Podstawowe pojęcia związane z Bezpieczeństwem teleinformatycznym

Podstawowe pojęcia

Teleinformatyka:

- Telekomunikacja

+

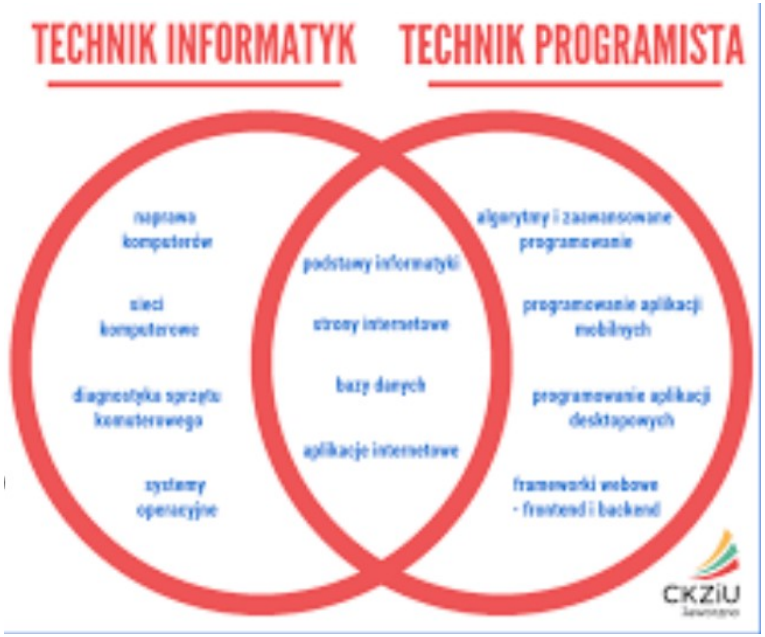
- Informatyka

Podstawowe pojęcia

- informatyk
- programista

Podstawowe pojęcia

- informatyk
- programista



Podstawowe pojęcia

- informatyk
- programista

Podstawowe różnice pomiędzy informatykiem, a programistą	
Informatyk	**Programista**
Żeby zostać informatykiem trzeba skończyć studia informatyczne	Żeby zostać programistą, to nie trzeba kończyć studiów informatycznych, mogą być to studia na kierunku automatyka i robotyka bądź matematyka lub po prostu musisz czuć to coś
Zajmuje się informacją automatyczną, a więc może tworzyć bazy danych lub też inne rzeczy przy pomocy aplikacji napisanych przez programistę	Zajmuje się tworzeniem aplikacji czy też stron internetowych
Informatyk to ogólny zawód, najczęściej zawód kojarzony z informatykiem w gminie lub innym urzędzie☺	Programista jest specjalizacją informatyka

https://candyweb.pl/informatyk-czy-programista-zasadnicze-roznice-i-dlaczego-nie-warto-sie-mylic/

NIE! - Podstawowe pojęcia

U mnie działa:

- maszyna wirtualna
- kontener (ang. docker)

Podstawowe pojęcia

Informatyka (ang. *computer science*):

- teoretyczna (algorytmy, automaty, kodowanie, inf.kwantowa …)
- inżynieria komputerowa (architektura komputerów, sieci komputerowe, systemy operacyjne …)
- praktyczna (grafika komputerowa, kryptologia …)
- systemy i technologie komputerowe (systemy wbudowane, sztuczna inteligencja, technologie webowe …)
- stosowana (biologia, chemia, …)

Podstawowe pojęcia

Bezpieczeństwo teleinformatyczne :

- Danych
- Sieci
- Aplikacji
- Systemu operacyjnego
- Dostępu
- W chmurze
- Internetu Rzeczy

- Bezpieczeństwo danych

- Dokument papierowy
- Dokument elektroniczny:
  - plik
  - rekord
  - koperta
- Pamięć
  - uruchomieniowa: ROM, Flash
  - operacyjna: SDRAM
  - masowa: Dysk „twardy”
  - przenośna: Pendrive, katra pamięci

- Bezpieczeństwo sieci

Bezpieczeństwo sieciowe to kompleksowa ochrona systemów informatycznych i sieci przed nieautoryzowanym dostępem, atakami, awariami, utratą danych i innymi zagrożeniami.

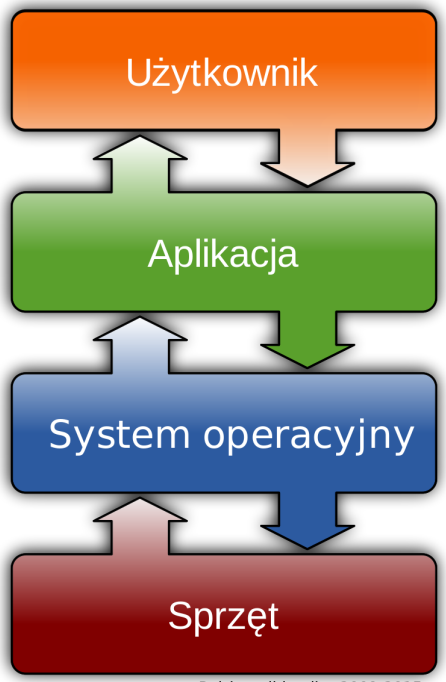
BS to atak na infrastrukturę.

Podstawowe pojęcia

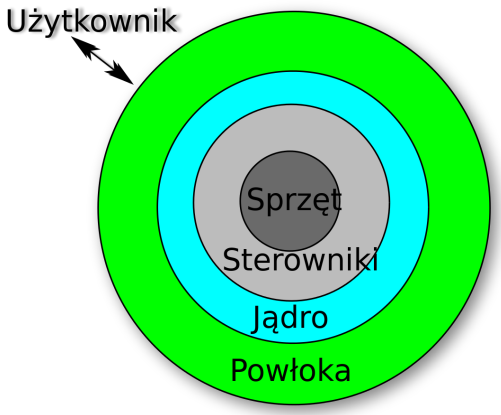
Bezpieczeństwo teleinformatyczne :

- Danych
- Sieci
- Aplikacji
- Systemu operacyjnego
- Dostępu
- W chmurze (BD)
- Internetu Rzeczy (BD)

- Bezpieczeństwo Systemu operacyjnego



Polska wikipedia, 2009-2015



Podstawowe pojęcia

Bezpieczeństwo teleinformatyczne :

- Danych
- Sieci
- Aplikacji
- Systemu operacyjnego
- Dostępu
- W chmurze (BD)
- Internetu Rzeczy (BD)

Podstawowe pojęcia

- Cyberbezpieczeństwo

Gdy nakłamiesz w CV i dostaniesz tą robotę:

Podstawowe pojęcia - mity

- Cyberbezpieczeństwo

Podstawowe pojęcia - fakty

- Cyberbezpieczeństwo

Podstawowe pojęcia

- **Cyberbezpieczeństwo** (ang. cybersecurity) to dziedzina zajmująca się ochroną sieci komputerowych, systemów informatycznych, urządzeń mobilnych i innych podłączonych do sieci urządzeń przed atakami cybernetycznymi, nieautoryzowanym dostępem, kradzieżą danych oraz innymi zagrożeniami związanymi z korzystaniem z **sieci**.

Podstawowe pojęcia

- **Cyberbezpieczeństwo** a **Bezpieczeństwo teleinformatyczne**?

- skupia się na specyficznych zagrożeniach wynikających z działań cyberprzestępców
- ogół działań podejmowanych w celu zapewnienia bezpieczeństwa przetwarzania i przesyłania informacji za pomocą różnych urządzeń i sieci teleinformatycznych

Podstawowe pojęcia

Kryptologia:

- Kryptografia

+

- Kryptoanaliza

Podstawowe pojęcia

Kryptologia:

- Kryptografia – nauka o zabezpieczaniu danych

+

- Kryptoanaliza – nauka o łamaniu mechanizmów kryptograficznych

Podstawowe pojęcia [2]

Kryptologia - wiedza naukowa obejmująca kryptografię i kryptoanalizę.

Kryptografia - dziedzina obejmująca zagadnienia związane z *utajnieniem* danych (w kontekście przesyłania wiadomości i zabezpieczenia dostępu do informacji) przed niepożądanym dostępem. Przez utajnienie należy tu rozumieć taką operację, która powoduje że wiadomość jest trudna do odczytania (rozszyfrowania) przez podmiot nie znający tzw. *klucza rozszyfrowującego* - dla takiego podmiotu wiadomość będzie wyłącznie niezrozumiałym ciągiem wartości (znaków).

Kryptoanaliza - dziedzina kryptologii zajmująca się *łamaniem* szyfrów, czyli odczytywaniem zaszyfrowanych danych bez posiadania kluczy rozszyfrowujących.
Dane, które poddawane będą operacjom ochrony kryptograficznej nazywać tu będziemy po prostu **tekstem jawnym** lub **wiadomością czytelną**.

Podstawowe pojęcia [2]

Kryptogram (**szyfrogram**) - zaszyfrowana postać wiadomości czytelnej.

Klucz szyfrowania - ciąg danych służących do szyfrowania wiadomości czytelnej w kryptogram za pomocą *algorytmu szyfrowania*. Klucz ten jest odpowiednio ustalany (uzgadniany) przez nadawcę w fazie szyfrowania.

Klucz rozszyfrowujący - ciąg danych służących do rozszyfrowania kryptogramu do postaci wiadomości czytelnej za pomocą algorytmu deszyfrowania. Naturalnie, klucz ten odpowiada w pewien sposób kluczowi szyfrowania wykorzystanemu w fazie szyfrowania.
W niektórych przypadkach będziemy mieli do czynienia z ciekawą własnością przemienności kluczy.

Przemienność kluczy - role dwóch kluczy z pary mogą ulec przestawieniu. Mianowicie informację zaszyfrowaną jednym kluczem można rozszyfrować tylko przy pomocy odpowiadającego mu drugiego klucza z pary, i odwrotnie, informację zaszyfrowaną drugim kluczem można rozszyfrować wyłącznie przy pomocy klucza pierwszego.

Podstawowe pojęcia

- Kompresja danych

Podstawowe pojęcia

- Hasło
- Klucz
- Login

Podstawowe pojęcia

- Hasło - (ang. password) to ciąg znaków, który służy do uwierzytelnienia użytkownika i zabezpieczenia dostępu do systemu lub konta.
- Klucz (ang. key) - to ciąg znaków, który jest używany w procesie szyfrowania i deszyfrowania danych.
- Login (pol. identyfikator) - to unikalny ciąg znaków, który pozwala na identyfikację użytkownika w systemie.

Podstawowe pojęcia

- Identyfikacja (ang. identification)
- Uwierzytelnianie (ang. authentication)
- Autoryzacja (ang. authorization)
- Kontrola dostępu (ang. access control)
- Poufność (ang. confidentiality)
- integralność (ang. data integrity)
- Autentyczność (ang. authenticity)
- Niezaprzeczalność (ang. nonrepudiation)

Podstawowe pojęcia [2]

1. Identyfikacja - możliwość rozróżnienia użytkowników, np. w systemie operacyjnym
2. Uwierzytelnianie - proces weryfikacji tożsamości użytkownika;
3. Autoryzacja - proces przydzielania praw (dostępu do zasobów) użytkownikowi
4. Kontrola dostępu - procedura nadzorowania przestrzegania praw (dostępu do zasobów)
5. Poufność - ochrona informacji przed nieautoryzowanym jej ujawnieniem
6. Integralność - ochrona informacji przed nieautoryzowanym jej zmodyfikowaniem (ew. detekcja takiej modyfikacji)
7. Autentyczność - pewność co do pochodzenia danych
8. Niezaprzeczalność - ochrona przed fałszywym zaprzeczeniem
   - przez nadawcę - faktu wysłania danych
   - przez odbiorcę - faktu otrzymania danych

Podstawowe pojęcia

- Polityka bezpieczeństwa
- Certyfikacja
- Analiza ryzyka
- Audyt

Podstawowe pojęcia

ISO27000

Polityka bezpieczeństwa – Zamierzenia i kierunek organizacji w zakresie zachowania dostępności, integralności i poufności informacji formalnie wyrażone przez jej najwyższe kierownictwo.

Polityka bezpieczeństwa – Dokument określający metody, narzędzia, praktyki i zasady których należy używać i przestrzegać w celu zapewnienia bezpieczeństwa informacji danej organizacji.

Dodatkowo w polityce bezpieczeństwa określony jest sposób, w jaki organizacja powinna zarządzać wrażliwymi danymi, chronić je i przetwarzać.

https://securitybeztabu.pl/polityka-bezpieczenstwa/

Podstawowe pojęcia

10) akredytacją bezpieczeństwa teleinformatycznego — jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;

11) certyfikacją — jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;

12) audytem bezpieczeństwa systemu teleinformatycznego — jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;

Podstawowe pojęcia

15) ryzykiem — jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

16) szacowaniem ryzyka — jest całościowy proces analizy i oceny ryzyka;

17) zarządzaniem ryzykiem — są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

Literatura do studiowania:

[1] Schneier B.: Applied Cryptography, J. Willey & Sons, 1994

[2] http://smurf.mimuw.edu.pl/node/1568

[3] Stokłosa J., Bilski T., Pankowski T., "Bezpieczeństwo danych w systemach informatycznych", PWN, 2001