Politechnika Wrocławska

CIA Triad

Cyberbezpieczeństwo

Krzysztof Bocian
Anna Płecha
Aneta Prządka

HR EXCELLENCE IN RESEARCH

Bezpieczeństwo Informacji

W rozumieniu telekomunikacji, bezpieczeństwo informacji spełnione jest wtedy, gdy spełnione są:

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

Dodatkowo rozróżniamy takie aspekty, jak:

- autentyczność
- rozliczalność
- niezaprzeczalność
- niezawodność

Nazywane są one funkcjami lub właściwościami bezpieczeństwa.

O bezpieczeństwie informacji możemy mówić na przykład w kontekście dostępu do danych, systemów, sieci, pomieszczeń.

Politechnika
Wrocławska

Poufność

HR EXCELLENCE IN RESEARCH

Poufność

Poufność:

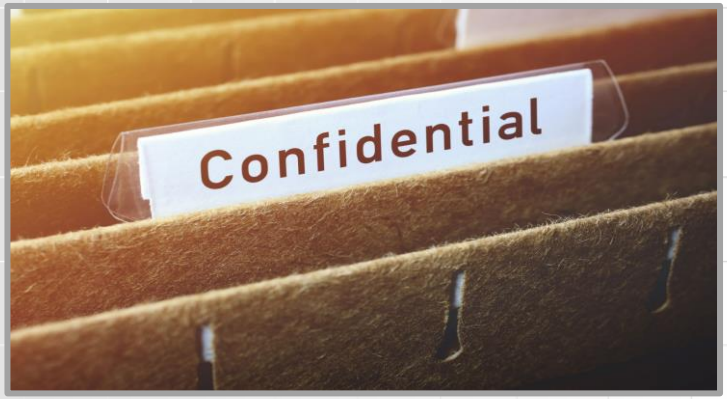
- jedna z trzech podstawowych funkcji bezpieczeństwa;
- zapewnia ochronę przed nieautoryzowanym dostępem do danych poufnych.

W jaki sposób jest zapewniana poufność?

- metody uwierzytelniania;
- kontrola dostępu;
- zasada najmniejszych uprawnień.

Dane poufne:

- NDA
- inne dane mające duże znaczenie dla pracy przedsiębiorstwa, których ujawnienie mogłoby mieć negatywny wpływ.



Źródło: https://btlaw.com/-/media/images/btlaw/content/confidential_detail.ashx?h=1280&w=1920&la=en&hash=5CBA742DB165746722E9693B64CE59BF

Bezpieczeństwo Informacji - metody uwierzytelniania

Poufność rozumiana jako ochrona przed niepowołanym dostępem może być zapewniana poprzez jedną z metod uwierzytelniania:

- coś, co się wie;
- coś, co się posiada;
- coś, czym się jest.

Możliwe zagrożenia:

- złamanie hasła;
- kradzież bądź zgubienie sprzętu fizycznego;
- złamanie słabych zabezpieczeń biometrycznych.

Najbezpieczniejszym rozwiązaniem w tym zakresie jest stosowanie uwierzytelniania wieloskładnikowego.

Bezpieczeństwo Informacji - kontrola dostępu

Poufność może być także zapewniania poprzez systemy kontroli dostępu:

- dostęp do poszczególnych pomieszczeń lub stref regulowany poprzez karty lub hasła dostępowe.

Możliwe zagrożenia:

- kradzież lub zgubienie karty dostępowej;
- złamanie hasła;
- częsty brak dodatkowej weryfikacji w postaci autoryzacji

Bezpieczeństwo Informacji - zasada najmniejszych uprawnień

Dla poufności duże znaczenie powinna mieć zasada najmniejszych uprawnień

- uprawnienia przyznawane są wyłącznie w zakresie koniecznym do realizacji przydzielonych działań;
- aktualność nadanych uprawnień powinna być stale kontrolowana i modyfikowana.

Możliwe zagrożenia:

- pracownik z przyznanymi zbyt dużymi uprawnieniami względem potrzeb wynikających z obowiązków może naruszyć pozostałe funkcje bezpieczeństwa;
- włamanie na konto tzw. pracownika szeregowego z nadmiernymi uprawnieniami może umożliwić nieautoryzowane przejęcie kontroli nad systemem lub aplikacją.

Politechnika
Wrocławska

Integralność

HR EXCELLENCE IN RESEARCH

Politechnika Wrocławska

Definicja

- Jeden z trzech najbardziej podstawowych i kluczowych potrzeb w zakresie Cyberbezpieczeństwa (CIA triad)
- Oznacza pewność, że informacje są wiarygodne i dokładne
- Polega na utrzymaniu spójności, dokładności i wiarygodności danych w całym cyklu ich życia, tzn. należy zapewnić brak możliwości zmian w trakcie ich przesyłu oraz przez osoby nieuprawnione (np. z naruszeniem poufności)

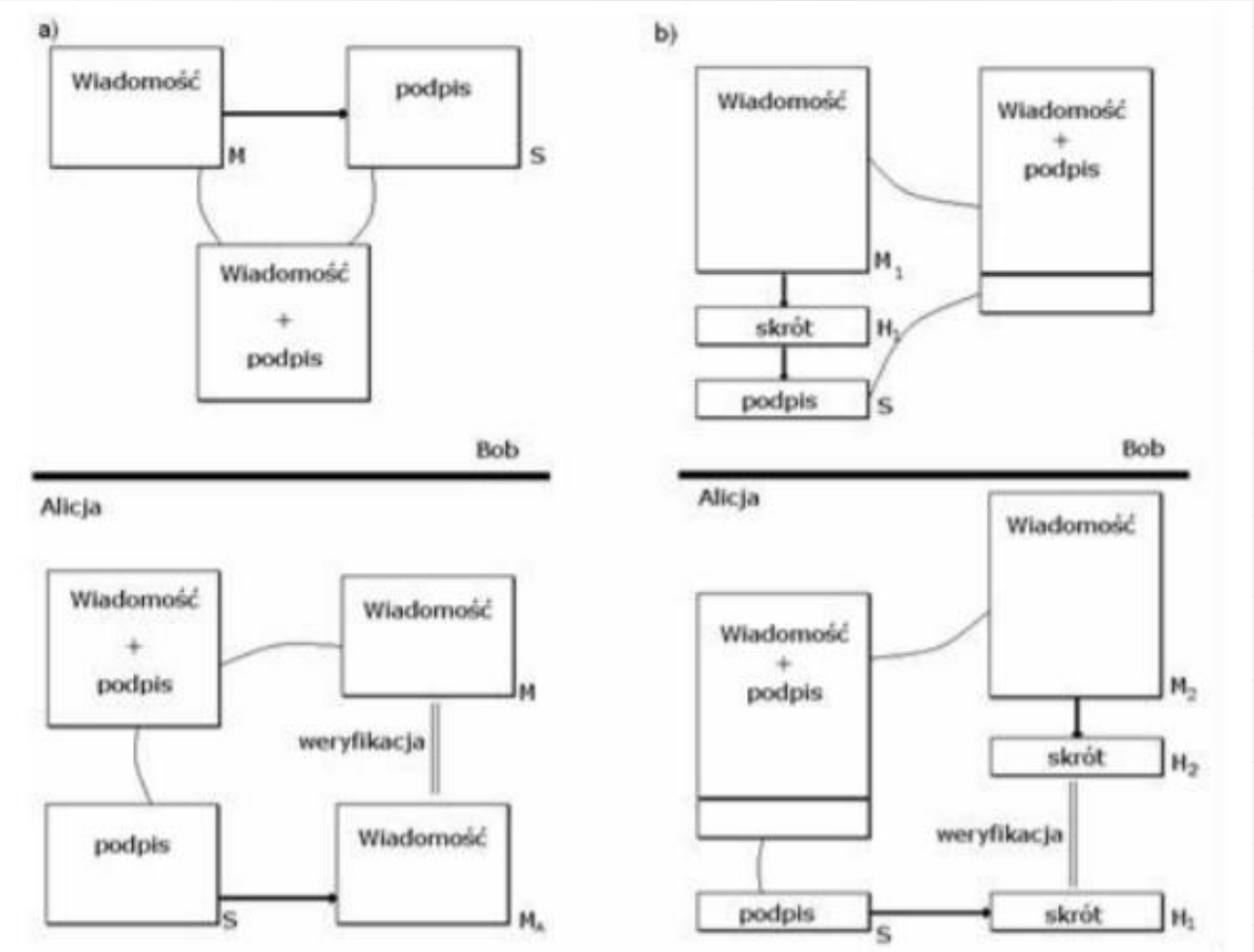
Politechnika Wrocławska

Przykłady wykorzystania integralności

- Szyfrowanie
- Hashowanie
- Podpisy cyfrowe
- Certyfikaty cyfrowe

Klasyfikacja schematów podpisu cyfrowego

Schemat podpisu cyfrowego



Rysunek. Schemat podpisu cyfrowego a) bez wykorzystania funkcji skrótu i b) z użyciem funkcji skrótu.

Zalety i wady podpisu cyfrowego

+ oszczędność czasu i pieniędzy
+ szybkość działania
+ wygoda używania
+ możliwość podpisu dokumentów elektronicznych
+ mniejsza szansa podrobienia
+ łatwość obsługi
+ łatwiejsza weryfikacja wprowadzonych zmian w dokumentach podpisanych

- koszta związane z ilością podpisów elektronicznych
- konieczność stosowania integralnego sprzętu
- brak bezpośredniego powiązania między podpisem, a cechami osobowymi osoby

Politechnika Wrocławska

Rodzaje ataków na schematy podpisów

- Przestępca może obliczyć informacje o kluczu prywatnym osoby podpisującej się kluczem albo znajduje skuteczny algorytm podpisywania funkcjonalnie równoważny prawidłowemu algorytmowi podpisu cyfrowego.
- Przestępca może utworzyć prawidłowy podpis cyfrowy dla określonej wiadomości lub klasy wiadomości wybranych przed atakiem
- Przestępca może sfałszować podpis dla co najmniej jednej wiadomości, a jego kontrola nad wiadomością jest znikoma lub żadna.

Politechnika Wrocławska

Dostępność

HR EXCELLENCE IN RESEARCH

Czym jest dostępność w CIA?

- Dostęp do spójnych informacji dla upoważnionych osób
- Zapewnienie dostępności wiąże się z utrzymaniem sprzętu i infrastruktury technicznej oraz systemów w odpowiednim stanie.

Politechnika Wrocławska

Jak zapewnić dostępność?

- Konserwacja sprzętu
- Utrzymanie prawidłowo działającego środowiska
- Aktualizacje oprogramowania
- Zapewnienie odpowiedniej przepustowości

Politechnika Wrocławska

Najlepsze praktyki wdrażania triady CIA

- Pewność, że pracownicy posiadają wiedze na temat zgodności i wymagań prawnych, aby zminimalizować błędy ludzkie w działaniu systemów
- Używanie oprogramowania do:
- tworzenia kopii zapasowych oraz odzyskiwania kopii zapasowych
- kontroli wersji,
- kontroli dostępu,
- kontroli bezpieczeństwa,
- dzienników danych i sum kontrolnych

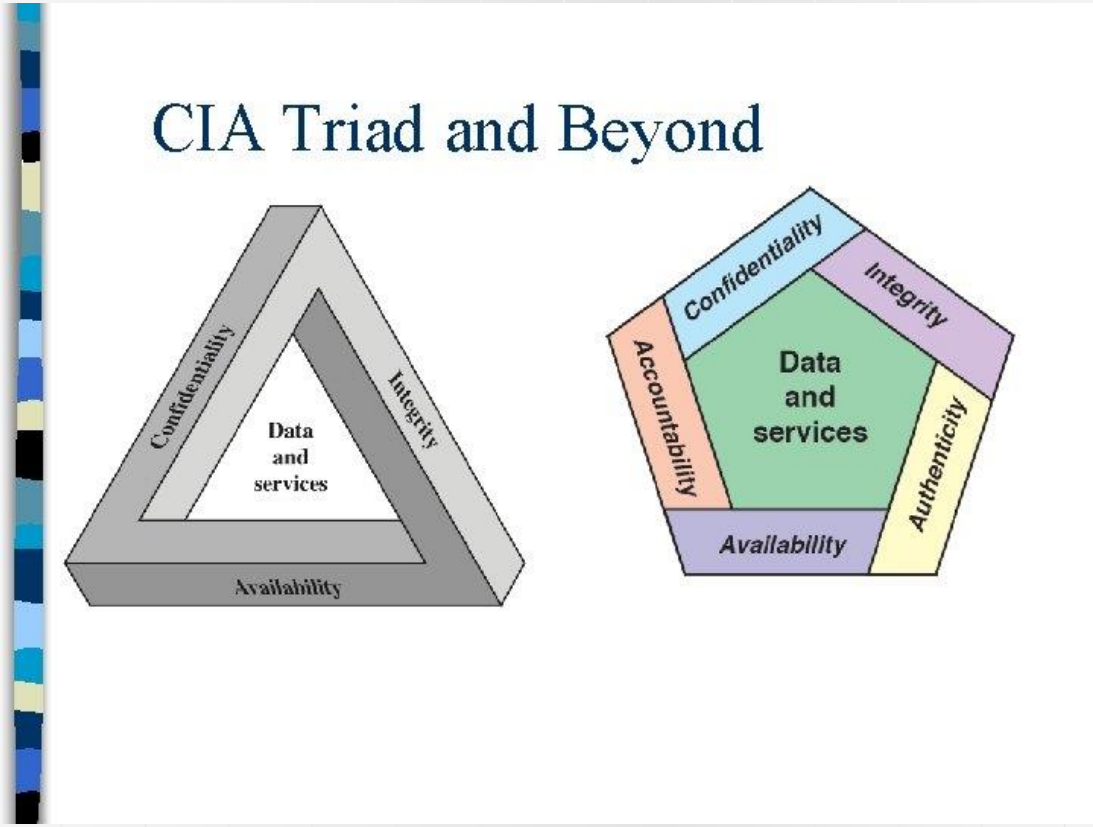
Politechnika
Wrocławska

Rozszerzenie CIA

HR EXCELLENCE IN RESEARCH

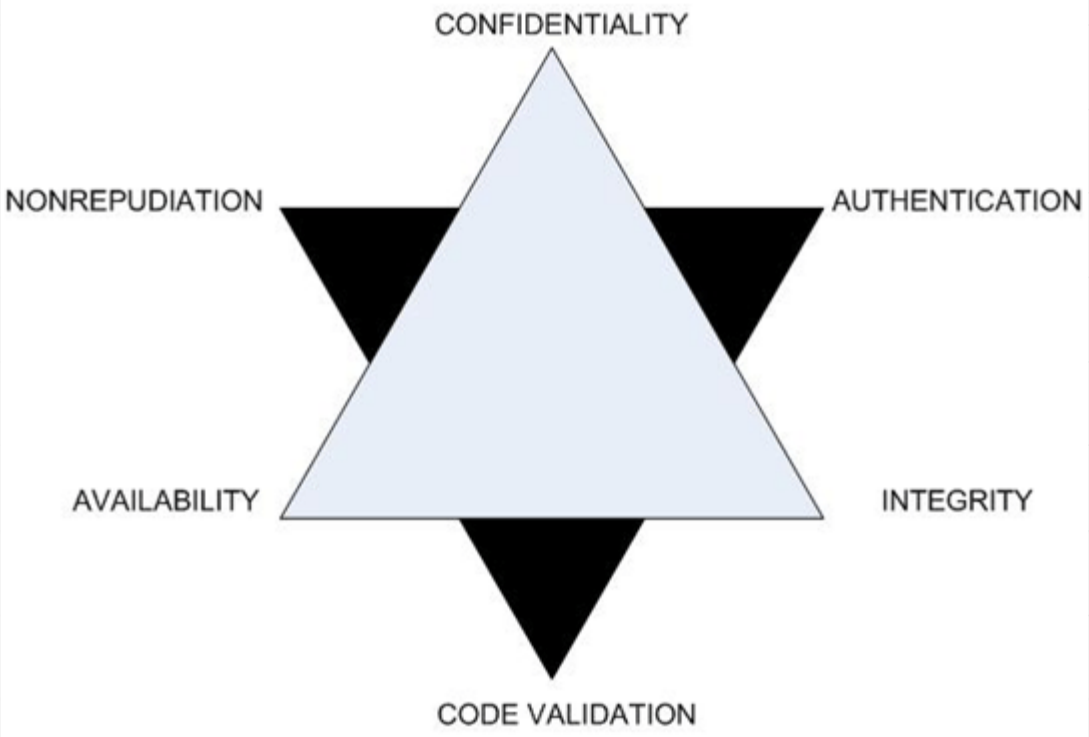
Politechnika Wrocławska

Rozszerzenie CIA



Politechnika Wrocławska

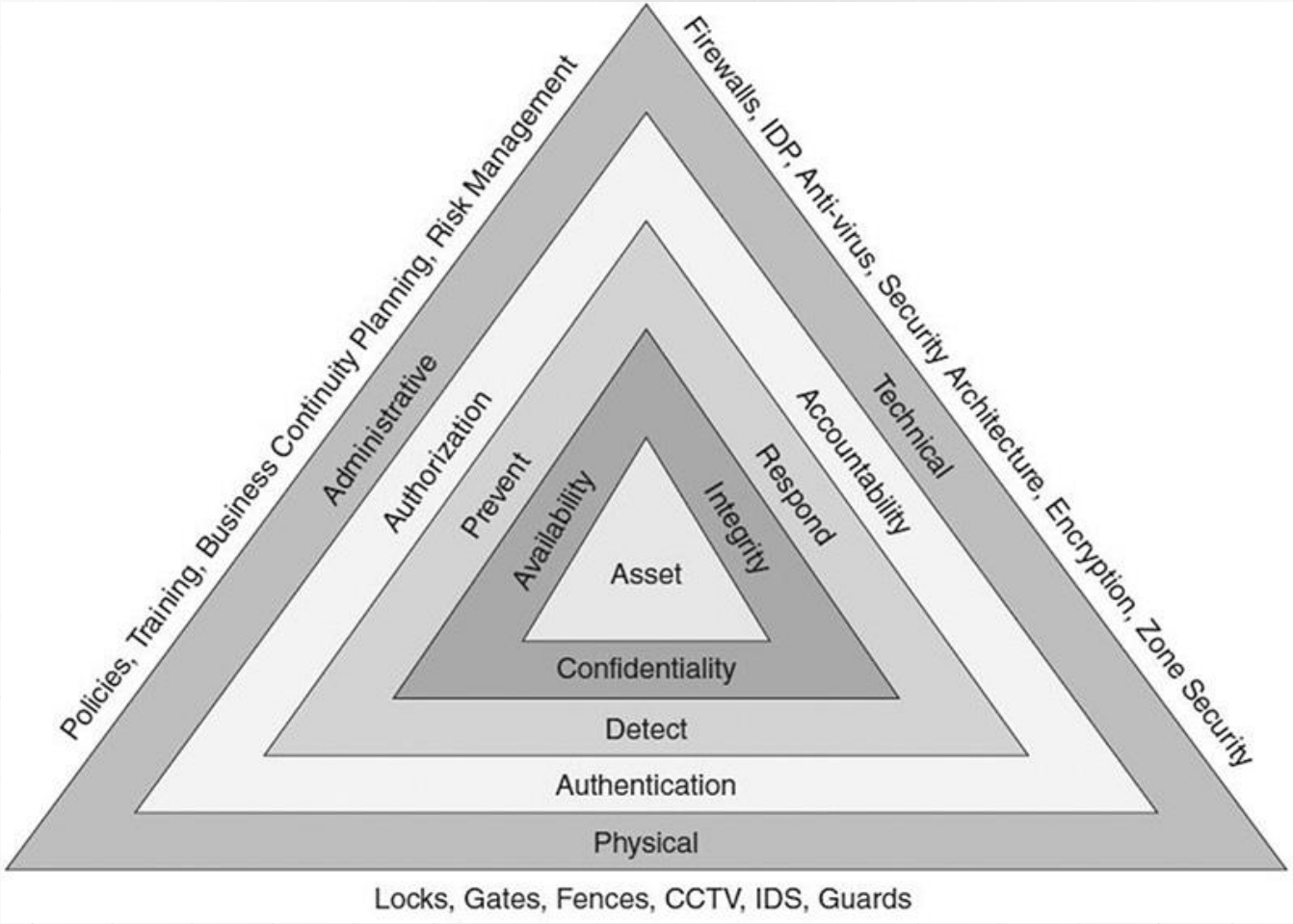
Rozszerzenie CIA



Politechnika Wrocławska

Rozszerzenie CIA

Rozszerzenie CIA



Politechnika Wrocławska

Podsumowanie

- Poufność: Systemy i dane są dostępne tylko dla autoryzowanych użytkowników.
- Integralność: systemy i dane są dokładne i kompletne.
- Dostępność: systemy i dane są dostępne, gdy są potrzebne.

- Ostatecznym celem bezpieczeństwa danych jest zapewnienie poufności, integralności i dostępności danych krytycznych i wrażliwych. Stosowanie zasad triady CIA pomaga organizacjom stworzyć skuteczny program bezpieczeństwa w celu ochrony ich cennych aktywów.

Politechnika Wrocławska

Bibliografia

- https://pl.wikipedia.org/wiki/Kontrola_dostępu
- https://pl.wikipedia.org/wiki/Uwierzytelnianie
- https://pl.wikipedia.org/wiki/Poufność
- https://firma.rp.pl/zarzadzanie/art18864741-nda-jak-zabezpieczyc-sie-przed-wyciekiem-poufnych-danych
- https://en.wikipedia.org/wiki/Information_security#Confidentiality
- http://ii.uwb.edu.pl/rudnicki/wp-content/uploads/2016/02/22.pdf
- https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
- https://home.agh.edu.pl/~meszka/talks/Pawel_Tokarski.pdf
- https://ikmj.com/wady-i-zalety-podpisu-elektronicznego/
- https://slidetodoc.com/cs-432-computer-and-network-security-spring-2017/
- https://informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/
- https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.3_Models_of_Security_-_CIA___Parkerian_Hexad
- https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=2
- http://www.kis.pwszchelm.pl/publikacje/V/Bartyzel.pdf