

Sicurezza Informatica a 360 gradi

Programma del corso

1. Introduzione alla sicurezza delle informazioni

- a) Sicurezza tecnica ed organizzativa
- b) Politiche, ruoli, responsabilità e rischi
- c) Sicurezza e fiducia
- d) minacce, vulnerabilità e protezione

2. Codice Maligno

- a) Programmi
- b) GUI
- c) Tipi di file
- d) codice maligno e tecniche di attacco
- e) principali difese per l'utente di personal computer
- f) Tipi di codice maligno: virus, worm ecc.
- g) anti-virus

3. Crittografia

- a) confidenzialità, autenticità, integrità
- b) principi ed ingredienti
- c) cifrario di Cesare e One-Time-Pad
- d) principio di Kerchoff
- e) tipi di algoritmi
- f) algoritmi simmetrici
- g) algoritmi a-simmetrici (RSA)
- h) algoritmi di hash
- i) MAC e H-MAC
- j) uso degli algoritmi crittografici

4. Autenticazione e controllo degli accessi

- a) identificazione, autenticazione, autorizzazione

- b) password, chiavi, biometria
 - c) autenticazione in rete
5. Infrastrutture a chiavi pubbliche (PKI)
- a) Certification Authority e Registration Authority
 - b) LDAP e X.500
 - c) Web of trust
6. Network security
- a) Firewall e difesa perimetrale
 - b) architetture di firewall
 - c) Proxy e Application Layer Gateway
 - d) Intrusion Detection System e Intrusion Prevention System
 - e) servizi di rete locale e internet
 - f) wireless
 - g) principali attacchi in rete
7. Disponibilità dei dati e delle risorse
- a) disponibilità e resilienza
 - b) business continuity e disaster recovery
 - c) infrastrutture hardware e gestione dei sistemi
 - d) duplicazione, backup e conservazione dei dati