

Bezpieczeństwo Komputerowej w Sieci Gminy. Urzędzie

Wstęp

Rozdział I Bezpieczeństwo

1. Bezpieczeństwo a prawo..... 4
2. Zadania: Co chronimy i w jaki sposób?..... 5
3. Wobec przedstawionych powyższych zagadnień co jest naszym zadaniem?..... 6
4. Motywy działania cyberprzestępców i ich rodzaje..... 6

Rozdział II Zabezpieczenia

1. Ochrona a włamanie – koszty..... 8
2. Rodzaje zabezpieczeń..... 9
3. Klasy zabezpieczeń..... 9

Rozdział III Polityka bezpieczeństwa

1. Polityka bezpieczeństwa w urzędzie – czy jest konieczna?..... 11
2. Audyt a Polityka Bezpieczeństwa Informacji..... 12
3. Proces realizacji i wdrożenia polityki bezpieczeństwa..... 13

Rozdział IV Atak sztuka czy przestępstwo

1. Ataki na systemy i ich rodzaje..... 14

- 2. Przeprowadzenie ataku pasywnego..... 14
- 3. Atak aktywny..... 16
- 4. Atak DNS – spoofing..... 17
- 5. Konie trojańskie..... 17

Rozdział V

Szyfrowanie danych w urzędzie lub instytucjach – potrzebne czy wręcz niezbędne?

- 1. Rodzaje..... 19
- 2. Symetryczne..... 19
- 3. Asymetryczne..... 19

Rozdział VI

Człowiek a bezpieczeństwo w sieci?

- 1. Rola człowieka..... 20
- 2. Obrona..... 21

Podsumowanie..... 23

Literatura

Załącznik