# Kryptografia i bezpieczeństwo danych - bezpieczeństwo informacji wprowadzenie

Sławomir Samolej
ssamolej.kia.prz.edu.pl
ssamolej@prz.edu.pl

# Bezpieczeństwo - definicja

- **Bezpieczeństwo** to ochrona czyichś zasobów przed:
  - Atakami na sieci komputerowe
  - Klęskami żywiołowymi
  - Wandalizmem
  - Utratą
  - Nadużyciem
- Należałoby podjąć próbę zabezpieczenia przed najbardziej prawdopodobnymi formami ataku i w najlepszym zakresie, przy uwzględnieniu środowiska w jakim ktoś się znajduje.

# Definicja

- **Bezpieczeństwo informacji** to:
  - Ochrona informacji i systemów informatycznych przed nieautoryzowanym
    - dostępem,
    - wykorzystaniem,
    - ujawnieniem,
    - zakłóceniem,
    - modyfikacją
    - zniszczeniem.

# Bezpieczeństwo - produktywność

„ Jedyny naprawdę bezpieczny system to taki, który jest odłączony od zasilania, zalany w bloku betonu i zamknięty w wyłożonym ołowiem pokoju patrolowanym przez uzbrojonych strażników – ale nawet w takiej sytuacji mam pewne wątpliwości.”

Prof. Eugene Spafford

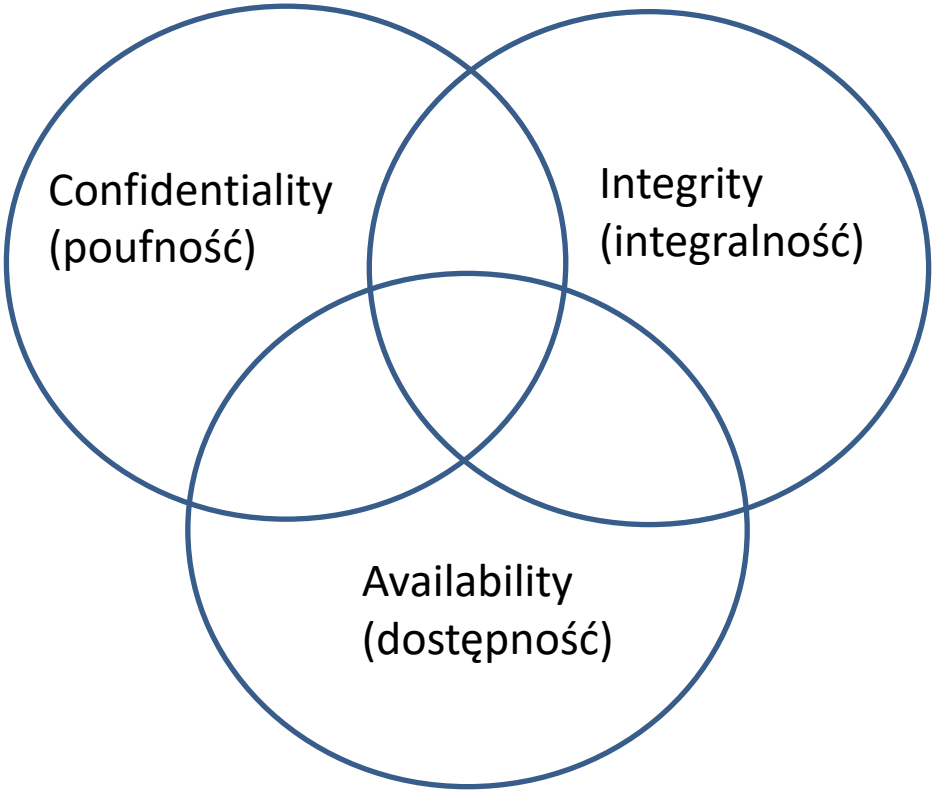
Zwiększenie poziomu bezpieczeństwa

->

obniżenie poziomu produktywności.

# Triada CIA

- Jeden z modeli rzeczywistości pozwalający opisać rzeczywistość z punktu widzenia bezpieczeństwa
- Pomaga w opisywaniu ataków




Odwrotnie: Disclosure/Alteration/Denial
(ujawnianie/zmiana/odmowa)

# Poufoność

- Zdolność do ochrony danych przed osobami, które nie są upoważnione do ich przeglądania

# Integralność

- Zdolność do zapobiegania zamianom danych w nieuprawniony lub niepożądany sposób.
  - Zapobieganie zamianom
  - Wykrywanie zmian
  - Możliwość cofnięcia zmian

# Dostępność

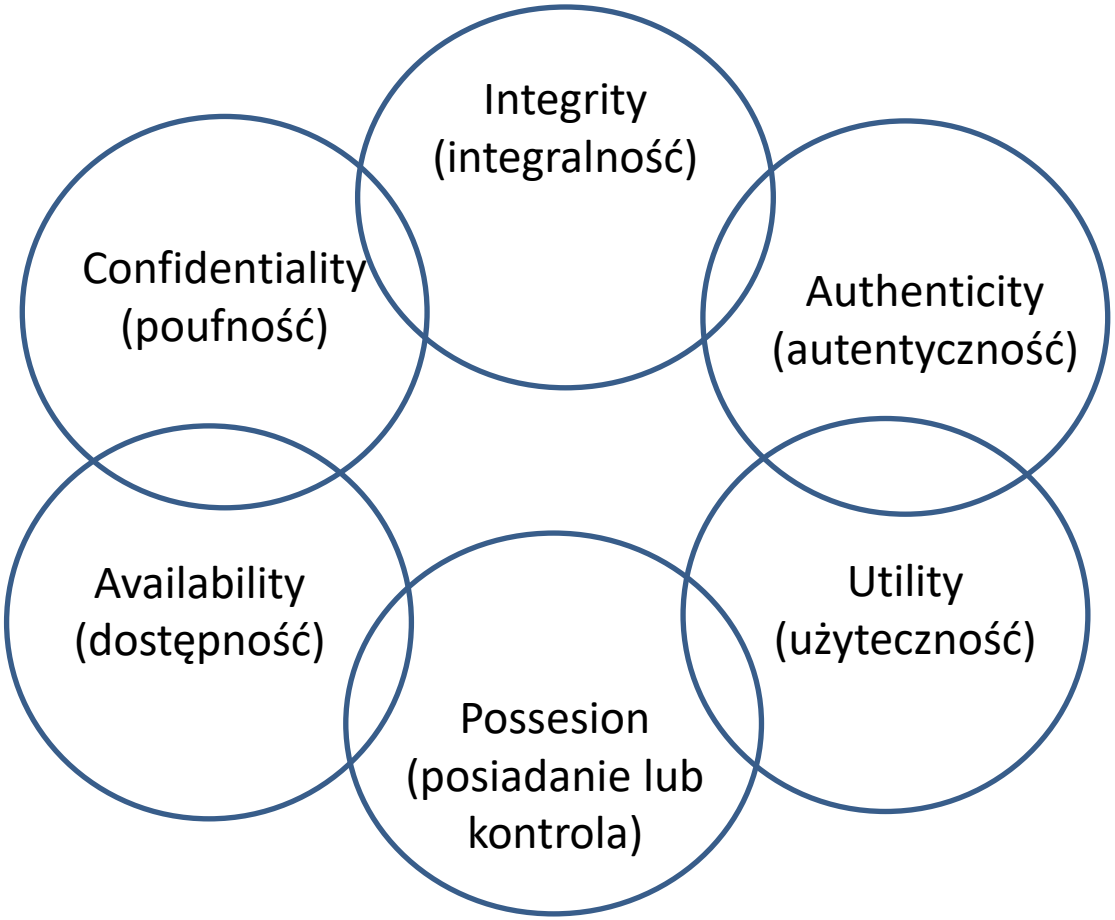
- Możliwość dostępu do Twoich danych, gdy ich potrzebujesz.
  - Awaria zasilania?
  - Uszkodzenie SO
  - Atak DoS

# Odniesienie do bezpieczeństwa - przykład

- Przykład: transport niezaszyfrowanych dysków z jedynymi kopiami danych ginie podczas przejazdu.
  - Powstaje incydent bezpieczeństwa:
    - Naruszenie poufności (pliki były niezaszyfrowane)
    - Naruszenie integralności (nie wiemy, czy zostały zmodyfikowane)
    - Naruszenie dostępności (nie mieliśmy dostępu do tej informacji)

# Heksada Parkera

- Rozszerzony model rzeczywistości do opisu bezpieczeństwa
- Pomaga w opisywaniu ataków



# Posiadanie lub sprawowanie kontroli

- Fizyczne dysponowanie nośnikiem, na którym przechowywanie są dane.
  - Można opisać utratę danych przechowywanych na danym fizycznym nośniku, bez angażowania innych czynników, takich jak dostępność
  - Jeśli w poprzednim przypadku część dysków byłoby zaszyfrowanych, to incydent można zdefiniować jako problem z posiadaniem, ale nie z poufnością

# Autentyczność

- Pozwala stwierdzić, czy dane zostały przypisane do odpowiedniego właściciela lub twórcy.
  - Podpisy elektroniczne?

# Użyteczność

- W jakim stopniu dane są użyteczne dla użytkownika
  - Zaszyfrowane dyski dla napastnika są mało użyteczne, ale te niezaszyfrowane bardzo…

# Rodzaje ataków

- **Przechwycenie**
  (interception)
- **Przerywanie**
  (interruption)
- **Modyfikowanie**
  (modification)
- **Podrabianie**
  (fabrication)

| | |
|---|---|
| C | Przechwycenie |
| I | Przerywanie<br>Modyfikowanie<br>Podrabianie |
| A | Przerywanie<br>Modyfikowanie<br>Podrabianie |

# Przechwycenie

- Umożliwienie nieautoryzowanym użytkownikom dostępu do danych, aplikacji lub środowiska celu.
- Są atakami przeciw poufności.
- Przykłady:
  - Nieautoryzowane przeglądanie lub kopiowanie plików
  - Podsłuchiwanie rozmów telefonicznych
  - Czytanie cudzych emaili
- Można je przeprowadzić na:
  - Danych w spoczynku
  - Danych w tranzycie
  - Danych w użyciu

| | |
|---|---|
| C | Przechwycenie |
| I | Przerywanie<br>Modyfikowanie<br>Podrabianie |
| A | Przerywanie<br>Modyfikowanie<br>Podrabianie |

# Przerywanie

- Tymczasowe lub stałe zniszczenie lub zablokowane dostępu do zasobów
- Wpływają na:
  - Dostępność
  - Integralność (jeśli doszło do manipulacji na procesach w bazie danych)

| C | Przechwycenie |
|---|---|
| I | Przerywanie<br>Modyfikowanie<br>Podrabianie |
| A | Przerywanie<br>Modyfikowanie<br>Podrabianie |

# Modyfikacja

- Manipulowanie zasobami
- Atak na:
  - Integralność
  - Dostępność

| | |
|---|---|
| C | Przechwycenie |
| I | Przerywanie<br>Modyfikowanie<br>Podrabianie |
| A | Przerywanie<br>Modyfikowanie<br>Podrabianie |

# Podrabianie

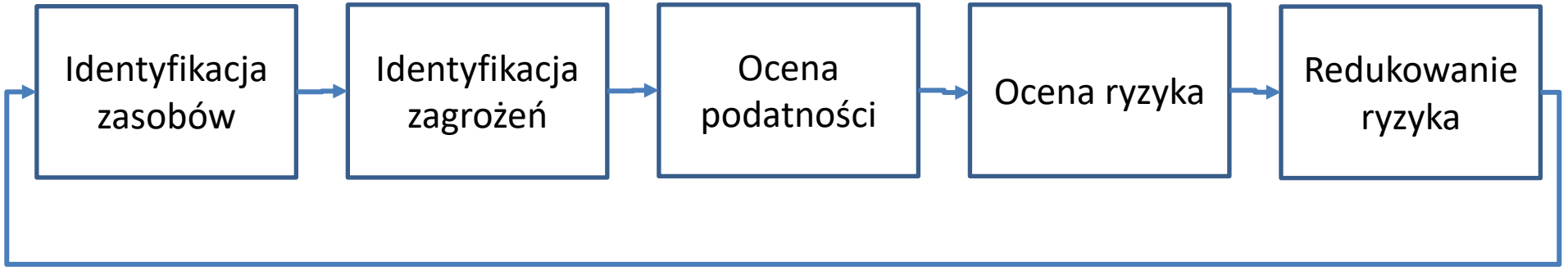
- Generowanie danych, procesów, komunikacji.
- Typ ataku na:
  - Integralność
  - Dostępność

| | |
|---|---|
| C | Przechwycenie |
| I | Przerywanie<br>Modyfikowanie<br>Podrabianie |
| A | Przerywanie<br>Modyfikowanie<br>Podrabianie |

# Zagrożenie, podatność, ryzyko

- **Zagrożenie** – coś, co ma potencjał wyrządzenia szkody.
- **Podatność** – słabe punkty lub luki w zabezpieczeniach, które mogą być wykorzystane do dokonania szkody.
- **Ryzyko** – prawdopodobieństwo, że wydarzy się coś złego.
- **Aby w danym środowisku istniało ryzyko, musi się pojawić zarówno zagrożenie jak i podatność, którą takie zagrożenie może wykorzystać.**

# Zarządzanie ryzykiem



# Identyfikacja zasobów

- Dokonanie inwentaryzacji wykorzystywanych zasobów
  (sprzęt, oprogramowanie, maszyny wirtualne itp…)
- Określenie, które są krytycznymi zasobami biznesowymi (interakcja z użytkownikami)

# Identyfikacja zagrożeń (zastosować triadę CIA lub heksadę Parkera)

- Aplikacja przetwarzająca płatności kartami kredytowymi:
  - **Poufność** – ujawnienie danych o transakcjach podmiotom nieuprawnionym spowoduje incydent niebezpieczeństwa
  - **Integralność** – jeśli dane zostaną uszkodzone, płatności będą przetwarzane w nieprawidłowy sposób
  - **Dostępność** – jeśli system ulegnie awarii, nie będzie można dokonać płatności
  - **Posiadanie** – utrata nośników kopii zapasowych skutkuje potencjalnym incydentem bezpieczeństwa
  - **Autentyczność** – brak poprawnych danych o kliencie może prowadzić do przetwarzania sfałszowanych transakcji
  - **Użyteczność** – jeśli dane zgromadzone będą nieważne lub nieprawidłowe, to ich użyteczność będzie ograniczona

# Ocena podatności 1/2 (zastosować triadę CIA lub heksadę Parkera)

- Aplikacja przetwarzająca płatności kartami kredytowymi:
  - **Poufność** – (ujawnienie danych) U nas: dane są szyfrowane w spoczynku i ruchu, systemy są poddawane regularnym pentestom -> ***to nie jest ryzyko***
  - **Integralność** – (uszkodzenie danych) U nas: w czasie przetwarzania weryfikujemy dane. Nieprawidłowe dane to odrzucenie transakcji -> ***to nie jest ryzyko***
  - **Dostępność** – (brak dostępu do systemu) U nas: nie mamy zaplanowanej nadmiarowości dla bazy danych. Uszkodzenie bazy odbierze nam możliwość przeprowadzania płatności -> ***to jest ryzyko***

# Ocena podatności 2/2 (zastosować triadę CIA lub heksadę Parkera)

- Aplikacja przetwarzająca płatności kartami kredytowymi:
  - **Posiadanie** – (utrata kopii) U nas: nasze nośniki kopii są zaszyfrowane i przekazywane ręcznie przez kuriera -> ***to nie jest ryzyko***
  - **Autentyczność** – (brak prawidłowych danych o kliencie) U nas: zapewnienie, że transakcję kartą rzeczywiście wykonuje dana osoba jest trudne -> ***to jest ryzyko***
  - **Użyteczność** – (nieważność danych) U nas: sprawdzamy sumy kontrolne numerów kart kredytowych, sprawdzamy adresy rozliczeniowe i na wiele innych sposobów sprawdzamy poprawność danych -> ***to nie jest ryzyko***

# Ocena ryzyka

- Aplikacja przetwarzająca płatności kartami kredytowymi:
  - **Dostępność** – (brak dostępu do systemu) U nas: nie mamy zaplanowanej nadmiarowości dla bazy danych. Uszkodzenie bazy odbierze nam możliwość przeprowadzania płatności -> ***to jest ryzyko***

***Jest zagrożenie i odpowiadająca mu  podatność***

# Redukowanie ryzyka

- Wprowadzenie **mechanizmów kontrolnych**:
  - Fizyczne mechanizmy kontrolne
    - Ogrodzenia, bramy, zamki, osłony, kamery,
    - Ogrzewanie i klimatyzacja, gaszenie ognia, rezerwowe generatory mocy
  - Logiczne mechanizmy kontrolne
    - Hasła, szyfrowanie, kontrola dostępu, zapory sieciowe, systemy wykrywania włamań
  - Administracyjne mechanizmy kontrolne
    - Reguły, prawa, polityki, procedury, wytyczne… (trzeba mieć możliwość egzekwowania…)

# Reagowanie na incydenty

- Jeśli nastąpił incydent bezpieczeństwa, należy na niego zareagować
- Reagowanie powinno być przygotowane wcześniej i przeprowadzone według etapów:
  - Przygotowanie
  - Wykrywanie i analiza
  - Ograniczanie
  - Eliminacja
  - Odzyskiwanie
  - Działania po incydencie

# Reagowanie na incydenty - przygotowanie

- Co można zrobić, zanim wystąpi incydent:
  - Tworzenie polityk działania i procedur
  - Prowadzenie szkoleń
  - Opracowywanie i utrzymywanie dokumentacji

# Reagowanie na incydenty – wykrywanie i analiza

- Wykrycie problemu, podjęcie decyzji, czy to jest incydent bezpieczeństwa i rozpoczęcie procedury reagowania
  - Problemy są wykrywane z zastosowaniem narzędzi lub usług bezpieczeństwa
    - Systemy wykrywania włamań, antywirusy, logi serwerów
  - Na pewnym etapie powinien się znaleźć człowiek, który podejmie decyzję, czy sprawa jest incydentem

# Reagowanie na incydenty – ograniczanie, eliminowanie, odzyskiwanie

- Faza rozwiązania incydentu
  - Ograniczanie strat – zapobieżeniu dalszym stratom (np. odłączenie serwera od sieci)
  - Eliminacja – próba usunięcia skutków incydentu
  - Odzyskiwanie – przywrócenie stanu sprzed incydentu

# Reagowanie na incydenty – działania po incydencie

- Analiza zaistniałego incydentu i próba zapobieżenia jego powtórzenia.