



BEZPIECZEŃSTWO INFORMACJI

Ochrona danych
jako fundament biznesu*

dr Rafał Bartłomiej Panfil

Zakład Bezpieczeństwa Wewnętrznego
Wydział Nauk Technicznych i Społecznych
Państwowa Akademia Nauk Stosowanych
im. Ignacego Mościckiego w Ciechanowie

rafal.panfil@pansim.edu.pl

*funkcjonowania organizacji

PROLOG

Dlaczego bezpieczeństwo informacji jest ważne?

- **Gwarantuje ciągłość działania organizacji**
- Chroni przed utratą danych
- Chroni reputację organizacji
- Zapewnia zgodność z przepisami prawa
- Minimalizuje ryzyko finansowe i prawne
- Wzmacnia zaufanie klientów i partnerów
- i wiele innych



MERITUM

PRZEDMIOT

PERSPEKTYWA

KONTEKST

INFORMACJE

BEZPIECZEŃSTWO

KOMUNIKACJA

ORGANIZACJA



INFORMACJA
ISTOTA I ZNACZENIE

DANE VS. INFORMACJE

PUNKT WYJŚCIA

INFORMACJA

ISTOTA I ZNACZENIE

Źródło: Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*.

Definicja: **Informacja to sygnał, który redukuje niepewność odbiorcy i umożliwia sterowanie systemem.**

SYGNAŁ

INFORMACJA

ISTOTA I ZNACZENIE

Źródło: Bateson, G. (1972). Steps to an Ecology of Mind.

Definicja: **Informacja to coś co czyni różnicę – czyli wszelkie dane, które mają znaczenie i wpływają na odbiorcę.**

ZMIANA

INFORMACJA

ISTOTA I ZNACZENIE

Źródło: Floridi, L. (2010). Information: A Very Short Introduction.

Definicja: **Informacja to dane, które zostały przetworzone i zinterpretowane w kontekście, nadając im znaczenie i użyteczność dla odbiorcy.**

ZNACZENIE

- **Informacje finansowe** – budżety, prognozy, wyniki finansowe, analizy kosztów.
- **Informacje o klientach** – dane kontaktowe, potrzeby, historia zakupów, segmentacja.
- **Informacje o rynku i konkurencji** – analizy trendów, benchmarki, raporty branżowe.
- **Informacje operacyjne** – procedury, procesy, zasoby, harmonogramy (w tym informacje niejawne).
- **Informacje kadrowe** – dane o pracownikach, struktura organizacyjna, kompetencje (w tym dane osobowe).
- **Własność intelektualna** – know-how, patenty, strategie produktowe, dokumentacja techniczna.
- **Informacje prawne i zgodności** – umowy, licencje, regulaminy, polityki zgodności.
- **Informacje strategiczne** – misja, wizja, cele długoterminowe, plany rozwoju
- I wiele innych.



**INFORMACJE, KTÓRE MAJĄ
STRATEGICZNE ZNACZENIE DLA
FUNKCJONOWANIA ORGANIZACJI**

BEZPIECZEŃSTWO jako perspektywa

- jako stan świadomości
- jako potrzeba
- jako wartość
- jak prawo
- jako konieczność

STAN VS. PROCES

PESYMIZM VS. OPTYMIZM

RYZYKA & ZAGROŻENIA

INFORMACJA

jako fundament komunikacji

- Komunikacja jako transfer informacji
- Komunikacja jako transfer znaczeń
- Komunikacja jak wywieranie wpływu
- Komunikacja jak proces psychospołecznego tworzenia rzeczywistości



KOMUNIKACJA

jako fundament organizacji

- **Sprawny przepływ informacji** – umożliwia szybkie podejmowanie decyzji.
- **Zrozumienie celów i zadań** – wspiera realizację strategii organizacji.
- **Budowanie współpracy i relacji** – między zespołami, działami i pracownikami.
- **Unikanie błędów i konfliktów** – dzięki jasnym i precyzyjnym przekazom.
- **Bezpieczna wymiana informacji** – chroni dane przed nieuprawnionym dostępem.
- **Kultura organizacyjna** – komunikacja kształtuje wartości i atmosferę pracy.
- **Reakcja na kryzysy** – dobra komunikacja ułatwia zarządzanie sytuacjami kryzysowymi.



INFORMACJA JAKO KLUCZOWY ZASÓB ORGANIZACJI

- **Wartość strategiczna** – informacja wspiera planowanie, decyzje i rozwój.
- **Zarządzanie informacją** – konieczność porządkowania, klasyfikacji i kontroli dostępu.
- **Poufność i integralność** – ochrona informacji przed nieautoryzowanym dostępem i manipulacją.
- **Cykl życia informacji** – tworzenie, przechowywanie, udostępnianie, archiwizacja, usuwanie.
- **Zgodność z regulacjami** – informacje muszą być przetwarzane zgodnie z prawem (np. RODO).
- **Wrażliwość informacji** – niektóre dane (np. osobowe, finansowe) wymagają szczególnej ochrony.
- **Źródło przewagi konkurencyjnej** – unikalna wiedza i dane wspierają innowacyjność.
- **Ryzyko utraty lub ujawnienia** – konsekwencje dla organizacji mogą być poważne (wizerunkowe, finansowe, prawne).



BEZPIECZEŃSTWO INFORMACJI

KRÓTKIE PODSUMOWANIE

Triada CIA:

- Poufność (Confidentiality)
- Integralność (Integrity)
- Dostępność (Availability)

Zarządzanie ryzykiem:

- Identyfikacja zagrożeń.
- Analiza ryzyka i ocena podatności.
- Planowanie ciągłości działania

**Najsłabsze
ogniwo?**

Środki ochrony informacji:

- Techniczne: środki fizyczne, szyfrowanie, backupy, firewalle, kontrola dostępu.
- Organizacyjne: polityki bezpieczeństwa, procedury reagowania na incydenty.
- Fizyczne: zabezpieczenia biura, dostęp fizyczny do danych.

Dziękuję za uwagę

dr Rafał Bartłomiej Panfil
Zakład Bezpieczeństwa Wewnętrznego
Wydział Nauk Technicznych i Społecznych
Państwowa Akademia Nauk Stosowanych
im. Ignacego Mościckiego w Ciechanowie



www.pansim.edu.pl



tel./fax: (23) 654 98 08



ul. Warszawska 52, 06-500 Mława

