

Guida alla Cybersecurity: Manuale pratico di Sicurezza Informatica



Questa guida si propone di fornire una panoramica dettagliata sulla Cybersecurity, ovvero sulla Sicurezza Informatica.

Valutazione: Nessuna valutazione

Prezzo

Prezzo base, tasse incluse 27,50 €

Prezzo di vendita 13,75 €

Prezzo di vendita, tasse escluse 13,75 €

Sconto -13,75 €

Ammontare IVA

7 giorni



[Fai una domanda su questo prodotto](#)

Descrizione

Questa guida si propone di fornire una panoramica dettagliata sulla Cybersecurity, ovvero sulla Sicurezza Informatica. La spiegazione degli argomenti va oltre una semplice guida introduttiva, proponendo le informazioni in ordine logico e progressivo per difficoltà, in modo che possano essere comprese anche dai non addetti ai lavori.

Tecnici, analisti, sistemisti, amministratori, hacker, Security manager, Data Protection Officer, e in pratica tutti coloro che per lavoro o per diletto si occupano di Cybersecurity, troveranno in questo testo un riferimento utile e pratico, corredato da esercizi e link di approfondimento, nonché considerazioni di carattere legale.

Argomenti principali

Capitolo 1 - Principi di base

1.1 Aspetti fondamentali della sicurezza

1.2 Pianificare soluzioni di disaster recovery e business continuity

1.3 Crittologia e cifratura (crittografia)

- 1.4 Principi di crittografia per la confidenzialità, l'integrità e l'autenticazione
- 1.5 Firma digitale
- 1.6 Il protocollo SSL e le smartcard

Capitolo 2 - Autenticazione, disponibilità e controllo di accesso

- 2.1 Schemi di autenticazione
- 2.2 Controllo di accesso
- 2.3 Requisiti per la disponibilità dei dati

Capitolo 3 - Codice maligno

- 3.1 Metodi per eseguire comandi e per infettare i computer
- 3.2 Come difendersi da adware e spyware
- 3.3 Categorie di codice virale
- 3.4 Antivirus

Capitolo 4 - Infrastruttura a chiave pubblica

- 4.1 Componenti principali dell'infrastruttura a chiave pubblica

Capitolo 5 - Sicurezza di rete

- 5.1 Tipologie di attacco
- 5.2 Sicurezza nelle reti wireless
- 5.3 Gestione e controllo dei servizi
- 5.4 Rischi e vulnerabilità nei protocolli e nei programmi
- 5.5 Rilevamento di informazioni utili per la sicurezza
- 5.6 Accesso a siti Web e reti private
- 5.7 Contraffazione dei messaggi di posta elettronica
- 5.8 Spam e contromisure

Capitolo 6 – Firewall

- 6.1 Firewall e loro caratteristiche
- 6.2 La zona demilitarizzata (DMZ)
- 6.3 Proxy
- 6.4 Firewall IP e firewall proxy

Capitolo 7 - Aspetti sociali, etici, legali

- 7.1 Concetti legati alla privacy
- 7.2 La protezione dei dati personali
- 7.3 Problematiche etiche legate al tracciamento sui luoghi di lavoro
- 7.4 Crimini informatici e contromisure
- 7.5 Aspetti tecnici e legali relativi alla protezione dei dati personali

Volume di 219 pagine con copertina flessibile (codice isbn 9788828855101)

A cura di: Riccardo Cervelli

Editore: Amazon self publishing (2024)

Recensioni

Nessuna recensione disponibile per questo prodotto.