Cybersecurity. Sicurezza reti informatiche

Elementi di sicurezza delle reti informatiche

Attestato rilasciato: Validazione delle competenze

Obiettivi:

Furto di dati? Aggressioni Hacker?

È difficile difendere la nostra privacy con tutti questi rischi!

Negli ultimi anni si sono moltiplicati e specializzati tanto gli apparati e sistemi informatici quanto i paralleli attaccanti o cracker. Proprio per questo la **sicurezza informatica** è un problema molto sentito, laddove i rischi di base sono il **furto di informazioni e l'infezione da parte di Virus**: si apre così la sfida alla difesa di cittadini, aziende e sistema Paese.

Diventa un gendarme della sicurezza reti!

Il nostro corso di **Elementi di sicurezza delle reti informatiche** intende fornire ai partecipanti i principi e le tecniche fondamentali per garantire la sicurezza dei sistemi operativi. Affrontando gli aspetti tecnici relativi alle strategie di sicurezza informatica.

Pre-requisiti: conoscenza delle tecniche di gestione di reti informatiche, in particolare delle funzionalità tipiche degli apparati di rete, della loro configurazione, e dei protocolli che li governano.

In osservanza delle prescrizioni regionali, il corso potrà essere erogato anche o esclusivamente

in modalità a distanza. L'eventuale erogazione in presenza sarà effettuata nella Sede di via Bologna, 78 - Torino.

[Attività co-finanziate, con risorse POR FSE 2014-2020, nell'ambito della Direttiva regionale relativa alla formazione continua dei lavoratori occupati - periodo 2019–2021 approvata dalla Giunta Regionale del Piemonte con Deliberazione n. 15-8879 del 6/05/2019, prorogata con D.G.R. n. 18-4252 del 3/12/2021 e DD nr. 50 del 01/02/2022].

Attenzione: il bando di Formazione Continua prevede l'assegnazione di voucher formativi a tutti i lavoratori domiciliati in Piemonte e aziende/liberi professionisti con almeno sede locale in Piemonte. Come da comunicazioni precedenti, tale bando è scaduto il 18/11/2022. Non essendo più possibile richiedere co-finanziamenti, l'unica modalità di accesso al corso prevede iscrizione con quota a prezzo pieno per tutte le tipologie di destinatari (costo sepcificato sotto nella sezione 'destinatari').

Programma didattico

Proteggere client e server dai possibili attacchi informatici

- Installare software e tool per il monitoraggio delle risorse
- Creare sistemi di gestione e monitoraggio degli utenti
- Attivare i sistemi di crittografia per la comunicazione e lo stoccaggio dei dati
- Configurare la sicurezza dei più diffusi servizi di rete sui server

Pericoli di sicurezza per le risorse informatiche

- Principi di sicurezza e metodologie
- Organizzazioni di sicurezza informatica Virus, Worms e Trojan Horses
- Metodologie di attacco Protezione dagli attacchi

Sistemi di monitoraggio secondo il metodo AAA

- I sistemi di Authentication, Authorization and Accounting
- Monitoraggio dell'accesso degli utenti
- Prevenzione degli accessi non autorizzati
- Protezione da connessioni di host e dispositive non autorizzati

- Segnalazione delle anomalie

Sistemi crittografici

- Tunnel sicuri con le VPN attraverso le reti ed internet
- I certificati digitali
- I sistemi di backup centralizzati
- La crittografia dei dati

Creare e gestire una infrastruttura di rete sicura

- Implementare la sicurezza sugli accessi locali delle reti LAN
- Configurare le protezioni degli apparati di rete
- Installare e configurare i firewall
- Installare e configurare i tunnel VPN

Protezione delle risorse di rete

- Protezione degli switch di L2 e L3
- Protezione dei router
- Protezione degli Access-Point Standard IEEE 802.1x

Sistemi firewall

- Monitoraggio e blocco del traffico di rete Sistemi IDS e sistemi IPS
- Controllo antivirus sul traffico
- Supervisione degli accessi remoti

Gestire la sicurezza delle risorse informatiche

- Approfondire le tematiche legate alla sicurezza dei dispositivi e dei servizi
- Pianificare la messa in sicurezza delle risorse
- Predisporre le procedure per l'aggiornamento e la configurazione dell'infrastruttura
- Valutare i potenziali rischi e implementare le procedure di protezione
- Ottimizzare le prestazioni dei sistemi crittografici
- Documentare l'infrastruttura ed i servizi di rete

Verifica finale

Requisiti, modalità di accesso, posti disponibili

Destinatari:
Titolo di studio richiesto: Scuola secondaria II grado / diploma professionale Qualifica
Modalità di accesso: ordine d'arrivo
Limite posti: 16

Date, orari, durata, sede di svolgimento:

Orario: 19:00-22:00 (2 gg a settimana)
Ore totali del corso: 60
Ore stage: 0
Inizio corso: Gennaio 2023
Fine iscrizione: 20/01/2023
Sede: Piattaforma online

Costo: €0,00 - €198,00...

Stato: A pagamento