



UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Cybersecurity for Data Science

2627-2-FDS02Q015

Obiettivi

Conoscenza e comprensione:

- punti esposti a rischi nelle strutture che costituiscono un sistema informatico
- principali tecniche di attacco informatico e loro impatto nelle strutture di elaborazione
- metodi di riduzione del rischio nei sistemi informatici, reti e software
- strumenti di ricerca e protezione dalle vulnerabilità, come firewall e antivirus

Applicare conoscenze e comprensione:

- analizzare un sistema informatico per individuare elementi che introducono rischi di sicurezza
- saper valutare correttamente il rapporto costi-benefici delle principali difese dei sistemi informatici, per diversi ambiti operativi
- saper configurare e usare correttamente i più comuni strumenti software per la sicurezza, anche da ambito open source

Contenuti sintetici

La cybersecurity: in quali tecnologie è rilevante, e suoi obiettivi: terminologia di base (vulnerabilità, exploit, ...); principio fondante: le tecnologie nascondono possibili utilizzi non previsti dai loro progettisti. Protezione dei dati: crittografia, filtraggio del traffico su rete, rilevazione delle minacce. Interventi non tecnologici per aumentare la sicurezza: consapevolezza e buone pratiche. Casi di studio: piattaforme di gestione dati, e irrobustimento della loro sicurezza.

Programma esteso

1-Introduzione alla cybersecurity:

- a.principio fondante, problemi specifici in ambito informatico
- b.ruoli: sviluppatori software, attaccanti, amministratori di sistema, analisti
- c.obiettivi: riservatezza, integrità, disponibilità
- d.esempi di incidenti

2-Vulnerabilità e attacchi:

- a.errori nel software, il "buffer overflow"
- b.debolezze delle reti, intercettazione e falsificazione dei dati
- c.ingegneria sociale
- d.raccolta di informazioni sulle strutture informatiche
- e.blocco dei servizi

3-Difese:

- a.aggiornare il software
- b.filtraggio e monitoraggio del traffico su rete
- c.buone pratiche

4-Crittografia:

- a.metodi (chiave simmetrica, chiave pubblica)
- b.alcuni strumenti (PGP, TLS)
- c.utilizzo errato della crittografia, cattive implementazioni

5-Aspetti di sicurezza specifici dei grandi archivi, piattaforme e difese

6-Casi di studio, incidenti reali e alcuni strumenti open source

Prerequisiti

.

Modalità didattica

- 10~12 lezioni da 2 ore svolte in modalità erogativa in presenza;
- 2~4 lezioni da 2 ore svolte in modalità erogativa in remoto asincrono;
- 6 attività di laboratorio da 3 ore svolte in modalità interattiva in presenza;

Materiale didattico

C. Pfleeger - S. Pfleeger, "Security in Computing", Pearson, 2015

Periodo di erogazione dell'insegnamento

primo Semestre

Modalità di verifica del profitto e valutazione

La verifica dell'apprendimento comprende una prova scritta e una breve relazione presentata a colloquio orale:

lo scritto consiste in alcune domande discorsive su una selezione di argomenti presentati a lezione (indicata all'inizio delle lezioni),

la relazione deve riguardare attività sperimentali su uno degli argomenti presentati a lezione, scelto dallo studente.

Le due prove contribuiscono al voto finale ciascuna per il 50% del totale.

Orario di ricevimento

Su appuntamento concordato via email.

Sustainable Development Goals
