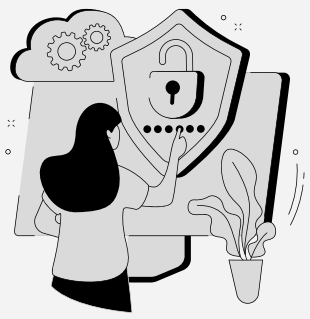
PORADNIK ZABEZPIECZENIA DANYCH

Kluczowe zasady bezpieczeństwa danych w przedsiębiorstwach

1 Zasada 3-2-1



3 kopie danych (oryginał + 2 kopie zapasowe)

2 różne nośniki (np. dysk lokalny + macierz / NAS)

1 kopia poza firmą (offsite) – najlepiej w chmurze

Dlaczego?

To minimalizuje ryzyko utraty danych w przypadku awarii, ataku lub błędu ludzkiego.

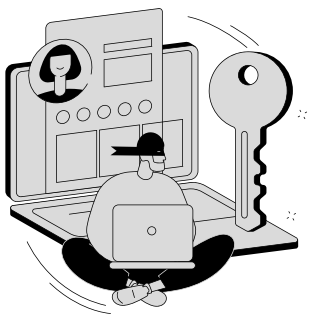
2 Ochrona przed zagrożeniami (insider protection)

Dostęp do backupów powinien być ograniczony tylko do uprawnionych osób

Należy stosować silne hasła i uwierzytelnianie wieloskładnikowe (MFA)

System backupu powinien chronić dane przed usunięciem lub modyfikacją (tzw. hardened repository)

3 Testowanie kopii zapasowych



Backup jest skuteczny tylko wtedy, gdy:

1. Jest wykonywany regularnie (automatycznie)
2. Jest cyklicznie testowany

Brak testów oznacza ryzyko, że w krytycznym momencie danych nie da się odzyskać.

4 Szyfrowanie danych

Backupy powinny być zawsze zaszyfrowane.

Dotyczy to zarówno danych przechowywanych, jak i przesyłanych

Chroni to firmę w przypadku wycieku lub kradzieży danych

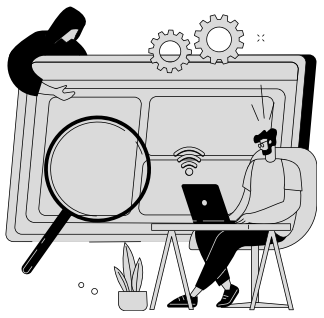
5 Zasada minimalnych uprawnień

Każdy użytkownik powinien mieć dostęp tylko do tych danych i systemów, które są niezbędne do jego pracy

Dlaczego?

1. Ogranicza ryzyko przypadkowego usunięcia danych
2. Minimalizuje skutki ataku (np. przejęcia konta)
3. Zwiększa kontrolę nad systemem

6 Segmentacja sieci



Infrastruktura IT powinna być podzielona na odseparowane części (np. produkcja, backup, dostęp użytkowników)

Korzyści

1. Ograniczenie rozprzestrzeniania się ataku (np. ransomware)
2. Większa kontrola nad ruchem sieciowym

+48 22 335 28 18

www.cloud4you.pl

kontakt@cloud4you.pl