Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI SICUREZZA E PROTEZIONE DEI DATI E DEI SISTEMI INFORMATICI

SETTORE SCIENTIFICO

INF/01

CFU

9

PROGRAMMA DIDATTICO

Il docente si riserva il diritto di modificare i titoli delle delle lezioni

1 - INTRODUZIONE ALLA CYBERSECURITY 2 - ELEMENTI FONDAMENTALI DEL PERIMETRO DI SICUREZZA E TERMINOLOGIA 3 - SICUREZZA DELLE INFORMAZIONI 4 - MINACCE, ATTACCANTI E RISCHIO INFORMATICO 5 - ATTACCHI, CONTROLLI E CONTROMISURE 6 - AUTENTICAZIONE 7 - MECCANISMI DI AUTENTICAZIONE 8 - CONTROLLO DEGLI ACCESSI 9 - CRITTOGRAFIA: CONCETTI GENERALI 10 - CIFRATURA A CHIAVE SIMMETRICA 11 - CIFRATURA A CHIAVE ASIMMETRICA 12 - SCAMBIO DELLE CHIAVI E CERTIFICATI 13 - SUPPORTO ALL'INTEGRITA' DELL'INFORMAZIONE 14 - FIRMA DIGITALE 15 - SUPPORTO ALLA DISPONIBILITÀ 16 - TIPI DI ATTACCO ALLA DISPONIBILITA' 17 - DISTRIBUTED DENIAL OF SERVICE E BOTNET 18 - I MALWARE 19 - COMPORTAMENTO ED EFFETTI DI UN MALWARE 20 - PROPAGAZIONE, ATTIVAZIONE E AREE DI RESIDENZA DI UN MALWARE 21 - CONTROMISURE PER I MALWARE 22 - ATTACCHI INFORMATICI: ATTACCHI AI BROWSER 23 - ATTACCHI TRAMITE SITI WEB 24 - ATTACCHI TRAMITE E-MAIL 25 - DIFESA PERIMETRALE DELLA RETE 26 - I FIREWALL 27 - SISTEMI DI DIFESA DALLE INTRUSIONI 28 - INTRUSION PREVENTION SYSTEMS E SIEM 29 - ANALISI E ASSESSMENT DI VULNERABILITÀ 30 - DISASTER RECOVERY - PANORAMICA 31 - DISASTER RECOVERY COME ATTIVITÀ STRATEGICA 32 - DISASTER RECOVERY COME PIANO OPERATIVO 33 - DISASTER RECOVERY COME PROGETTO AZIENDALE 34 - VERSO UN PIANO DI RIPRISTINO 35 - SVILUPPARE IL PIANO DELLE WORKSTATION E DEI LOCALI 36 - SVILUPPARE IL PIANO DI RIPRISTINO DI INFRASTRUTTURA IT E DEI DATI

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione

Lo studente acquisirà la conoscenza delle problematiche di protezione dati e sarà in grado di comprendere le possibili soluzioni nei diversi ambiti applicazione. Conoscerà le principali caratteristiche degli attacchi informatici contro i principali sistemi operativi.

Capacità di applicare conoscenza e comprensione

Lo studente sarà in grado di assicurare privatezza e sicurezza in scenari emergenti, dove i dati sono spesso memorizzati, gestiti ed elaborati da server esterni non completamente fidati. Saprà in grado di comprendere la sulla documentazione tecnica fornita dai servizi con cui interagisce e individuare la tipologia di documentazione necessaria

per lo svolgimento delle sue funzioni.

Autonomia di giudizio

Lo studente avrà acquisito sensibilità sul tema della protezione dati, e sarà in grado di individuare le soluzioni tecnologiche per garantire la privatezza e la protezione dati in diversi scenari, e di scegliere il metodo di analisi più adeguato a capire le funzionalità di un programma malevolo.

Abilità comunicative

Lo studente saprà presentare gli argomenti svolti nel corso con rigore formale e completezza. Sarà in grado di utilizzare la terminologia tecnica e formale nella presentazione delle soluzioni da lui individuate e di interfacciarsi in modo efficiente con gli attori del settore.

Capacità di apprendimento

Lo studente sarà in grado di consultare la letteratura scientifica del settore per approfondire autonomamente gli argomenti del corso in relazione ad aspetti formali non approfonditi durante le lezioni.

Programma didattico

Programma didattico (per macro aree + numero lezioni previste)

Introduzione alla protezione dei dati (9 lezioni)

Controllo dell'accesso: politiche, modelli e meccanismi (9 lezioni)

Basi di dati multilivello (9 lezioni)

Integrità delle query (9 lezioni)

Condivisione controllata di dati in query distribuite (9 lezioni)

Differential privacy e blockchain (9 lezioni)

Modalità di raccordo con altri insegnamenti (indicare le modalità e gli insegnamenti con i quali sarà necessario raccordarsi)

Nessun raccordo

OBIETTIVI

Il corso ha l'obiettivo di fornire una visione aggiornata degli ultimi sviluppi della cybersecurity, di presentare, in una prospettiva critica, i principi alla base della sicurezza dei sistemi informatici e di analizzare le minacce a cui sono sottoposti i sistemi di calcolo con relative contromisure. Vengono analizzati i problemi di vulnerabilità della sicurezza nell'ambito dei Database, della protezione e privatezza dei dati. Vengono illustrate le nozioni di base delle metodologie di progettazione di sistemi sicuri, e discussi esempi di applicazione, infine analizzati i principali approcci per definire le politiche di sicurezza ed i principali attacchi ai protocolli e alle infrastrutture di rete.

MODALITÀ DI ESAME ED EVENTUALI VERIFICHE DI PROFITTO IN ITINERE

/**/
L'esame può essere sostenuto sia in forma scritta che in forma orale.

L'esame orale consiste in un colloquio nel corso del quale il docente formula di solito tre domande. L'esame scritto consiste nello svolgimento di un test con 31 domande. Per ogni domanda lo studente deve scegliere una di 4 possibili risposte. Solo una risposta è corretta.

Sia le domande orali che le domande scritte sono formulate per valutare sia il grado di comprensione delle nozioni teoriche sia la capacità di ragionare utilizzando tali nozioni. Le domande sulle nozioni teoriche consentiranno di valutare il livello di comprensione. Le domande che richiedono l'elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l'autonomia di giudizio maturati dallo studente.

Le abilità di comunicazione e la capacità di apprendimento saranno valutate attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze, e-tivity report, studio di casi elaborati) proposti dal docente o dal tutor.

MODALITÀ DI ISCRIZIONE E DI GESTIONE DEI RAPPORTI CON GLI STUDENTI

/**/
L'iscrizione ed i rapporti con gli studenti sono gestiti mediante la piattaforma informatica che permette l'iscrizione ai corsi, la fruizione delle lezioni, la partecipazione a forum e tutoraggi, il download del materiale didattico e la comunicazione con il docente.

Un tutor assisterà gli studenti nello svolgimento di queste attività.

Attività di didattica erogativa (DE) 54 Videolezioni + 54 test di autovalutazione

Impegno totale stimato: 54 ore

Attività di didattica interattiva (DI) ed e-tivity con relativo feed-back al singolo studente da parte del docente o del tutor Redazione di un elaborato

Partecipazione a una web conference

Svolgimento delle prove in itinere con feedback

Svolgimento della simulazione del test finale, Totale 9 ore

Attività di autoapprendimento 162 ore per lo studio individuale

Libro di riferimento Dispense del docente.