Zapewnienie bezpieczeństwa systemu informatycznego jest dziś nie lada wyzwaniem. Między administratorami a napastnikami trwa ciągły wyścig zbrojeń. Agresorzy dysponują bardzo różnymi narzędziami i często postępują w sposób nieprzewidywalny. W efekcie każde zabezpieczenie usługi czy zasobu, mimo że początkowo wydaje się doskonałe, prędzej czy później okazuje się podatne na ataki. Jedyną rzeczą, jaką może zrobić **administrator bezpieczeństwa systemu**, jest ciągłe utrzymywanie stanu gotowości, a także odpowiednio wczesne wykrywanie prób ataku i sukcesywne ich neutralizowanie. Poza tym powinien cały czas się uczyć i aktualizować swoją wiedzę.

Ta książka to kolejne, zaktualizowane i uzupełnione wydanie znakomitego podręcznika przeznaczonego dla projektantów systemów i administratorów bezpieczeństwa. Poruszono w niej zagadnienia określania zagrożeń systemów komputerowych i sieci, oceny względnego ryzyka tych zagrożeń i opracowywania efektywnych kosztowo i przyjaznych dla użytkownika środków zaradczych. Wyjaśniono także najważniejsze zasady utrzymywania bezpieczeństwa systemu i wskazano, dlaczego ich przestrzeganie ma kluczowe znaczenie. Zaprezentowano również metody projektowe pozwalające na zaspokojenie wymagań bezpieczeństwa komputerowego, szeroko omówiono ważniejsze standardy w tej dziedzinie, a poszczególne kwestie zilustrowano za pomocą praktycznych przykładów.

Najciekawsze zagadnienia:

- Zasady bezpieczeństwa i ich wdrożenie
- Bezpieczeństwo oprogramowania i infrastruktury
- Elementy kryptografii
- Praca administratora bezpieczeństwa
- Zapewnienie bezpiecznej pracy sieci

Cyberobrona: bądź czujny i przygotuj się!

Spis treści