Sicurezza Informatica

Con l'evolversi tecnologico, il ruolo della sicurezza informatica in ambito privato e lavorativo ricopre sempre più un ruolo principale nell'individuazione dei pericoli e delle contromisure da adottare in caso di compromissione di dati e sistemi. Se si considera che oltre l'80% dei problemi di sicurezza ha origine proprio all'interno delle organizzazioni e che spesso dipendono da un utilizzo poco consapevole degli strumenti informatici, è facile capire come tecniche e sistemi di protezione aziendali da soli non possono bastare a contenere fenomeni di compromissione di dati e sistemi.

- **Introduzione alla Sicurezza Informatica**

  La tecnologia che ci circonda esige per motivi di privacy e di mantenimento di dati ed informazioni di dotarsi di sistemi per proteggere tali esigenze.

- **Costi della sicurezza**

  Quanto costa non adottare politiche di sicurezza, e quali sono i costi che ne condizionano l'adozione.

- **Analisi dei rischi**

  L'analisi per individuare i punti critici o di ridotta robustezza dell'infrastruttura informatica.

- **Politiche di sicurezza**

  Politiche ed approcci da adottare per proteggersi da eventuali danni.

- **Minacce / Vulnerabilità**

  Chi è interessato a compromettere i dati, come agisce. Quali sono i punti deboli dei sistemi interconnessi.

- **Sistemi di sicurezza**

  Strumenti perimetrali di difesa quali firewall e proxy, sistemi di prevenzione quali IDS/IPS, segmentazione reti e sistemi di autenticazione per gli accessi alla rete.

- **Framework nazionale di Cyber Security**

  E' il primo documento italiano che definisce la metodologia che un'azienda può seguire per rendere più sicura la sua infrastruttura informatica.

Le Insidie della Rete

Il corso tratta tutta una serie di problematiche di pericoli nascosti in cui è sempre più possibile cadere utilizzando i molteplici strumenti informatici a disposizione nella vita di tutti i giorni che utilizzano la rete per comunicare e diffondere informazioni.

Casi di frodi on line, furti di identità, violazione account e raggiri effettuati con tecniche di social engineering.

- **Introduzione alle insidie**

  In un mondo digitale interconnesso è sempre più facile cadere vittima di truffe e raggiri nonché di vedere qualcun altro che agisce a nostro nome ed utilizza i nostri dati.

- **Malware**

  Spesso derubricati come virus, per capire come agiscono ed i veri pericoli che nascondono a seconda delle tipologie.

- **Programmi Peer to Peer**

  Utilizzati per scaricare file ma che nascondono moltissimi pericoli soprattutto per la diffusione del materiale scaricato.

- **Violazione account**

  Chi è interessato e come avvengono le violazioni di account di posta, social network, smarthphone etc.

- **Furto password**

  Metodi utilizzati per il furto delle password per poi violare ed utilizzare a scopi illeciti identità digitali.

- **Social Engineering**

  Lo studio dei comportamenti individuali di un individuo al fine di ottenere informazioni che poi vengono utilizzate per poterla attaccare. Sono tecniche che tendono a sfruttare le debolezze di una persona per poterla poi trarre in inganno.