecipanti fosse insufficiente o per altri motivi, SUPSI si riserva il diritto di annullare il corso. In tal caso, gli iscritti saranno avvisati tempestivamente e, se avranno già versato la quota di iscrizione, saranno integralmente rimborsati. Qualora sia il partecipante a rinunciare, quest'ultimo è tenuto al versamento del 50% della quota di iscrizione se notifica l'annullamento:
- nei 7 giorni che precedono l'inizio del corso, se iscritto alla formazione breve (0-9 ECTS)
- nei 21 giorni che precedono l'inizio del corso, se iscritto alla formazione lunga (10-60 ECTS)
Casi particolari possono essere analizzati e decisi con la direzione di dipartimento. In caso di rinunce notificate successivamente ai termini di cui sopra, il partecipante non avrà diritto al rimborso e l'intera quota di iscrizione diverrà immediatamente esigibile. Sono fatte salve eventuali deroghe previste nei regolamenti di ogni singolo corso, alle quali si fa espressamente richiamo. Chi fosse impossibilitato a partecipare può proporre un'altra persona previa comunicazione a SUPSI e accettazione da parte del responsabile del corso. In caso di rinuncia al corso per malattia o infortunio del partecipante, la fattura inerente la quota di iscrizione potrà essere annullata, a condizione che sia presentato un certificato medico.

Modifiche
SUPSI si riserva il diritto di modificare il programma, la quota di iscrizione e il luogo dei corsi a seconda delle necessità organizzative.

Copertura assicurativa infortuni
I partecipanti non sono assicurati da SUPSI.

Privacy
Il trattamento dei dati avviene nel rispetto della legislazione svizzera (Legge federale sulla protezione dei dati e relativa Ordinanza).

Foro competente
Per eventuali controversie il foro competente è Lugano, che è pure il foro esecutivo ai sensi della LEF (Legge federale sulla esecuzione e sul fallimento). Il diritto applicabile è quello svizzero.