Chyba każda sieć komputerowa na świecie była już atakowana przez hakerów. Niektóre z ataków były skuteczne, inne nie. Efekty skutecznego ataku hakerów mogą być różne -- od braku szkód, aż po utratę ważnych danych lub, co często okazuje się znacznie gorsze -- wydostanie się takich danych na zewnątrz. Co sprawia, że niektóre sieci opierają się atakom hakerów, a inne nie? Sekret tkwi w zabezpieczeniach i pracy administratora.

W książce "101 zabezpieczeń przed atakami w sieci komputerowej" każdy, kto chce zabezpieczyć swoją sieć przed niepowołanym dostępem, znajdzie niezbędną do tego wiedzę. Książka przedstawia różne rodzaje ataków, sposoby ich wykrywania i metody ochrony sieci przed nimi. Opisuje ataki na różne warstwy i elementy sieci oraz zasady korzystania z zapór sieciowych.

- Wykrywanie sniffingu i ochrona przed nim
- Skanowanie portów i IP-spoofing
- Ataki typu DoS
- Wirusy, robaki i programy szpiegujące
- Zabezpieczanie procesu logowania
- Ochrona przed atakiem przez przepełnienie bufora
- Technologie i architektury zapór sieciowych
- Systemy wykrywania ataków typu IDS

Jeśli chcesz, aby administrowana przez Ciebie sieć była bezpieczna, skorzystaj ze sposobów przedstawionych w tej książce.