# Introduzione alla *Cybersecurity*

Il corso affronta il problema della sicurezza, analizzando tutti i componenti a rischio presenti in un'azienda che utilizza sistemi informatici connessi con reti aperte basate sul protocollo TCP/IP. Una volta introdotte le problematiche di scenario, si esaminano gli attacchi ai sistemi e le possibili azioni e contromisure. Vengono presentati approfondimenti specifici sulle tecniche più diffuse tra gli hacker per attaccare un sistema.
Il corso prosegue con la sicurezza applicativa, cioè l'insieme delle metodologie e degli strumenti adottati per rendere sicure le applicazioni informatiche che gli utenti autorizzati utilizzano per accedere, elaborare e memorizzare i dati presenti nel sistema informativo aziendale.
L'attenzione viene poi focalizzata sulla sicurezza di rete e vengono esaminate le possibili soluzioni per realizzare una adeguata protezione perimetrale utilizzando Firewall e IPS.
Il corso si conclude con la crittografia, utilizzata come strumento per assicurare riservatezza e integrità ai dati e per prevenire rischi derivanti dall'accesso non autorizzato alle informazioni veicolate tramite servizi di larga diffusione, come, la posta elettronica e il WWW.

## Agenda (3 giorni)

**Cybersecurity:**

- Cybersecurity e Information Security
- Sicurezza di rete
- Sicurezza delle applicazioni

**Cybersecurity: attacchi/minacce e possibili contromisure**

- Rapporti sulla sicurezza
- Norme di riferimento
- Principali minacce
  - Attacchi tradizionali
  - Credential stuffing
  - Ransomware
  - DOS e DDOS
  - Advanced Persistent Threats (APT)
  - Fattore umano
- Sicurezza delle applicazioni
- Vulnerabilità
- Web App Hacking
  - Command execution
  - File upload
  - XSS (Cross Site Scripting) Reflected & Stored
  - SQL Injection & SQL Injection blind
  - Cross Site Request Forgery (CSRF)

**Sicurezza in rete**

- Sicurezza perimetrale, il firewall
  - Stateless Packet Filtering
  - Proxy
  - Stateful Firewall
  - Application Inspection and Control Filtering
  - Firewall zonali
  - Secure Web Gateway
  - Web Application Firewall
  - Funzionalità complementari
- IPS, SIEM, SOC e altro
- Introduzione alle VPN

**Laboratorio:**

- Information gathering

**Crittografia e certificati digitali**

- Crittografia simmetrica classica
- Lab: GPG e OpenSSL
- Crittografia simmetrica o a chiave segreta
- Crittografia asimmetrica o a chiave pubblica
- Steganografia

- Funzioni di hashing ed HMAC
- Verifica della autenticità: i codici MAC
- Certificati Digitali e PKI

## Obiettivi

Al termine del corso i partecipanti sono in grado di:

- avere una chiara comprensione delle problematiche della sicurezza informatica e delle più comuni tipologie di attacco
- conoscere gli strumenti più idonei per rivelare/contrastare attacchi informatici.

## Destinatari

Responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete, progettisti di sistemi di rete e tutti coloro che desiderano avere una visione d'insieme delle varie tematiche connesse alla sicurezza dei sistemi e delle reti.

## Prerequisiti

Conoscenza di base sulle reti di computer, sui principali protocolli TCP/IP, sui sistemi operativi e sui linguaggi di programmazione.