Wprowadzenie docsystemów informacyjnych

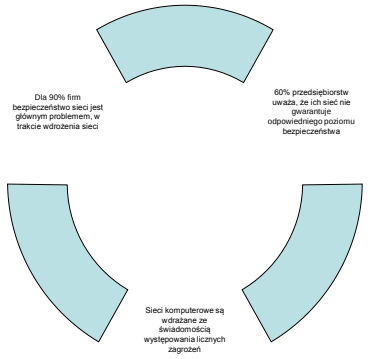
Problem bezpieczeństwa

- Tylko system zapewniający całkowite **bezpieczeństwo pracy oraz danych** może być akceptowany jako narzędzie biznesowe!
- Dlatego projektowanie systemów informacyjnych musi być związane z **gwarancją** ich bezpiecznej pracy!

Poza względami merytorycznymi za stosowaniem zabezpieczeń przemawiają także względy emocjonalne.

Przykro jest pomyśleć, że wnętrze naszego systemu komputerowego, które dla wielu staje się bez mała drugim domem, penetrują różne paskudne wirusy komputerowe czy robaki sieciowe!

Problemy bezpieczeństwa są istotne dla firm, w których instalowane są systemy informatyczne



Pojęcie „bezpieczeństwa" wiąże się z wieloma aspektami życia i może być postrzegane w różny sposób.

- Jak podaje słownik języka polskiego:
- *„Bezpieczeństwo" to stan niezagrożenia, spokoju, pewności [Szymczak 2002],*
- *„Bezpieczeństwo" to pojęcie trudne do zdefiniowania. Sytuacja, w której istnieją formalne, instytucjonalne, praktyczne gwarancje ochrony [Smolski i in.1999].*

Z praktycznego punktu widzenia zadowalająca jest definicja:

Bezpieczeństwo systemu komputerowego – stan systemu komputerowego, w którym ryzyko urzeczywistnienia się zagrożeń związanych z jego funkcjonowaniem jest ograniczone do akceptowalnego poziomu.

Najlepszymi specjalistami od bezpieczeństwa komputerowego są byli hakerzy

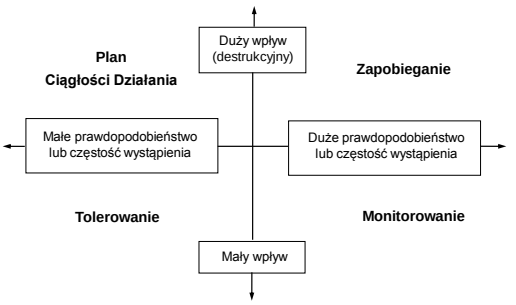

The New York Times Archive

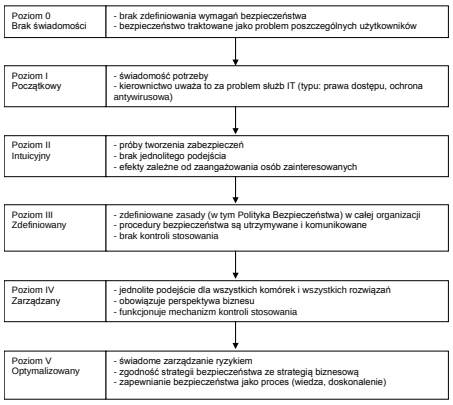
A Most-Wanted Cyberthief Is Caught in His Own Web

February 16, 1995, Thursday
By JOHN MARKOFF, (Special to The New York Times), National Desk

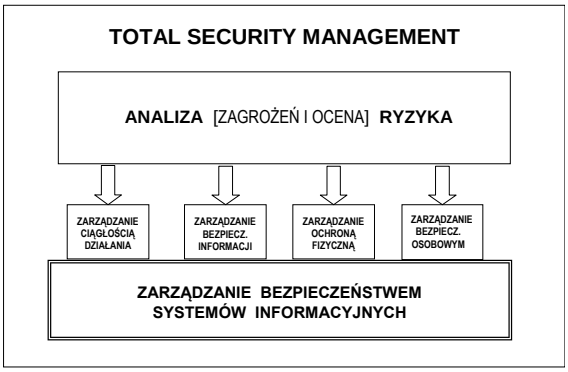
mitnicksecurity consulting, LLC

Rodzaje postępowania w zapewnianiu bezpieczeństwa





Poziomy dojrzałości zarządzania bezpieczeństwem informacji



Każdy projektant Systemu Informatycznego musi dążyć do implementacji w nim także

Systemu Zarządzania Bezpieczeństwem Informacji

(SZBI, ang. ISMS)

Odpowiednie działania należy prowadzić zgodnie z normami:

- **PN-I-07799-2:2005 (BS-7799-2)**
- **PN ISO/IEC 17799:2003 (BS-7799-1)**

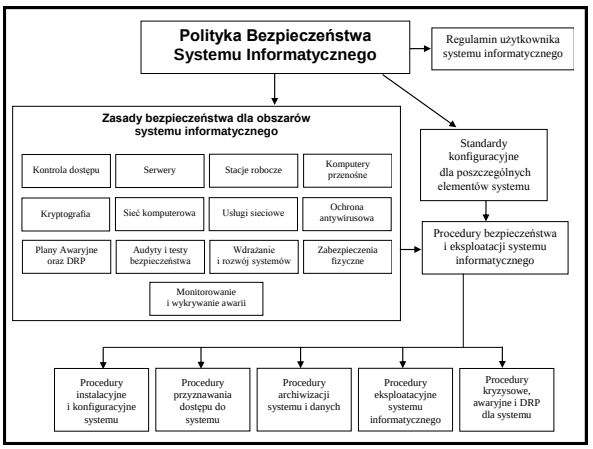
z uwzględnieniem najnowszych rewizji wspomnianych norm, czyli:

- **ISO/IEC 27001:2005**
- **ISO/IEC 17799:2005**

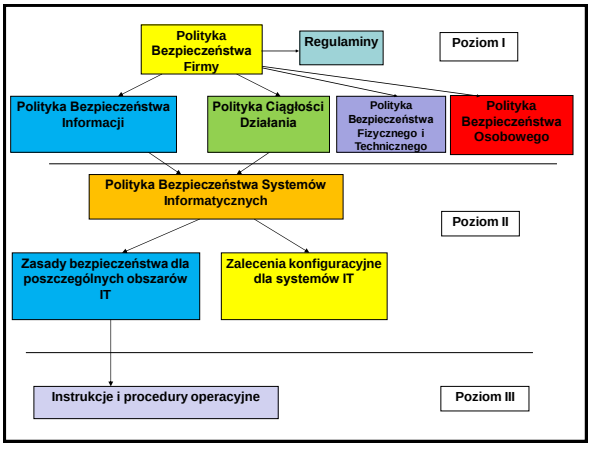
Norma ISO 27001 zakłada, że każdy system informatyczny powinien posiadać (pod)system zarządzania bezpieczeństwem informacji typu ISMS (*Information Security Manegement System)*

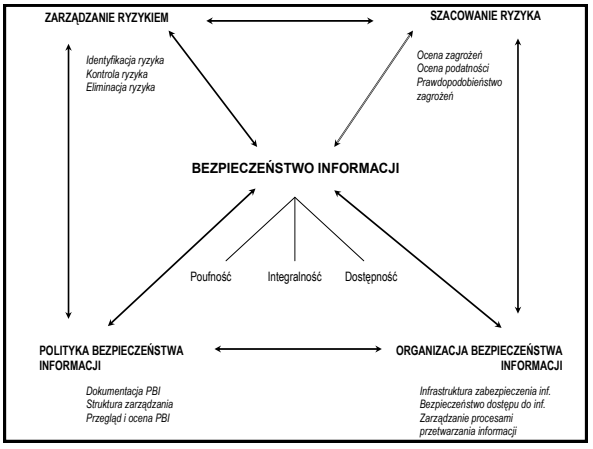
- System ISMS powinien realizować zadania związane z bezpieczeństwem zgodnie z tzw. schematem PDCA:

- P - planuj (ang. *plan)*
- D – wykonaj (ang. *Do*)
- C – sprawdzaj (ang. *Check*)
- D – działaj (ang. *Act*)

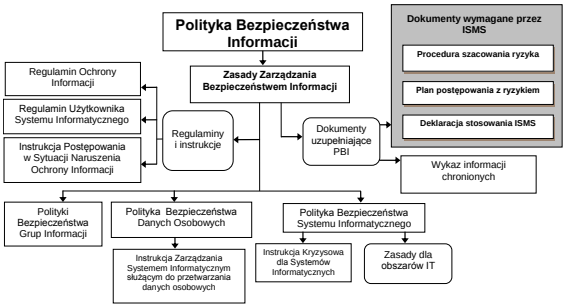


Elementy składające się na politykę bezpieczeństwa





Mapa dokumentów Polityki Bezpieczeństwa Informacji wraz z dokumentami wymaganymi przez ISMS



ISMS – Information Security Management System, norma ISO 27001 (w Polsce PN-ISO/IEC 27001:2007)

Klasyfikacja zagrożeń 1:

ze względu na charakter przyczyny:

świadoma i celowa działalność człowieka - chęć rewanżu, szpiegostwo, wandalizm, terroryzm, chęć zaspokojenia własnych ambicji

wydarzenie losowe - błędy i zaniedbania ludzkie, awarie sprzętu i oprogramowania, temperatura, wilgotność, zanieczyszczenie powietrza, zakłócenia w zasilaniu, klęski żywiołowe, wyładowania atmosferyczne, katastrofy

Klasyfikacja zagrożeń 2:

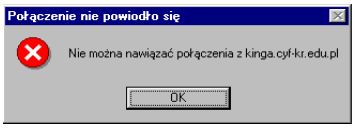
ze względu na umiejscowienie źródła zagrożenia:

wewnętrzne - mające swoje źródło wewnątrz organizacji użytkującej system informacyjny

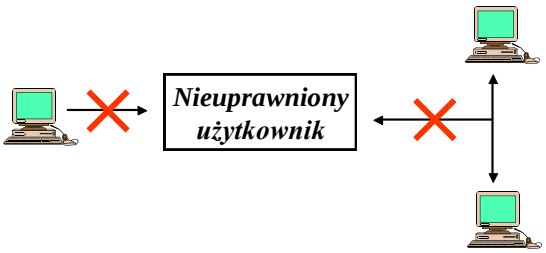
zewnętrzne - mające swoje źródło na zewnątrz organizacji (poprzez sieć komputerową, za pośrednictwem wirusów komputerowych)

Atrybuty systemu informacyjnego, wynikające z wymogu jego bezpieczeństwa:

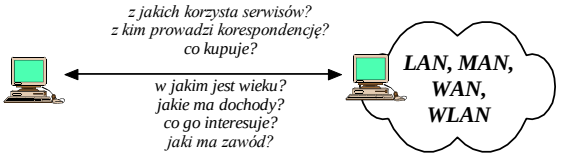
Dostępność - system i informacje mogą być osiągalne przez uprawnionego użytkownika w każdym czasie i w wymagany przez niego sposób.



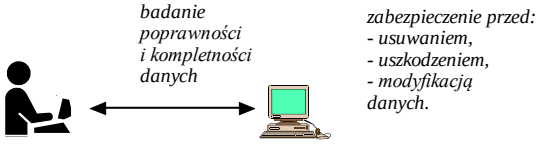
Poufność - informacje ujawniane są wyłącznie uprawnionym podmiotom i na potrzeby określonych procedur, w dozwolonych przypadkach i w dozwolony sposób



Prywatność - prawo jednostki do decydowania o tym, w jakim stopniu będzie się dzielić z innymi swymi myślami, uczuciami i faktami ze swojego życia osobistego

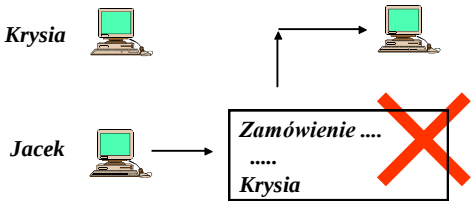


Integralność - cecha danych i informacji oznaczająca ich dokładność i kompletność oraz utrzymanie ich w tym stanie

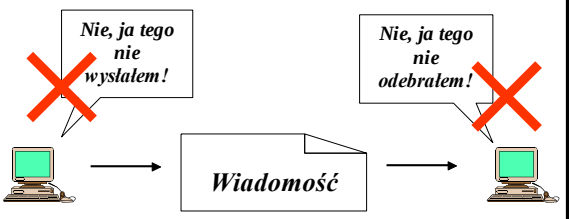


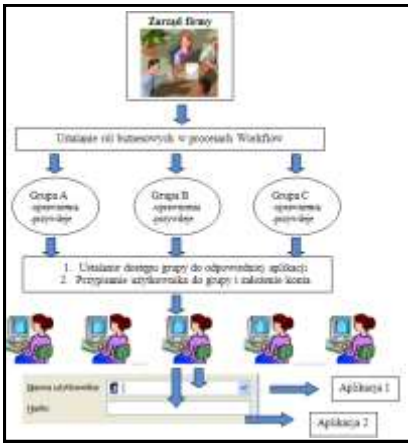
Uwierzytelnianie osób – zagwarantowanie, że osoba korzystająca z systemu jest rzeczywiście tą, za którą się podaje.

Uwierzytelnianie informacji – zagwarantowanie, że informacja rzeczywiście pochodzi ze źródła, które jest w niej wymienione



Niezaprzeczalność – brak możliwości zaprzeczenia faktowi wysłania lub odebrania informacji





Poszczególni użytkownicy mogą mieć w tym samym systemie różne role, zależnie od tego, jak są zalogowani

Integracja danych osobowych w katalogu tożsamości

Zagadnieniom bezpieczeństwa systemów informatycznych poświęcone są liczne normy i standardy (polskie i międzynarodowe)

- PN-I-13335-1:1999,
- PN-ISO/IEC 17799:2003,
- ISO/IEC JTC 1-SC27,
- ISO/IEC JTC 1-SC6
- ... i wiele innych.

Trzeba ich bezwzględnie przestrzegać!

Zasoby systemu informacyjnego zapewniające jego prawidłowe i bezpieczne funkcjonowanie:

ludzkie - potencjał wiedzy ukierunkowany na rozwiązywanie problemów systemu; użytkownicy pełniący role nadawców i odbiorców informacji oraz adresaci technologii informacyjnych;

informacyjne - zbiory danych przeznaczone do przetwarzania (bazy danych, metod, modeli, wiedzy);

proceduralne - algorytmy, procedury, oprogramowanie;

techniczne - sprzęt komputerowy, sieci telekomunikacyjne, nośniki danych.

Zasoby systemu informatycznego są cenne i muszą być chronione

Należy jednak pamiętać o bardzo ważnej zasadzie:

„Nie należy na ochronę zasobu przeznaczać więcej niż jest on wart.”

Sama wartość zasobu to nie wszystko. Przy szacowaniu należy również wziąć pod uwagę kilka czynników:

- straty spowodowane jego utratą,
- straty wynikające z nieosiągniętych zysków,
- koszty straconego czasu,
- koszty napraw i zmian,
- koszty pozyskania nowego zasobu.

Przeciętny koszt godzinnej awarii systemu informacyjnego

Charakter Firmy	Koszt jednogodzinnej awarii w tys. dolarów
Brokerska	6480
Energetyczna	2800
Karty Kredytowe	2580
Telekomunikacyjna	2000
Wytwórcza	1600
Finansowa	1500
Sprzedaż detaliczna	1100
Farmaceutyczna	1000
Chemiczna	704
Ochrona Zdrowia	636
Rezerwacja Biletów Lotniczych	90

Głównym kryterium przy tworzeniu hierarchii ważności zasobów jest ich wpływ na funkcjonowanie systemu:

- **zasoby strategiczne** - decydują o strategii przedsiębiorstwa. Wymagania ochronne bardzo wysokie,
- **zasoby krytyczne** – mają wpływ na bieżące funkcjonowanie przedsiębiorstwa. Wymagania ochronne wysokie,
- **zasoby autoryzowane** – podlegają ochronie na podstawie ogólnie obowiązujących przepisów. Wymagania ochronne umiarkowane,
- **zasoby powszechnie dostępne** – ogólnie dostępne. Wymagania ochronne – brak.

Dobrze zaprojektowany system informacyjny musi być gotowy do odparcia ataku z każdej strony!

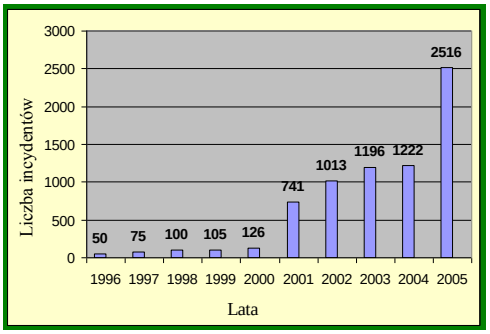
Jest zawsze mnóstwo osób, które chcą się dostać do zawartości naszych komputerów

Większość poważnych incydentów związanych z zagrożeniem systemów informatycznych było spowodowane nieostrożnością personelu, który miał legalny dostęp do systemu

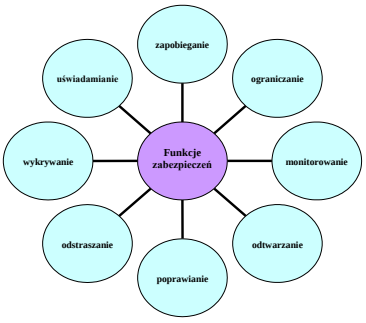
Jak powiedział kiedyś Albert Einstein:

*„Tylko dwie rzeczy są nieskończone: wszechświat i **ludzka głupota**, chociaż co do tego pierwszego nie mam pewności”*

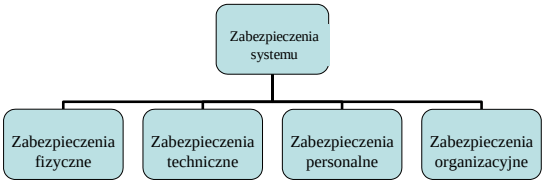
Problem zagrożenia systemów informatycznych narasta



Zabezpieczenia realizują jedną lub wiele następujących funkcji:

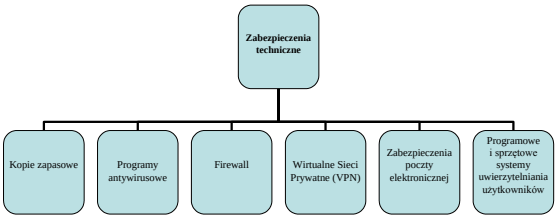


Podział zabezpieczeń



Ważną rolę odgrywa zabezpieczenie fizyczne komputerów

Zabezpieczenia techniczne



Zacznijmy od zagadnień bezpieczeństwa fizycznego

Najczęściej system informatyczny jest niedostępny z banalnego powodu:
braku zasilania

Alternatywne źródła zasilania systemów komputerowych
Zasilacze awaryjne (UPS - Uninterruptible Power Supply)

Różne konfiguracje zasilania awaryjnego

Rozproszone zasilanie awaryjne:

Centralne zasilanie awaryjne:

Dłuższą niezależność od zasilania gwarantują ***Agregaty prądotwórcze***

Źródło zasilania: benzyna, olej napędowy, gaz ziemny, gaz płynny;

Czas osiągania pełnej sprawności – kilkanaście lub kilkadziesiąt sekund (dlatego muszą być stosowane łącznie z zasilaczami UPS);

czas nieprzerwanej pracy – do kilkunastu dni.

Dublowanie dysków

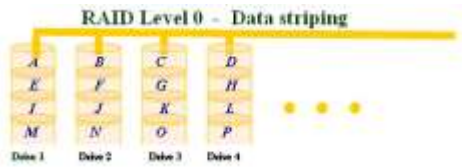
Technologia RAID:
Redundant Array of Independent/Inexpensive Disks
Nadmiarowa macierz niezależnych/niedrogich dysków

RAID 0 (disk striping, paskowanie dysków)

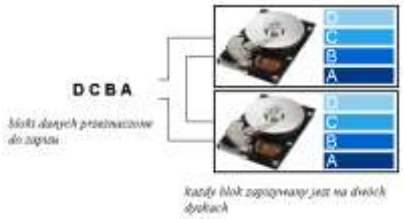
rośnie wydajność systemu (jednoczesny zapis kolejnych bloków danych),

zastosowanie technologii RAID 0 nie zwiększa poziomu bezpieczeństwa (czasami nawet zmniejsza).

RAID 0 przy większej liczbie dysków



RAID 1 (mirroring, obraz lustrzany)

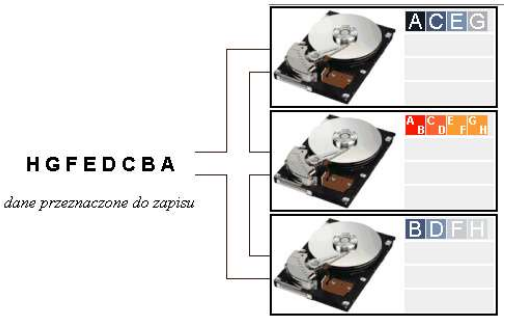


technika ta zapewnia wysoki poziom bezpieczeństwa,

łączna pojemność wynosi 50% sumarycznej pojemności dysków.

RAID 1 przy większej liczbie dysków

RAID 3 (stripe set with parity, paskowanie z oddzielnym dyskiem przechowującym bity parzystości)



Zasada działania

Zapis danych:

Dysk	Wartości
dysk 1 - dane	1 1 1 0 1 1 0 0
dysk 2 - dane	1 0 1 1 0 0 1 1
dysk 3 - dane	0 1 0 0 1 1 0 1
dysk 4 - bity parzystości (XOR)	0 0 0 1 0 0 1 0

Odtwarzanie danych:

Dysk	Przed awarią	Awaria dysku z danymi
1 – dane	1 1 1 0 1 1 0 0	1 1 1 0 1 1 0 0
2 – dane	1 0 1 1 0 0 1 1	x x x x x x x x
3 – dane	0 1 0 0 1 1 0 1	0 1 0 0 1 1 0 1
4 - bity parzystości	0 0 0 1 0 0 1 0	0 0 0 1 0 0 1 0
Odtworzenie		1 0 1 1 0 0 1 1

Właściwości RAID 3

- RAID 3 zapewnia wzrost wydajności i wzrost bezpieczeństwa,
- pozwala na odtworzenie danych po awarii jednego z dysków,
- zapewnia lepsze wykorzystanie powierzchni dysku niż RAID 10 (tylko jeden dysk przechowuje dodatkowe informacje /bity parzystości/),
- wymaga zastosowania przynajmniej trzech dysków,
- jakakolwiek modyfikacja danych wymaga uaktualnienia zapisów na dysku parzystości; może to powodować spadek wydajności systemu w sytuacji (konieczne jest oczekiwanie na dokonanie zmian na dysku zawierającym bity parzystości).

RAID 3 przy większej liczbie dysków

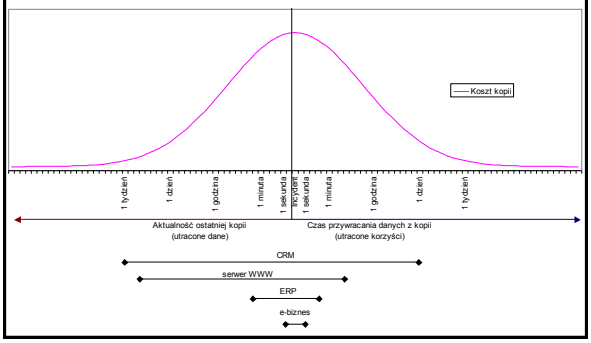
RAID 5 bity parzystości rozproszone na wszystkich dyskach

Technologia zbliżona do RAID 3 - ale nie powoduje spadku wydajności spowodowanego oczekiwaniem na dokonanie zapisu na dysku parzystości,

pozwala na zwiększenie wydajności i zapewnia bezpieczeństwo danych.

RAID 5 przy większej liczbie dysków

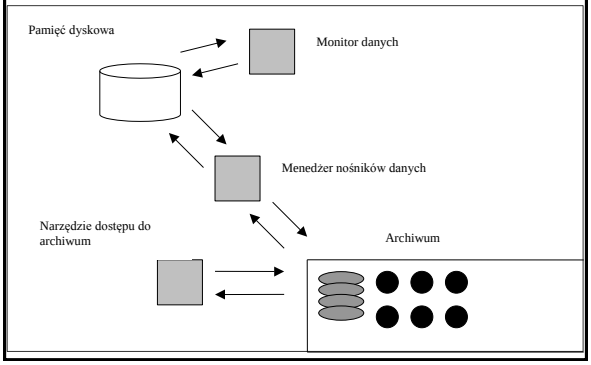
Sposobem zwiększenia bezpieczeństwa danych jest tworzenie kopii



Rodzaje kopii stosowane do zabezpieczenia systemu

Rodzaj kopii	Kopia pełna	Kopia różnicowa	Kopia przyrostowa
Kopiowane dane	wszystkie dane	dane od ostatniej kopii pełnej	dane od ostatniej kopii
Zaleta	szybkie odtwarzanie danych w przypadku awarii	stosunkowo szybkie odtwarzanie	szybkie wykonywanie
Wada	długi czas dokonywania kopii	średni czas wykonywania rosnący wraz z liczbą kopii od ostatniej pełnej	powolne odtwarzanie (uszkodzenie choć jednej powoduje utratę późniejszych danych)

Narzędzia do archiwizacji danych

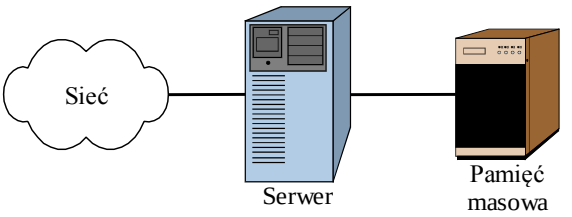


Zaawansowane systemy pamięci zewnętrznej

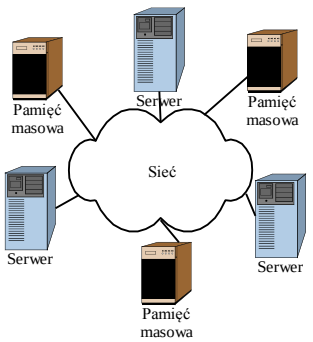
Wymogi stawiane systemom pamięci zewnętrznej:

- duża pojemność,
- odporność na awarie,
- możliwość współdzielenia danych (urządzenia są współużytkowane przez wiele systemów komputerowych).

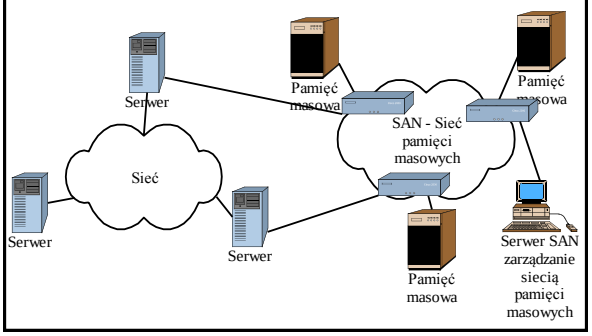
Systemy typu SAS (*Server Attached Storage*)



Systemy typu NAS (*Network Attached Storage*)



Systemy typu SAN (*Storage Area Network*)



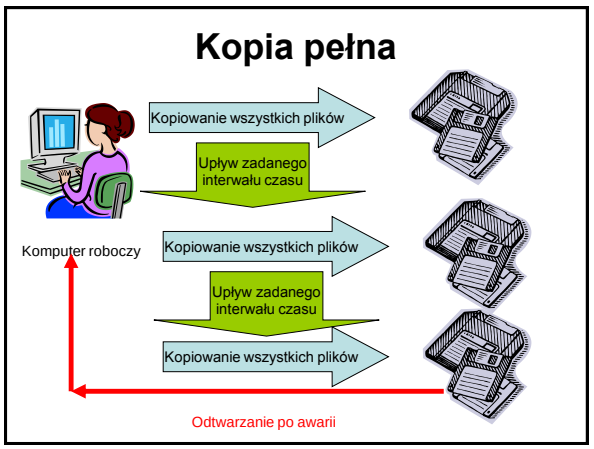
Kopie zapasowe można podzielić ze względu na strategie dodawania plików do tworzonej kopii:

- Kopia pełna
- Kopia przyrostowa
- Kopia różnicowa

Kopia pełna – kopiowaniu podlegają wszystkie pliki, niezależnie od daty ich ostatniej modyfikacji.

Wada: wykonywania kopii jest czasochłonne.

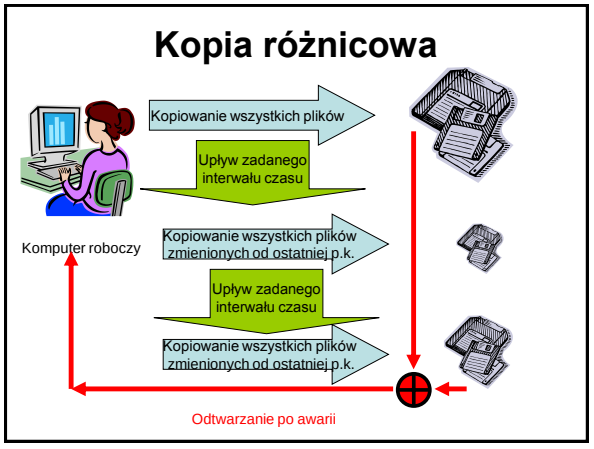
Zaleta: odzyskiwanie danych jest szybkie



Kopia różnicowa – kopiowane są pliki, które zostały zmodyfikowane od czas utworzenia ostatniej pełnej kopii.

Wada: odtworzenie danych wymaga odtworzenia ostatniego pełnego backupu oraz ostatniej kopii różnicowej

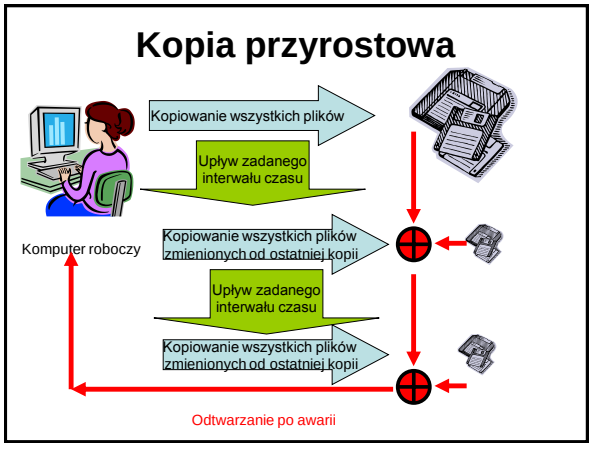
Zaleta: czas wykonywania kopii jest stosunkowo krótki (na początku!)



Kopia przyrostowa – kopiowane są jedynie pliki, które zostały zmodyfikowane od czasu tworzenia ostatniej pełnej lub przyrostowej kopii.

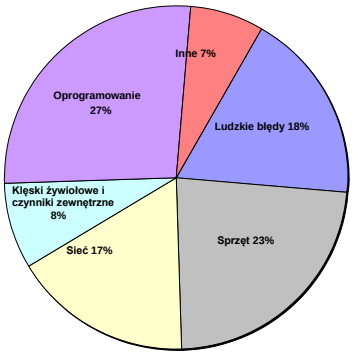
Wada: przed zrobieniem tej kopii należy wykonać kopie pełną oraz odtworzenie danych wymaga odtworzenia ostatniego pełnego backupu oraz wszystkich kopii przyrostowych

Zaleta: czas wykonywania kopii jest dość krótki



Na tworzenie warunków bezpieczeństwa *systemów komputerowych* w firmie składają się działania **techniczne** i działania **organizacyjne**

Główne przyczyny awarii systemów

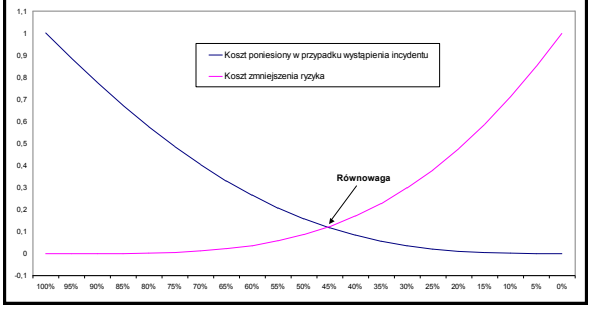


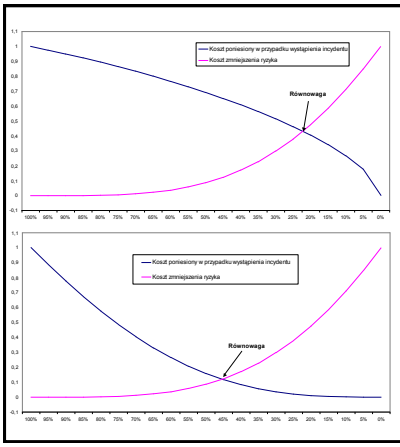
Sposoby zapewnienia dostępności pracy systemu informatycznego oraz ich koszty

Co oznacza określony poziom niezawodności i dostępności systemu informatycznego

Ilość "dziewiątek"	Procentowa dostępność systemu w roku	Czas trwania awarii w roku	Jednostka	Czas trwania awarii w tygodniu	Jednostka
1	90%	37	Dni	17	Godziny
2	99%	3,65	Dni	1,41	Godziny
3	99,9%	8,45	Godziny	10,5	Minuty
4	99,99%	52,5	Minuty	1	Minuty
5	99,999%	5,25	Minuty	6	Sekundy
6	99,9999%	31,5	Sekundy	0,6	Sekundy

Techniki ograniczania ryzyka są kosztowne, więc trzeba ustalić opłacalny poziom zabezpieczeń





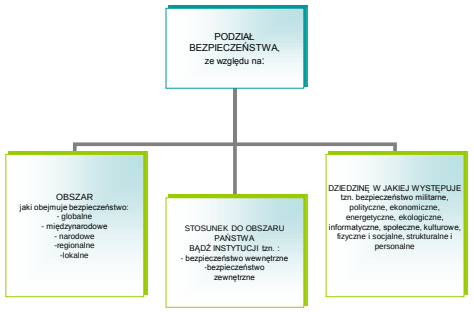
Punkt równowagi zależy od stopnia **krytyczności** zabezpieczanego systemu

Ze sprawami bezpieczeństwa nie należy przesadzać!

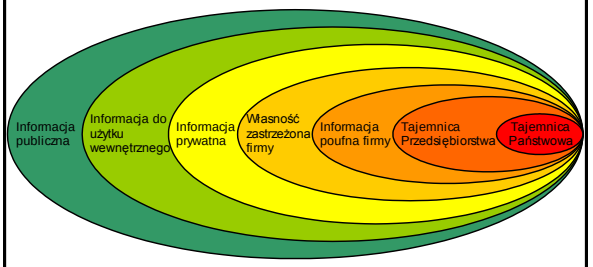
Pożądany poziom zabezpieczeń zależy od profilu instytucji:

Profil instytucji i poziom zabezpieczenia	
Profil instytucji	**Poziom zabezpieczenia systemu informacyjnego**
Uszkodzenie systemu informacyjnego prowadzi do całkowitego załamania instytucji i może mieć poważne konsekwencje polityczne, społeczne lub ekonomiczne.	**maksymalny**
W przypadku uszkodzenia systemu informacyjnego część organizacji nie może funkcjonować. Dłuższe utrzymywanie się tego stanu może mieć poważne konsekwencje dla instytucji lub jej partnerów.	**wysoki**
Konsekwencją poważnego i długotrwałego uszkodzenia systemu informacyjnego może być upadek instytucji.	**średni**
Uszkodzenie systemu informacyjnego może spowodować jedynie niewielkie perturbacje w funkcjonowaniu instytucji.	**niski**

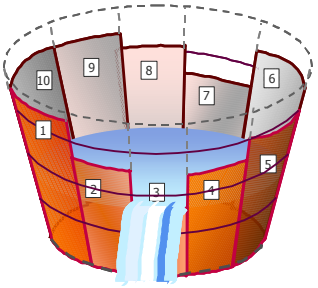
Podział bezpieczeństwa



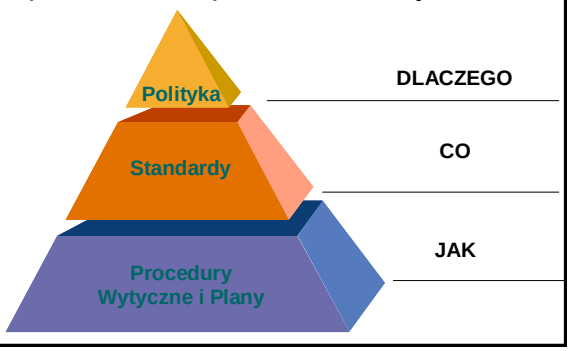
Klasyfikacja stopnia poufności danych



Trzeba pamiętać, że przyczyną kryzysu jest zawsze **najsłabiej** chroniony element



Sposoby budowy wysokiego poziomu bezpieczeństwa systemu



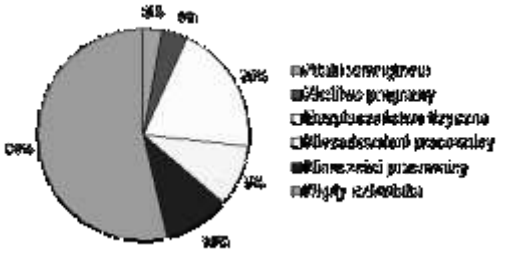
Typy najczęściej spotykanych zagrożeń w sieci komputerowej

- fałszerstwo komputerowe,
- włamanie do systemu, czyli tzw. hacking,
- oszustwo, a w szczególności manipulacja danymi,
- manipulacja programami,
- oszustwa, jakim są manipulacje wynikami,
- sabotaż komputerowy,
- piractwo,
- podsłuch,
- niszczenie danych oraz programów komputerowych

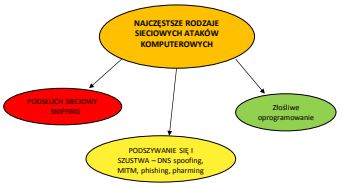
Klasyfikacja ataków na systemy komputerowe:

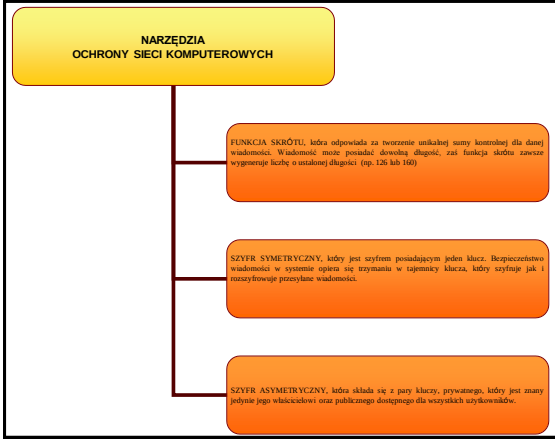
- atak fizyczny,
- atak przez uniemożliwienie działania,
- atak przez wykorzystanie „tylnego wejścia”,
- atak poprzez błędnie skonfigurowaną usługę,
- atak przez aktywne rozsynchronizowanie tcp

Wpływ poszczególnych czynników na bezpieczeństwo systemów komputerowych:



Najczęstsze rodzaje sieciowych ataków komputerowych





Ochrona Systemu Informatycznego powinna być **całościowa**, musi obejmować takie aspekty jak:

- Fizyczne bezpieczeństwo serwera,
- Bezproblemowe zasilanie,
- Strategię tworzenia kopii zapasowych,
- Procedury awaryjne,
- Zasady dostępu do samego serwera,
- Ochronę sieciową.

Dla zachowania bezpieczeństwa przetwarzania informacji stosowane są różne techniki:

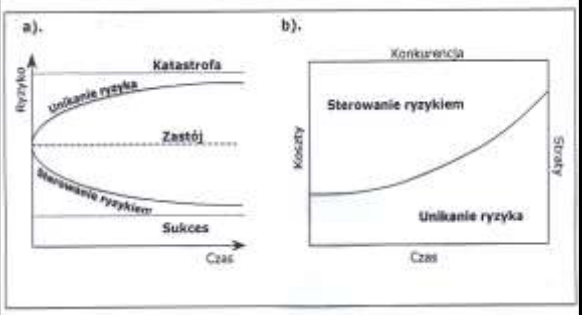
Łatwiejsze do zdefiniowania i do **wyegzekwowania** są z reguły działania techniczne

Najważniejsze z działań technicznych polegają na szyfrowaniu przesyłanych i przechowywanych informacji oraz korzystanie z techniki podpisów elektronicznych

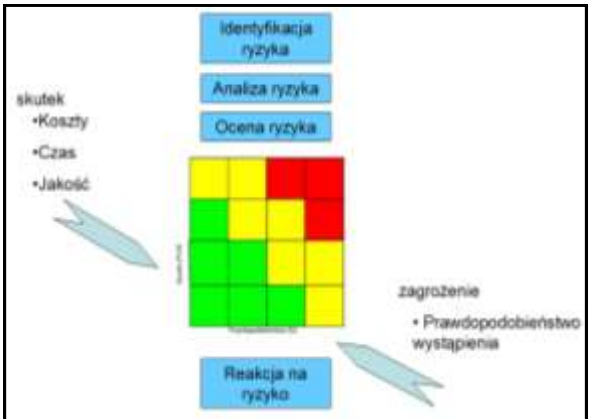
Bezpieczne algorytmy realizacji transakcji w sieciach komputerowych oparte są na kryptografii

*Najczęściej stosowanymi **algorytmami kryptograficznymi z kluczem jawnym,** mającymi na celu ochronę danych podczas transmisji internetowych wykorzystywanych w handlu elektronicznym, są algorytmy RSA i ElGamala.*

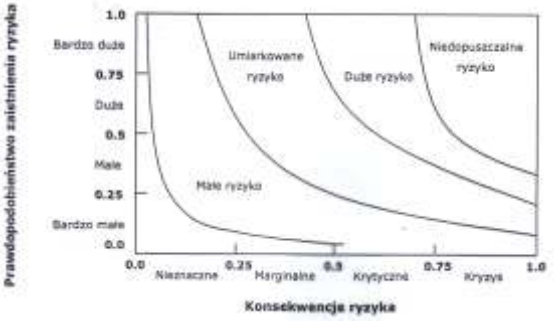
Ryzyka można unikać albo można nim świadomie sterować



Pod pojęciem **sterowania ryzykiem** kryje się działanie mające na celu ograniczanie ryzyka poprzez planowanie, projektowanie i wdrażanie rozwiązań mających zapewnić utrzymanie ryzyka na poziomie możliwym do zaakceptowania.

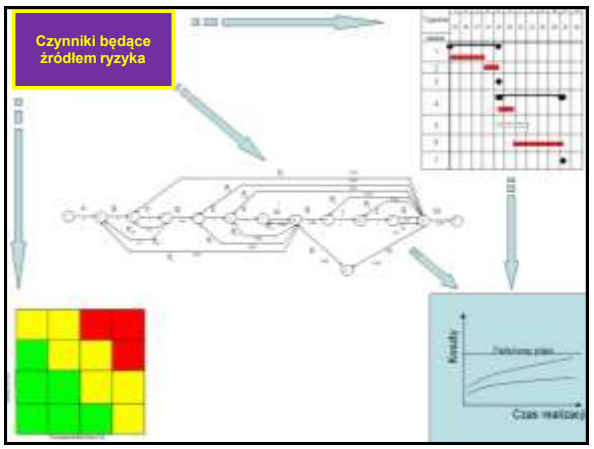


Można rozważać różne kategorie ryzyka



Etapy przygotowania strategii zabezpieczeń

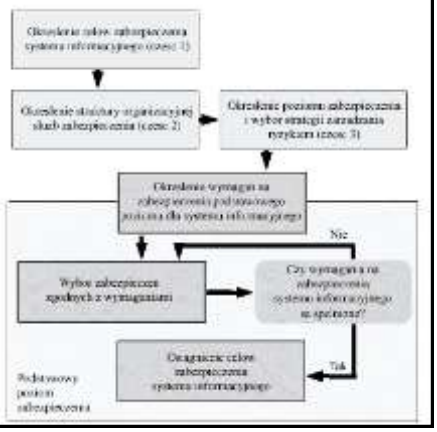
1. Sprecyzowanie, co i przed czym mamy chronić, czyli określenie zasobów chronionych i zagrożeń.
2. Określenie prawdopodobieństwa poszczególnych zagrożeń
3. Określenie zabezpieczeń, czyli, w jaki sposób chronimy zasoby
4. Ciągłe analizowanie SI i zabezpieczeń w celu aktualizacji procedur zabezpieczających poprawiania jego ewentualnych błędów



W procesie sterowania ryzykiem można wyróżnić następujące etapy:

- wskazywanie zagrożeń,
- rozpoznawanie zagrożeń,
- analiza ryzyka,
- planowanie i przeciwdziałanie ryzyku,
- określenie i projektowanie działań,
- wdrażanie standardów i procedur,
- przeciwdziałanie ryzyku.

Wybór strategii zarządzania ryzykiem w procesie planowania zabezpieczeń



Rozwiązania dotyczące zabezpieczenia technicznego

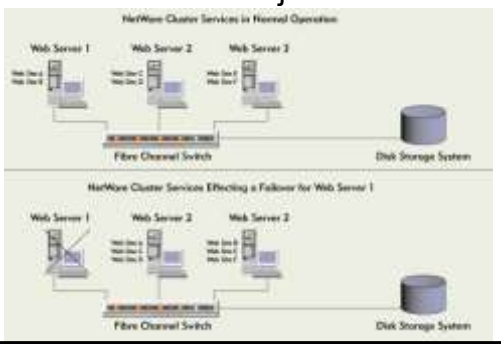
Rozwiązania klastrowe

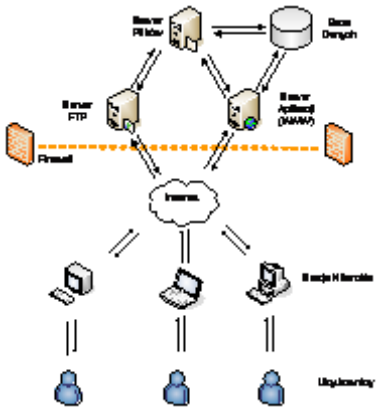
Klaster - grupa połączonych ze sobą komputerów.

Klaster zapewnia:

- wysoką wydajność,
- dostępność,
- odporność na awarie.

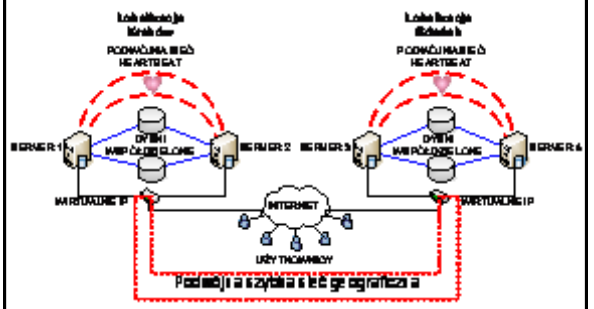
Klastry wysokiej dostępności - komputery mogące zamiennie realizować swoje zadania.



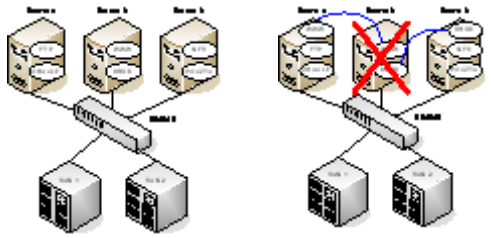


Schemat aplikacji internetowej wraz z elementami jej zabezpieczenia

Przykładowe rozwiązanie systemu o zwiększonej dostępności



VERITAS Cluster Server
przed i po awarii jednego komputera



Elementy klastrów wysokiej dostępności:

Elementy sprzętowe systemów klasy HA:

- serwery (realizujące usługi WWW, obsługę poczty, DNS, ...),
- sieci łączące (Ethernet, sieci światłowodowe),
- systemy pamięci masowej -
  - –tablice RAID,
  - –rozwiązania klasy SAN.

Elementy programowe systemów klasy HA:

- oprogramowanie wykrywające awarię,
- oprogramowanie pozwalające na przejęcie zadań uszkodzonego elementu,
- oprogramowanie pozwalające na równoważenie obciążeń.

Bezpieczeństwo z informatycznego punktu widzenia to:

- *Stan, w którym komputer jest bezpieczny, jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze stawianymi mu oczekiwaniami [Garfinkel, Stafford 1997],*
- *Miara zaufania, że system i jego dane pozostaną nienaruszone [Adamczewski 2000].*

Dziesięć tak zwanych „niezmiennych zasad bezpieczeństwa”

Zasady te sformułowane przez pracownika firmy Microsoft Scott’a Culp’a w 2000 roku, pomimo ogromnego postępu dokonującego się w dziedzinie zabezpieczeń, w dalszym ciągu są aktualne i obrazują słabości wszystkich dostępnych systemów zabezpieczeń

1. *Jeżeli osoba o złych zamiarach potrafi zmusić użytkownika do uruchomienia jej programu na jego komputerze, to komputer ten przestaje być jego komputerem.*
2. *Jeżeli osoba o złych zamiarach potrafi zmienić system operacyjny w komputerze użytkownika, to komputer ten przestaje być jego komputerem.*
3. *Jeżeli osoba o złych zamiarach miała nieograniczony dostęp fizyczny do komputera użytkownika, to komputer ten przestaje być jego komputerem.*
4. *Jeżeli osoba o złych zamiarach będzie w stanie umieścić programy w witrynie sieci Web danej organizacji, to witryna ta przestaje być jej witryną.*

5. *Słabe hasła niwelują silne zabezpieczenia*. Nawet jeśli system został zaprojektowany w sposób bezpieczny, ale użytkownicy oraz administratorzy używają pustych lub łatwych do odgadnięcia haseł, to wszelkie zabezpieczenia staną się nieefektywne w momencie złamania któregoś z haseł przez atakującego.
6. *Komputer jest bezpieczny jedynie w takim stopniu, w jakim jego administrator jest godny zaufania*.

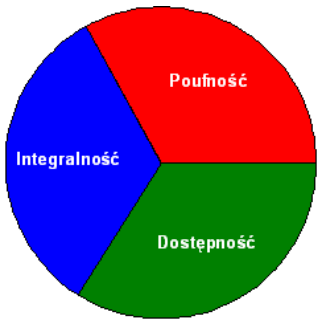
7. *Zaszyfrowane dane są bezpieczne jedynie w takim stopniu, w jakim jest bezpieczny klucz deszyfrujący*. Żaden algorytm szyfrujący nie zabezpieczy szyfrogramu przed napastnikiem, który posiada lub może zdobyć klucz deszyfrujący. Samo szyfrowanie nie jest rozwiązaniem problemów biznesowych, jeżeli w organizacji nie istnieją dobrze określone i przestrzegane procedury związane z zarządzaniem kluczami.
8. *Nie aktualizowane skanery antywirusowe są tylko trochę lepsze niż całkowity brak*.
9. *Całkowita anonimowość jest niepraktyczna, zarówno w życiu jak i Internecie*.

Technologia nie jest panaceum.

Pomimo iż technologia pomaga zabezpieczyć systemy komputerowe, to nie jest ona – i nigdy nie będzie – rozwiązaniem samym w sobie.

Do utworzenia bezpiecznego środowiska organizacji konieczne jest połączenie technologii z ludźmi i procesami

Obszary, w których ryzyko może obejmować dane zgromadzone w systemie informacyjnym



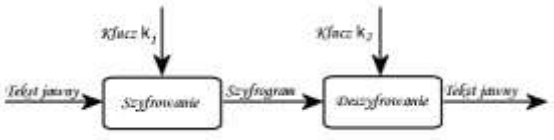
Ważną techniką zwiększającą bezpieczeństwo systemów informatycznych jest **szyfrowanie** komunikatów i danych.

Istnieje obecnie wiele technik szyfrowania, ale powszechnie używane są głównie dwie:

Technika symetryczna (klucza tajnego)

Technika asymetryczna (klucza publicznego i prywatnego)

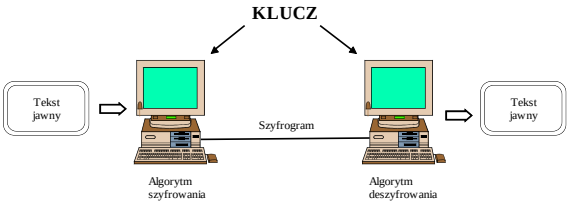
Ogólny schemat procesu szyfrowania



Jeśli klucze k_1 oraz k_2 są identyczne, to mamy do czynienia z kryptografią symetryczną. Ogromnie ważna jest wtedy sprawa zapewnienia tajności klucza.

Jeśli klucz k_1 jest inny, niż związany z nim klucz k_2 - to mamy do czynienia z kryptografią asymetryczną, a klucze mają nazwy: k_1 jest to klucz publiczny, a k_2 to klucz prywatny (musi być strzeżony, ale jest tylko jeden)

Symetryczne algorytmy kryptograficzne – w trakcie szyfrowania i deszyfrowania wykorzystywany jest ten sam klucz



Problemy związane z szyfrowaniem symetrycznym

- sposób przekazania klucza,
- konieczność stosowanie oddzielnego klucza dla każdej pary nadawca - odbiorca.

Zalety i wady algorytmów symetrycznych

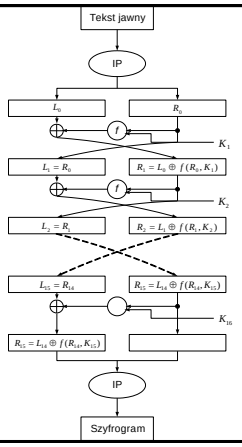
Zalety	Wady
Umożliwiają szybkie szyfrowanie danych	Konieczność utrzymania w tajemnicy klucza symetrycznego po obu stronach kanału komunikacji
Klucze symetryczne są relatywnie krótkie	Potrzeba stosowania ogromnej liczby kluczy w dużych sieciach komunikuje się wiele osób
Wykorzystywane do konstruowania innych mechanizmów kryptograficznych, takich jak: funkcje skrótu, czy podpis elektroniczny	Konieczność częstej wymiany kluczy (zwykle ustalenie nowego klucza dla każdej sesji), co podyktowane jest względami bezpieczeństwa.
Proste transformacje oparte o klucz symetryczny są proste do analizy i mogą służyć do konstrukcji mocnych szyfrów	Konieczność udostępnienia kluczy tajnych zaufanej trzeciej stronie

Lista kilku popularnych algorytmów symetrycznych:

- BLOWFISH,
- DES,
- IDEA,
- RC2,
- RC4,
- SAFER.

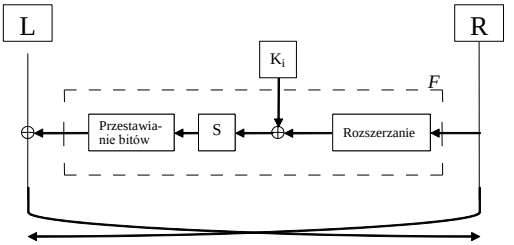
Zestawienie algorytmów symetrycznych

Lp.	Nazwa algorytmu	Typ algorytmu	Szybkość kodowania	Długość klucza	Poziom bezpieczeństwa	Uwagi
1.	DES	blokowy	średnia	56 bitów	średni	standard publiczny w USA
2.	3DES	blokowy	mała	2x56 bitów	średni	standard publiczny w USA
3.	IDEA	Blokowy	średnia	128 bitów	wysoki	chroniony patentem
4.	RC3	Blokowy	duża	zmienna	prawdopodobnie wysoki	utajniony, własność RSA Inc.
5.	RC4	Strumieniowy	bardzo duża	zmienna	niski, podatny na złamanie	nie zaleca się implementacji w nowych systemach



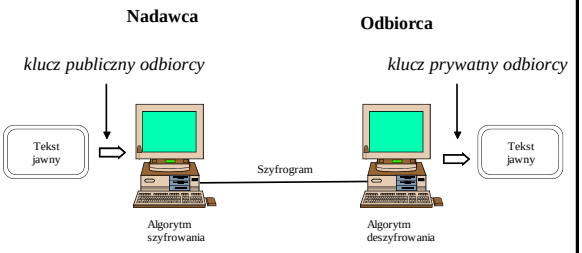
Schemat szyfrowania algorytmem DES

Struktura pojedynczej tury algorytmu DES



Asymetryczne algorytmy kryptograficzne

– w trakcie szyfrowania i deszyfrowania wykorzystywane są inne klucze (tzw. *klucz publiczny* i *klucz prywatny*)



Użycie klucza prywatnego i publicznego

Kluczy publicznych może być dowolnie dużo i może je mieć każdy, kto chce poufnie korespondować z odbiorcą

Klucz prywatny **musi być tylko jeden**, bo na tym opiera się cała metoda!

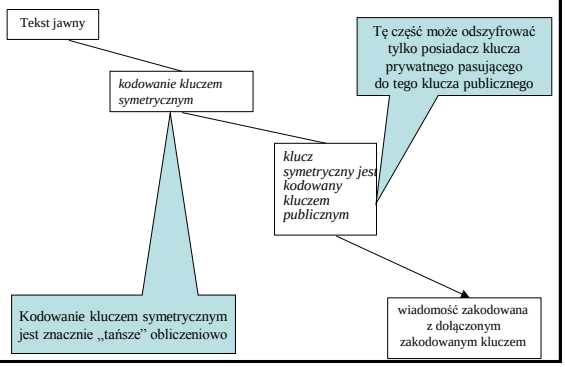
. Porównanie algorytmów asymetrycznych

Lp.	Nazwa algorytmu	Szybkość kodowania	Długość klucza	Poziom bezpieczeństwa	Uwagi
1.	Diffiego-Hellmana	Duża	Zmienna	Wysoki	Pierwszy algorytm asymetryczny
2.	Rabina	Średnia	Zmienna	Średni	Nie nadaje się do podpisów
3.	EIGamala	Średnia	Zmienna, większa niż 512 bitów	Wysoki	Podpis/ szyfrowanie
4.	Plecakowy	Mała	Zmienna	Żaden (algorytm złamany)	Nie stosowany w praktyce
5.	RSA	Bardzo duża	Zmienna	Wysoki/Bardzo wysoki	Bardzo dużo implementacji
6.	DSA	Bardzo duża	Zmienna	Wysoki/Bardzo wysoki	Być może posiada furtkę

Zalety i wady algorytmów asymetrycznych

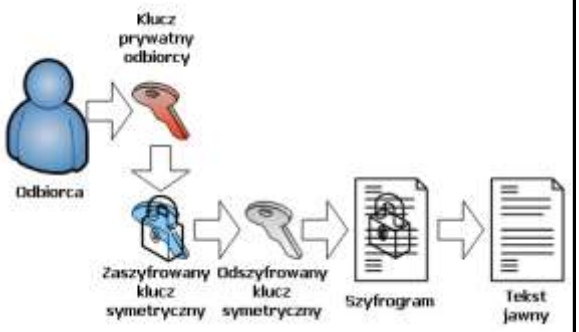
Zalety	Wady
Jedynie klucz prywatny musi pozostać tajny, choć autentyczność kluczy publicznych musi być również zagwarantowana.	Prędkość kodowania przy użyciu kluczy asymetrycznych jest wielokrotnie niższa w porównaniu z szyfrowaniem symetrycznym.
Administrowanie kluczami asymetrycznymi pozwala na obecność zaufanej trzeciej, która nie ma dostępu do kluczy prywatnych użytkowników.	Wielkość kluczy asymetrycznych jest znacznie większa niż w przypadku zastosowania kluczy symetrycznych
W komunikacji wieloosobowej liczba kluczy jest zdecydowanie mniejsza niż w przypadku zastosowania kryptografii symetrycznej.	Szyfrowanie asymetryczne charakteryzuje zdecydowanie krótszy od symetrycznego okres funkcjonowania w kryptografii.
Nie ma potrzeby wymieniać kluczy tak często, jak kluczy symetrycznych.	
Stanowią podstawę dla sprawnie funkcjonującego mechanizmu podpisu elektronicznego.	

Przesyłanie wiadomości kodowanej przy pomocy dwóch kluczy

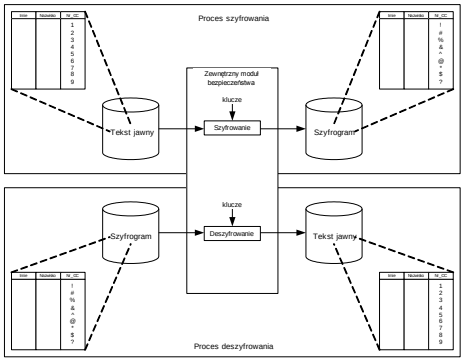


Schemat szyfrowania hybrydowego

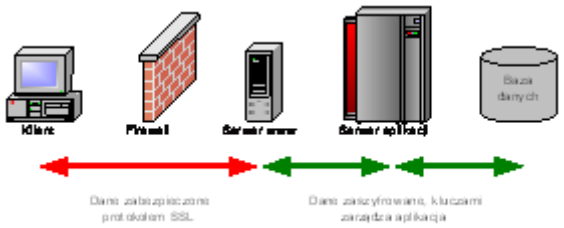
Proces deszyfrowania w systemie hybrydowym



Szyfrowane powinny być nie tylko przesyłane komunikaty, ale także dane przechowywane w bazie danych



W różnych częściach systemu mogą być stosowane różne metody szyfrowania danych

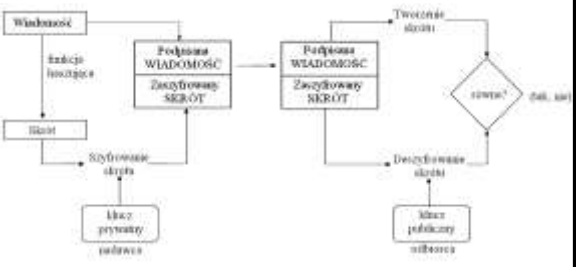


Porównanie i zastosowanie kryptografii symetrycznej i asymetrycznej

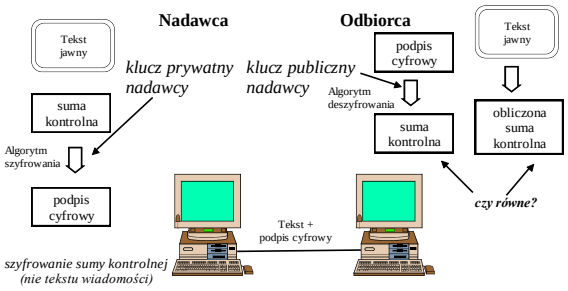
Cechy	Szyfrowanie symetryczne	Szyfrowanie asymetryczne
Wymogi (ilość kluczy)	Szyfrowanie i deszyfrowanie jednym samym kluczem (jeden klucz)	Szyfrowanie jednym kluczem deszyfrowanie drugim kluczem (para kluczy)
Bezpieczeństwo	Niskie - nadawca musi odbiorcy także przesłać klucz (możliwość przechwycenia klucza)	Wysokie – każdy ma swój klucz nie ma potrzeby przesyłania klucza
Szybkość	Duża szybkość szyfrowania i deszyfrowania informacji (DES 100 razy szybszy od RSA)	Mała szybkość deszyfrowani i szyfrowania informacji
Niezaprzeczalność	Trudność generacji podpisu cyfrowego	Łatwość generacji podpisu cyfrowego
Dystrybucja kluczy	Kłopotliwa, trudność w dołączaniu nowych użytkowników systemu kryptograficznego	Łatwość w dołączaniu nowych użytkowników systemu kryptograficznego
Zastosowanie	Szyfrowanie plików Protokoły PGP, SSL wykorzystują odpowiednio IDEA, DES do kodowania wiadomości	Przesyłanie danych Protokoły PGP, SSL stosują RSA do dystrybucji klucza tajnego Tworzenie podpisów elektronicznych Protokół DSS wykorzystuje RSA

Z zagadnieniem szyfrowania danych w celu zapewnienia ich **poufności** wiąże się zagadnienie elektronicznego podpisywania dokumentów, mające na celu zapewnienie ich **niezaprzeczalności**

Proces składania i weryfikacji podpisu elektronicznego



Inny sposób przedstawienia podpisu



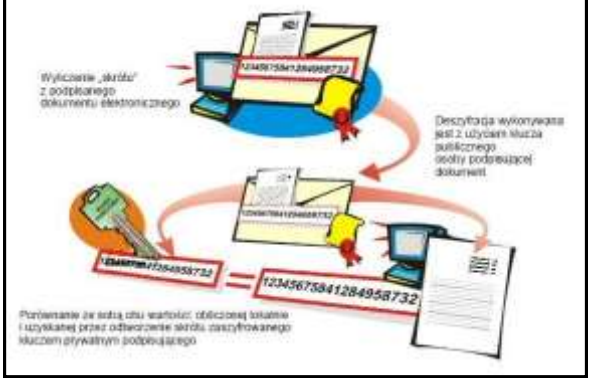
Jeśli chcemy używać kryptografii do generowania podpisu elektronicznego, to musimy dodatkowo zapewnić, że posiadacz klucza prywatnego jest naprawdę tym, za kogo się podaje.

Służy do tego dostawca usług certyfikacyjnych.

Na polskim rynku działają obecnie (2007) trzy kwalifikowane podmioty świadczące usługi certyfikacyjne.

Nazwa podmiotu	Rodzaj oferowanych usług
Krajowa Izba Rozliczeniowa SA	1) Wydawanie kwalifikowanych certyfikatów 2) Znakowanie czasem
Polska Wytwórnia Papierów Wartościowych SA	1) Wydawanie kwalifikowanych certyfikatów 2) Znakowanie czasem
Unizeto Technologies SA	1) Wydawanie kwalifikowanych certyfikatów 2) Znakowanie czasem 3) Weryfikowanie statusu certyfikatów w trybie on-line 4) Walidacja danych 5) Poświadczenie odbioru i przedłożenia 6) Poświadczenie depozytowe 7) Poświadczenie rejestrowe i repozytoryjne

Weryfikacja podpisu dokumentu elektronicznego

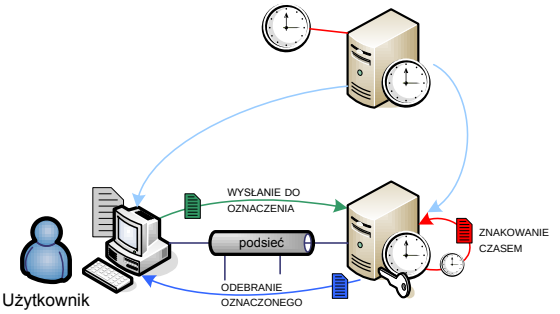


Schemat podpisywania dokumentów elektronicznych

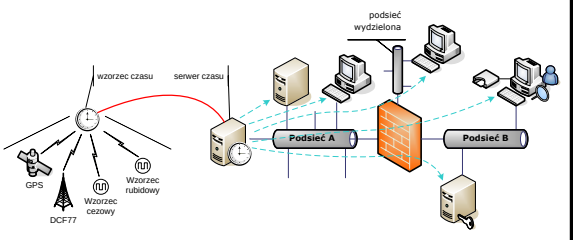
Schemat szyfrowania wiadomości kluczem publicznym

Schemat znakowania wiarygodnym czasem

System znakowania czasem



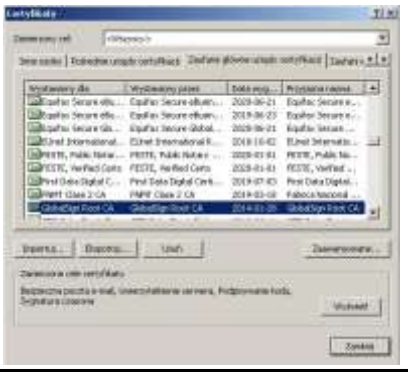
Propagacja czasu w sieci



Informacja ogólne o certyfikacie

Szczegóły certyfikatu

Lista zainstalowanych certyfikatów

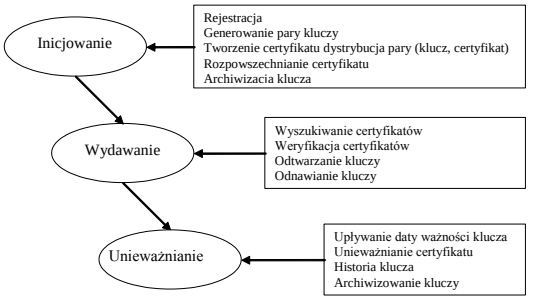


Instalacji certyfikatu osobistego

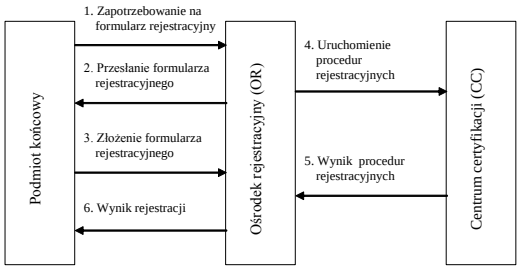
Przykładowa konfiguracja zabezpieczeń MS Outlook z zainstalowanym certyfikatem

Dodatkowe przyciski, służące podpisywaniu i szyfrowaniu wiadomości

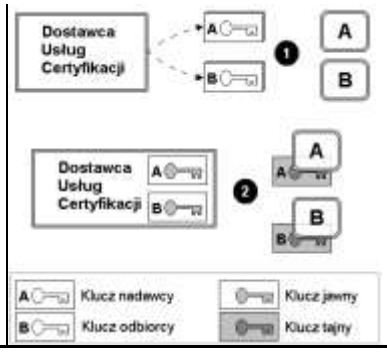
Fazy zarządzania cyklem życia kluczy i certyfikatu



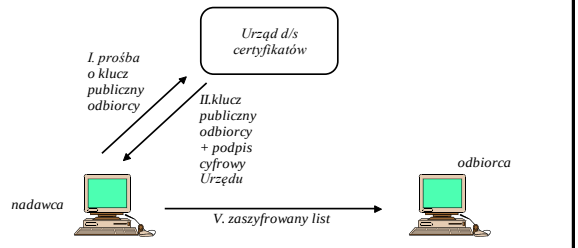
Przykładowy proces inicjowania cyklu życia klucza i certyfikatu



Przydział kluczy publicznych i tajnych przez dostawcę usług certyfikacji

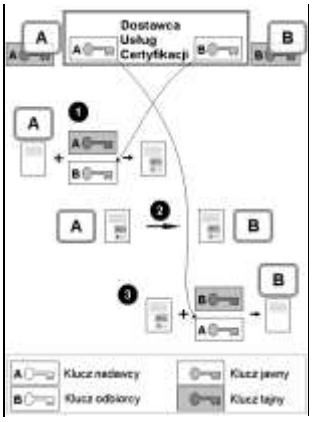


Schemat przetwarzania dokumentu podpisanego elektronicznie



III. weryfikacja podpisu cyfrowego Urzędu
IV. zaszyfrowanie listu kierowanego do odbiorcy

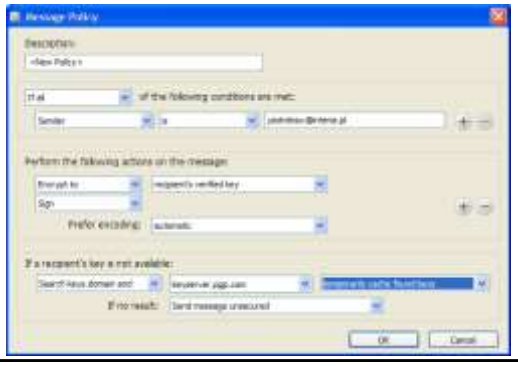
VI. deszyfracja listu (kluczem prywatnym odbiorcy)



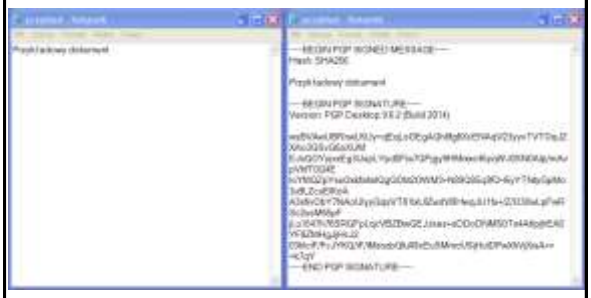
Etapy przesyłania dokumentu zaszyfrowanego za pomocą asymetrycznego systemu krypto-graficznego

Certyfikowany klucz PGP

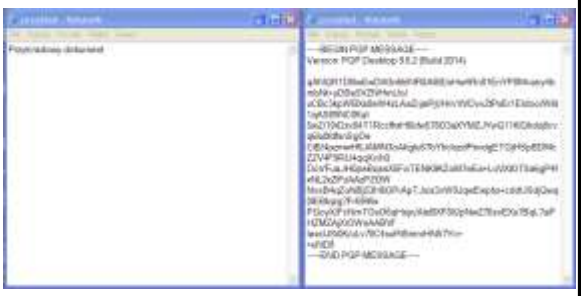
Definiowanie polityki wiadomości



Dokument przed i po podpisaniu PGP

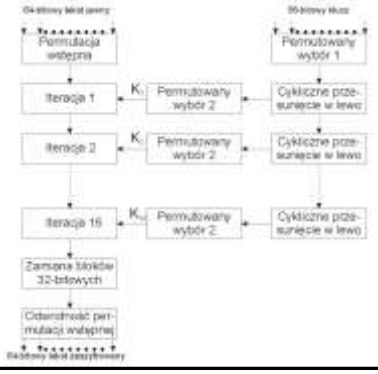


Dokument przed i po zaszyfrowaniu PGP

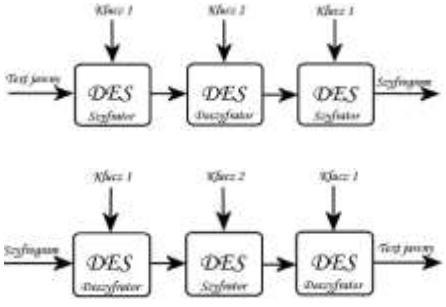


Wybór algorytmów kryptograficznych podczas generowania klucza PGP

Ogólny schemat szyfrowania za pomocą DES

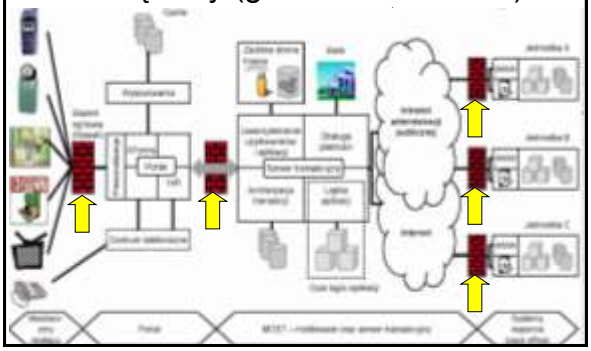


Schemat algorytmu 3DES

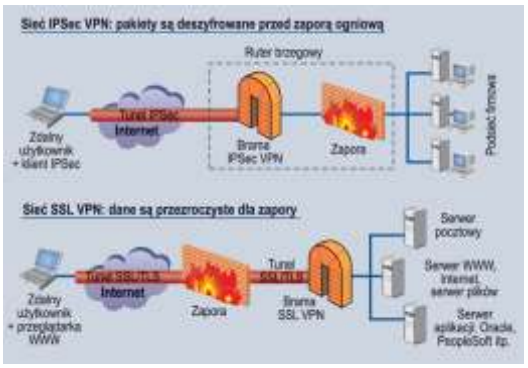


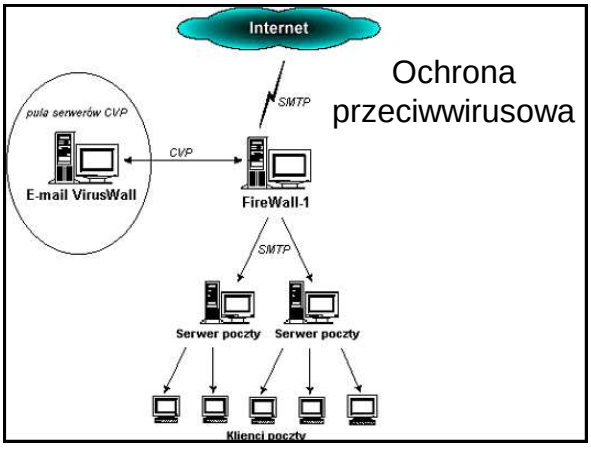
Zagrożenie	Sposoby niwelowania
Transmisja danych	Szyfrowanie połączeń, wirtualne sieci prywatne (VPN ang. *Virtual Private Network*), dedykowane łącza zestawione, podpisy elektroniczne
Autoryzacja	Procedury bezpieczeństwa, hasła dostępu, ograniczenie dostępu do serwera wyłącznie dla ustalonych adresów IP, narzędzia uwierzytelniania –podpis elektroniczny, certyfikaty uwierzytelniające, narzędzia wspomagające –tokeny, listy haseł jednorazowych
Dostępność	Stosowanie urządzeń (UPS ang. *Uninterruptable Power Supply*) podtrzymujących napięcie w przypadku zaniku prądu, dedykowane oprogramowanie blokujące niepożądane połączenia -zapory ogniowe (ang. *firewall*), aktualizacja oprogramowania
Płatności	Wykorzystywanie specjalistycznych serwisów obsługujących płatności w Internecie (np. eCard, PolCard), sprawdzenie kontrahenta w Krajowym Rejestrze Dłużników.

Najczęstszym źródłem zagrożeń dla systemu informatycznego jest świat zewnętrzny (głównie sieci WAN)



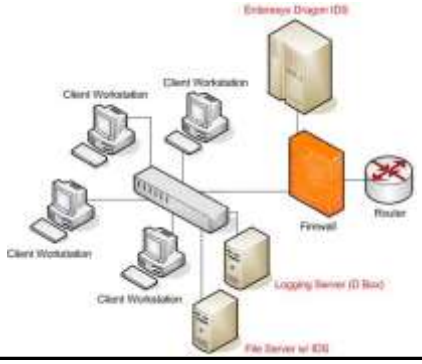
Różne sposoby ustawiania ściany ogniowej



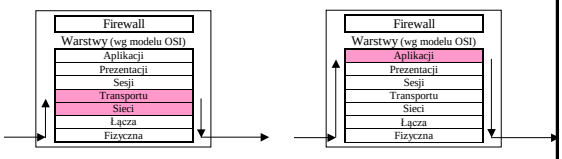


Ochrona przeciwwirusowa

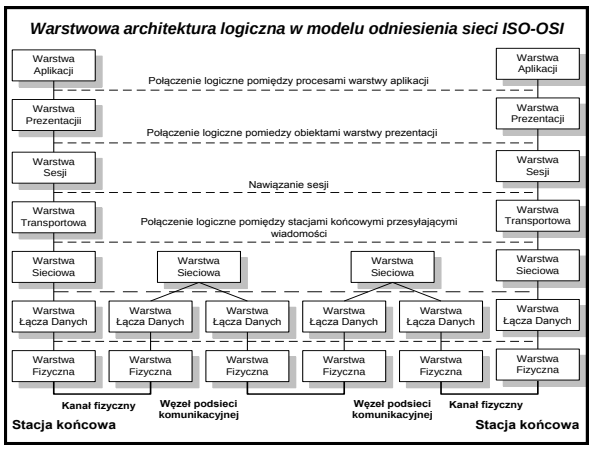
Systemy wykrywania włamań (IDS – Intrusion Detection System)

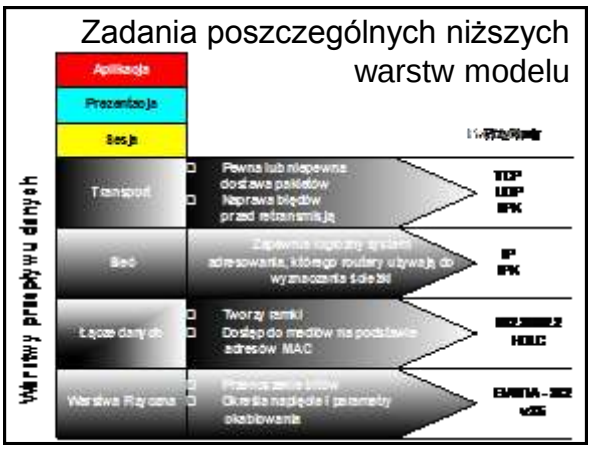


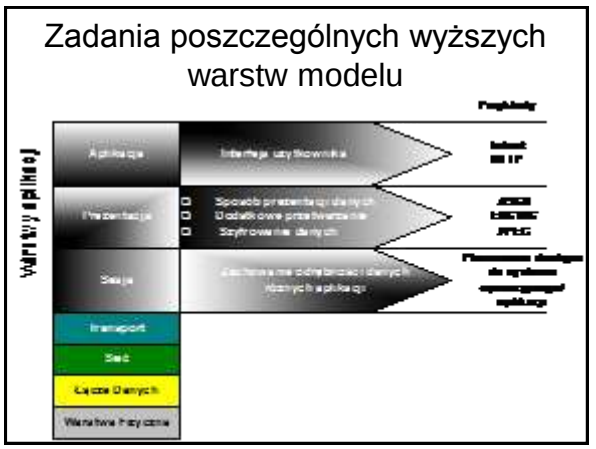
„Ścianę ogniową” można zbudować na poziomie filtracji pakietów albo na poziomie analizy treści informacji

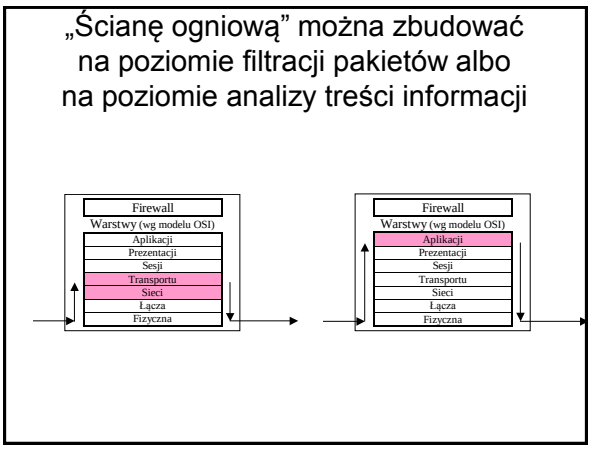


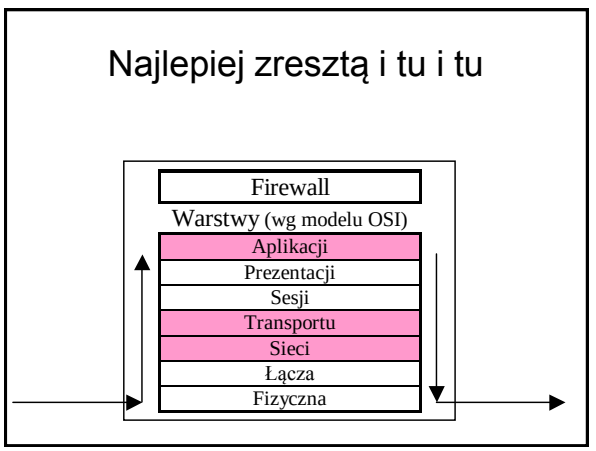
Dygresja:
Siedmiowarstwowy model sieci ISO/OSIS


Warstwowa architektura logiczna w modelu odniesienia sieci ISO-OSI
Warstwa Aplikacji
Połączenie logiczne pomiędzy procesami warstwy aplikacji
Warstwa Prezentacji
Połączenie logiczne pomiedzy obiektami warstwy prezentacji
Warstwa Sesji
Nawiązanie sesji
Warstwa Transportowa
Połączenie logiczne pomiędzy stacjami końcowymi przesyłającymi wiadomości
Warstwa Sieciowa
Warstwa Łącza Danych
Warstwa Fizyczna
Kanał fizyczny
Węzeł podsieci komunikacyjnej
Węzeł podsieci komunikacyjnej
Kanał fizyczny
Stacja końcowa
Stacja końcowa


Zadania poszczególnych niższych warstw modelu
Aplikacja
Prezentacja
Sesja
Transport
Sieć
Łącze danych
Warstwa Fizyczna
Warstwy przepływu danych
TCP
UDP
IPX
IP
IPX
HDLC

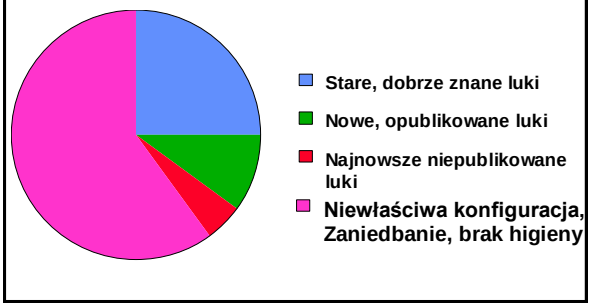

Zadania poszczególnych wyższych warstw modelu
Warstwy aplikacji
Aplikacja
Prezentacja
Sesja
Transport
Sieć
Łącze Danych
Warstwa Fizyczna


„Ścianę ogniową” można zbudować na poziomie filtracji pakietów albo na poziomie analizy treści informacji
Firewall
Warstwy (wg modelu OSI)
Aplikacji
Prezentacji
Sesji
Transportu
Sieci
Łącza
Fizyczna
Firewall
Warstwy (wg modelu OSI)
Aplikacji
Prezentacji
Sesji
Transportu
Sieci
Łącza
Fizyczna

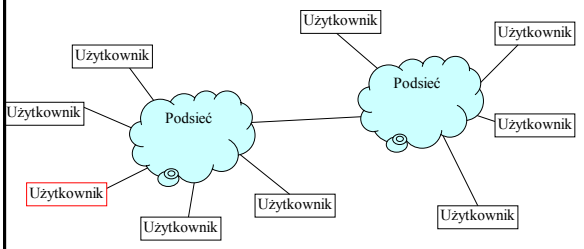

Najlepiej zresztą i tu i tu
Firewall
Warstwy (wg modelu OSI)
Aplikacji
Prezentacji
Sesji
Transportu
Sieci
Łącza
Fizyczna


Koszty ponoszone na zabezpieczenia są zależne od rodzaju stosowanej polityki bezpieczeństwa.
$ Koszty incydentu
$ Koszty zabezpieczeń
$ Koszty zabezpieczeń
Polityka reaktywna: zabezpieczenia są wprowadzane gdy wydarzy się incydent wskazujący na to, że w systemie starych zabezpieczeń jest luka
Polityka pro-aktywna: zabezpieczenia są wprowadzane zanim wydarzy się incydent wskazujący na to, że w systemie starych zabezpieczeń jest luka

Statystyka rzeczywistych przyczyn włamań do systemów informatycznych

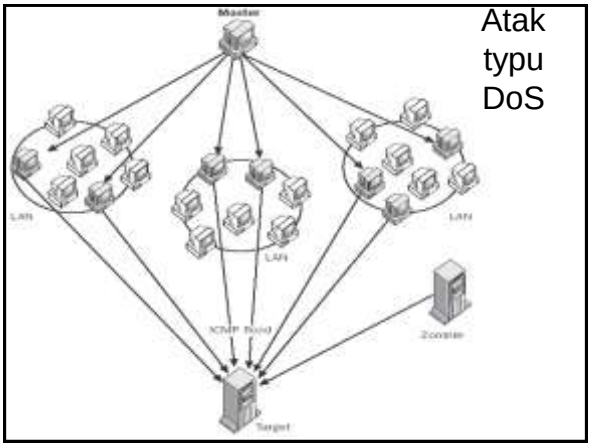


Najczęściej źródłem i przyczyną problemu jest nieostrożny użytkownik jednej z podsieci

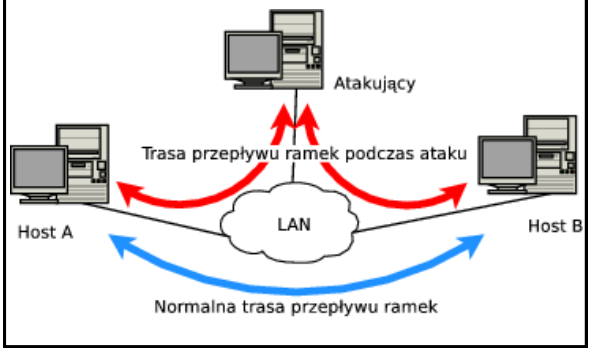


Przykładowe formy zagrożeń

Atak typu DoS



Spoofing



Każdy projekt informatyczny jest przedsięwzięciem wysokiego ryzyka

OBSZAR RYZYKA	SZCZEGÓŁOWE ŹRÓDŁA RYZYKA
Otoczenie społeczno-ekonomiczne	Podejście do TI
	Niespójny system gospodarczy i prawny
	Zmiany sytuacji na rynku
	System edukacji
	Brak standardów
	Niska kultura informacyjna
Otoczenie technologiczne	Niedorozwój telekomunikacji
	Brak standardów przesyłania danych
	Przewaga techniki mikrokomputerowej
Organizacja	Nieokreślone cele oraz brak wizji i strategii
	Niechęć, niezdolność do zmiany
	Relacje władzy i własności
	Brak współpracy kierownictwa i użytkowników
	Brak standardów i procedur
	Nagłe zmiany struktury
	Zatrudnienie i podnoszenie kwalifikacji
	Nierozpoznane umiejętności firmy
	Niesprawność kontroli
	Niesprawność zarządzania TI
Twórcy SI	Nieumiejętność pracy zespołowej
	Podejście do zamierzenia
	Nieznajomość metod, technik i narzędzi
Projekt	Obszerność i złożoność zadania projektowego
	Wycinkowe projektowanie i oprogramowywanie SI
	Brak business planu

Źródła ryzyka i zagrożenia

ŹRÓDŁA RYZYKA	ZAGROŻENIA
Podejście do TI	Strach przed zmianą Nieumiejętność celowego zakupu i wykorzystania TI
Niespójny system gospodarczy i prawny Zmiany sytuacji na rynku	Zmiana celów i zadań organizacji Konieczność częstych zmian oprogramowania Niedostosowanie do wymogów klientów Niewydolność systemu
System edukacji	Nieumiejętność pracy zespołowej Nieznajomość zarządzania Nieumiejętność wykorzystania narzędzi

Źródła ryzyka i zagrożenia – cd.

Brak standardów	Niespójność danych Czasochłonność wprowadzania i uzyskiwania danych
Niska kultura informacyjna	Nieskuteczność zabezpieczeń Nieumiejętność wykorzystania większości funkcji TI
Niedorozwój telekomunikacji	Opóźnienia w przesyłaniu danych i ich przekłamania Utrudniony dostęp do informacji Wysokie koszty eksploatacji
Brak standardów przesyłania danych	Pracochłonność opracowywania danych Nieczytelność danych Niewielkie możliwości wykorzystania danych
Przewaga techniki mikrokomputerowej	Nieznajomość innych technologii Niedopasowanie technologii do potrzeb Duże wydatki na TI

Źródła ryzyka i zagrożenia – cd.

Nieokreślone cele oraz brak wizji i strategii	Nieokreślone cele systemu informacyjnego Komputeryzowanie istniejących procedur Nieuwzględnienie potrzeb wynikających ze wzrostu firmy
Niechęć, niezdolność do zmiany	Wykorzystywanie TI jako kalkulatora Brak poczucia celowości zastosowań TI Niezgodność zastosowań z organizacją
Relacje władzy i własności	Trudności w ustaleniu potrzeb informacyjnych Nieustalona odpowiedzialność za zamierzenie Utrudnienia w sterowaniu projektem
Brak współpracy kierownictwa i użytkowników	Niemożliwość sprecyzowania potrzeb Niedopasowanie SI do rzeczywistych potrzeb Opóźnienia projektu i przekroczenie budżetu

Źródła ryzyka i zagrożenia – cd.

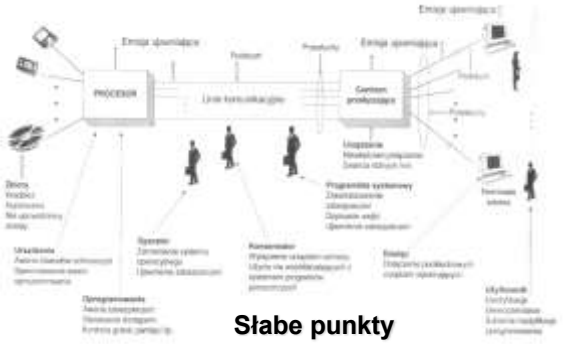
Brak standardów i procedur	Dominacja TI nad organizacją Nieumiejętność określenia zadań
Nagłe zmiany struktury	Odchodzenie użytkowników i zmiany potrzeb Nieustalone role organizacyjne Doraźne zmiany procedur i standardów
Zatrudnienie i podnoszenie kwalifikacji	Nieznajomość, brak zrozumienia i obawa przed TI Nieumiejętność formułowania i rozwiązywania problemów Brak motywacji i zainteresowania użytkowników
Nierozpoznane umiejętności firmy	Nietrafne zastosowania zakłócające procedury Nieprzydatność, niefunkcjonalność narzędzi

Źródła ryzyka i zagrożenia – cd.

Niesprawność kontroli	Niesprecyzowane potrzeby dotyczące kontroli Celowe omijanie mechanizmów kontrolnych
Niesprawność zarządzania TI	Nieumiejętność planowania i niecelowe wydawanie środków Nietrafione zakupy wyposażenia i oprogramowania Zaniechanie planowania i egzekwowania efektów
Nieumiejętność pracy zespołowej	Zakłócenia w wykonywaniu prac Błędna strukturyzacja systemu Niespójne, błędne rozwiązania
Podejście do zamierzenia	Zaniechanie lub powierzchowność analizy Pomijanie badania pracy Dostosowanie użytkowników do TI, a nie SI do potrzeb „Komputeryzacja” zamiast zmiany

Źródła ryzyka i zagrożenia - koniec

Nieznajomość metod, technik i narzędzi	Stosowanie metod znanych zamiast potrzebnych Niekompletna analiza, niespójna specyfikacja Niewykorzystywanie możliwości narzędzi Nietrafne oceny kosztów, efektów i czasu trwania projektu
Obszerność i złożoność zadania projektowego	Brak analizy problemów Trudność opanowania złożoności, nietrafna strukturyzacja
Wycinkowe projektowanie i oprogramowywanie SI	Niewłaściwa kolejność opracowywania i wdrażania modułów Niespójność modułów systemu
Brak business planu	Nieświadomość celów oraz kosztów i efektów Nieliczenie się z kosztami, pomijanie oczekiwanych efektów



Słabe punkty sieci komputerowych

Postępowanie w razie wykrycia zagrożenia z zewnątrz

1. **PROTECT AND PROCEED**

   (chroń i kontynuuj)

2. **PURSUE AND PROSECUTE**

   (ścigaj i oskarż)

PROTECT AND PROCEED

Strategię tą obierają organizacje, w których:

1. Zasoby nie są dobrze chronione
2. Dalsza penetracja mogłaby zakończyć się dużą stratą finansową
3. Nie ma możliwości lub woli ścigania intruza
4. Nieznane są motywy włamywacza
5. Narażone są dane użytkowników
6. Organizacja nie jest przygotowana na działania prawne w wypadku strat doznanych przez użytkowników

PURSUE AND PROSECUTE

W myśl strategii pursue and prosecute pozwala się intruzowi kontynuować niepożądane działania dopóki się go nie zidentyfikuje, aby został oskarżony i poniósł konsekwencje.

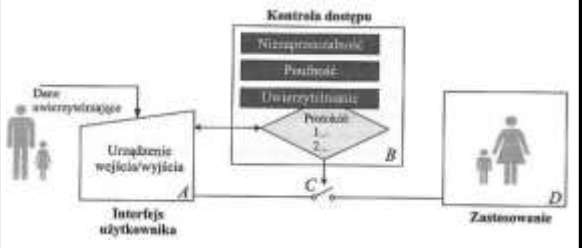
Jest to strategia o wiele bardziej ryzykowna!

Ważna jest weryfikacja ludzi pragnących się znaleźć wewnątrz systemu (autoryzacja i autentykacja)

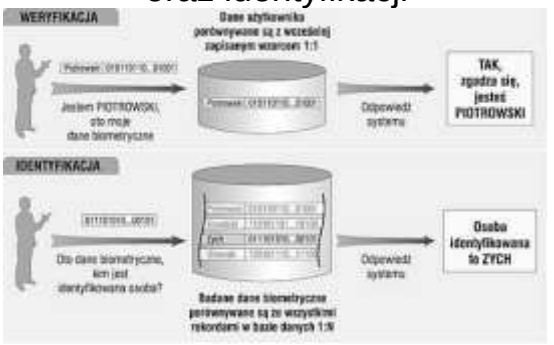
Weryfikacja może się odbywać w oparciu o trzy rodzaje kryteriów:

- *„coś, co masz”* – klucze, karty magnetyczne
- *„coś, co wiesz”* – PIN, hasła, poufne dane
- *„coś, czym jesteś”* – metody biometryczne

Ochrona kontroli dostępu



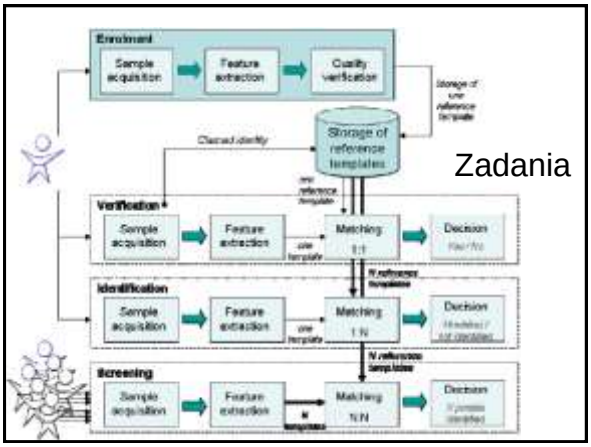
Schematy procesów weryfikacji oraz identyfikacji



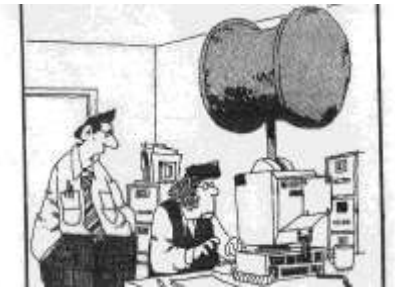
Poziomy bezpieczeństwa w systemach kontroli dostępu

Identyfikacja typu „coś co wiesz”

Zadania



Najwygodniejsze dla konstruktorów systemów informatycznych są metody oparte na hasłach lub PIN



Identyfikacja typu „coś co masz”

tokeny

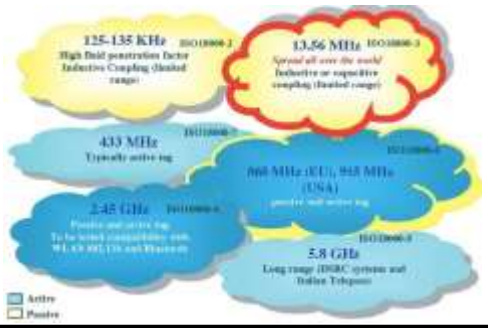
Sprawdzanie kart magnetycznych lub chipowych

Technologia RFID (*Radio Frequency Identification*)

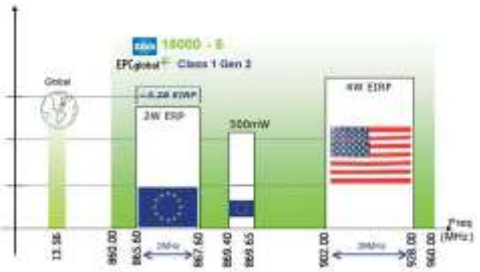
Passive RFID tags

Active RFID tags

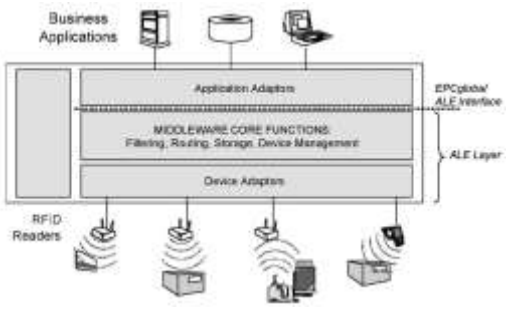
Wykorzystanie różnych pasm częstotliwości



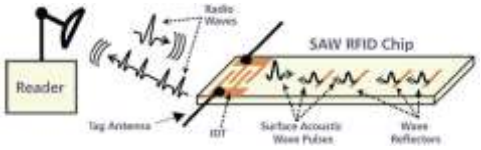
Podstawowe standardy



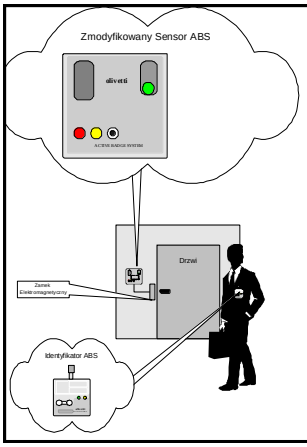
ALE (*Application Level Events*) Layer



Identyfikator typu SAW (*Surface Acoustic Wave*)

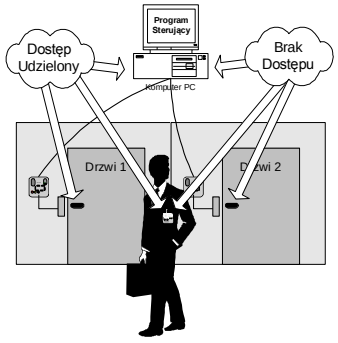


RFID - Identyfikacja radiowa: a), b), c), d), e) – identyfikatory, f) czytnik



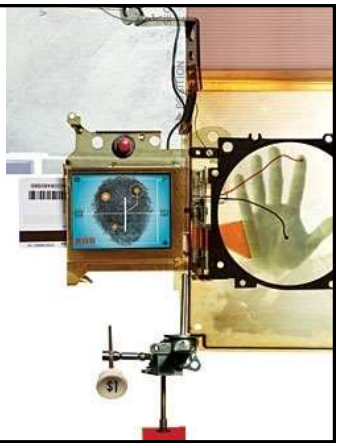
Pozornie wygodne dla użytkownika są metody oparte na stosowaniu identyfikatora, którego stan może być sprawdzany nawet zdalnie

Ta sama osoba może mieć wtedy dostęp do jednych zasobów i brak dostępu do innych zasobów



Jednak identyfikator można zgubić, zniszczyć, albo może on zostać skradziony

Najwygodniejsze dla użytkownika są metody **biometryczne**, ale wymagają one stosowania skomplikowanej i kosztownej aparatury

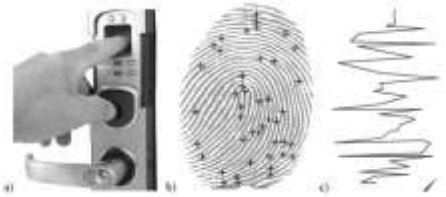


Tymi metodami da się zabezpieczać dostęp do różnych systemów oraz usług

Skanowanie kształtu dłoni

Przykład zabezpieczenia biometrycznego:

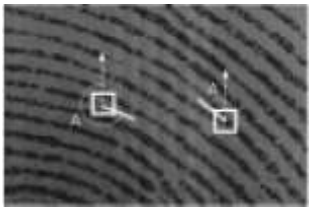
a) zamek biometryczny, b) punkty charakterystyczne na odcisku palca, c) krzywa łącząca te punkty.



Cyfrową analizę odcisków palców z upodobaniem stosują Amerykanie

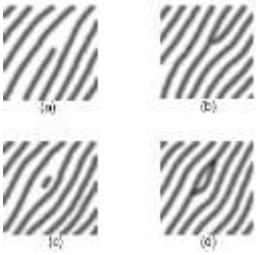
Sposób automatycznej analizy odcisku palca

Do najbardziej znanych metod biometrycznych należy skanowanie odcisku palca i ocena jego szczegółów

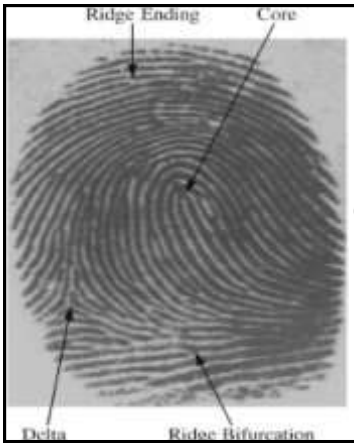


Wzorce bruzd wszystkich palców mają drobne szczegóły nazywane minucjami, które odróżniają jeden odcisk od drugiego

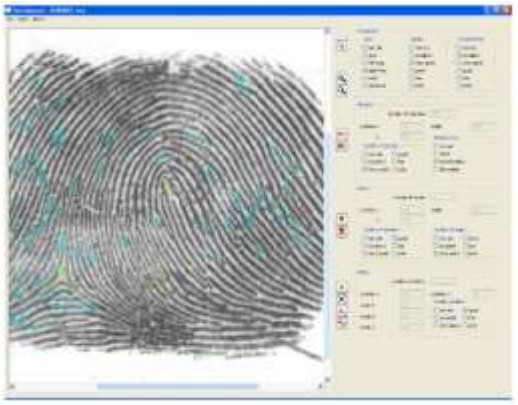
Przykładowe minucje



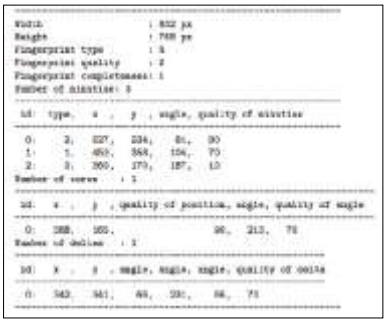
. (a) Ridge ending (b) Ridge bifurcation
(c) Short ridge (d) Ridge enclosure



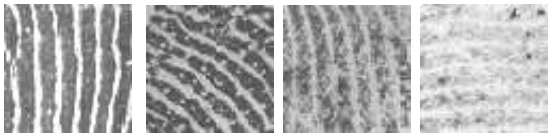
Zaletą jest tu łatwe pozyskiwanie danych oraz dobrze ustalone cechy charakterystyczne odcisków



Automatycznie generowany kod odcisku palca

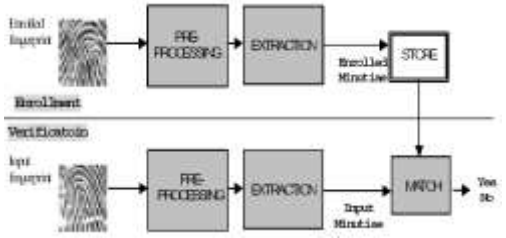


Wadą jest to, że obrazy odcisków palców bywają bardzo złej jakości

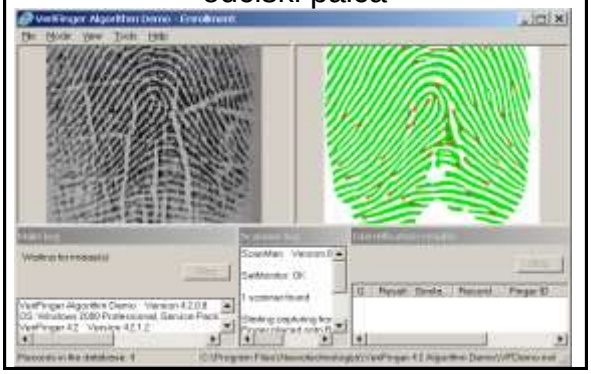


Przy korzystaniu z odcisków palców jako z kryterium identyfikacji osób trzeba sobie zdawać sprawę z konieczności oczyszczania komputerowego rejestrowanych obrazów

Weryfikacja osoby na podstawie odcisku palca polega na porównaniu minucji odczytanych na aktualnie wprowadzonym odcisku oraz minucji dla wzorca zarejestrowanego w bazie osób zaakceptowanych.



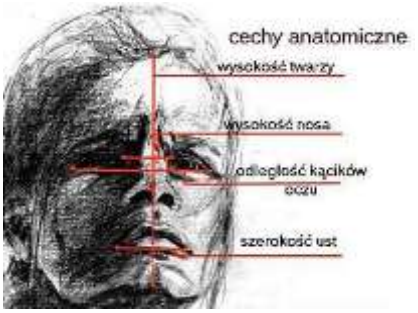
Działanie programu analizującego odciski palca



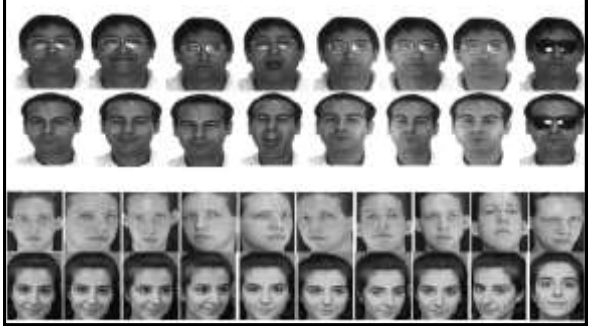
Rozpoznawanie twarzy

Ilustracja problemów:
- **różnic oświetlenia (a),**
- **pozy (b)**
- **wyrazu twarzy (c)**

Podstawowe szczegóły geometrii rozmieszczenia cech anatomicznych ludzkiej twarzy

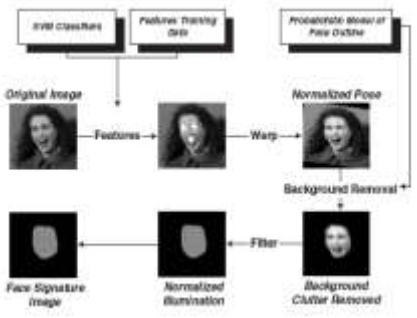


Twarze o różnych wyrazach

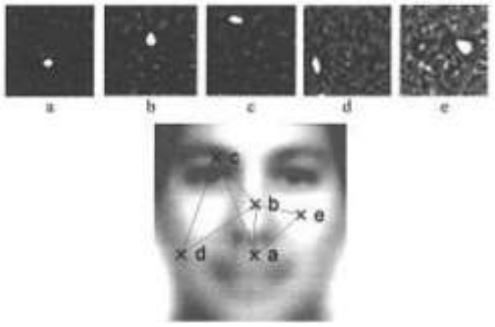


Szkic algorytmu rozpoznawania

Kolejne przekształcenia obrazu



Rozpoznawanie twarzy oparte na cechach: (a-e) lokalne wykrywanie i lokalizacja cech.

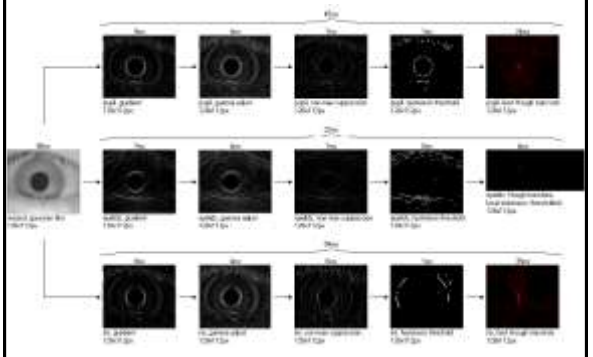


Duże nadzieje wiąże się też aktualnie z możliwościami identyfikacji poprzez analizę obrazu tęczówki oka

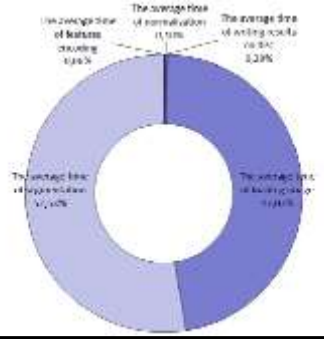
Pierwszy program do identyfikacji ludzi na podstawie tęczówki oka przedstawił John Daugman w 1993 roku.

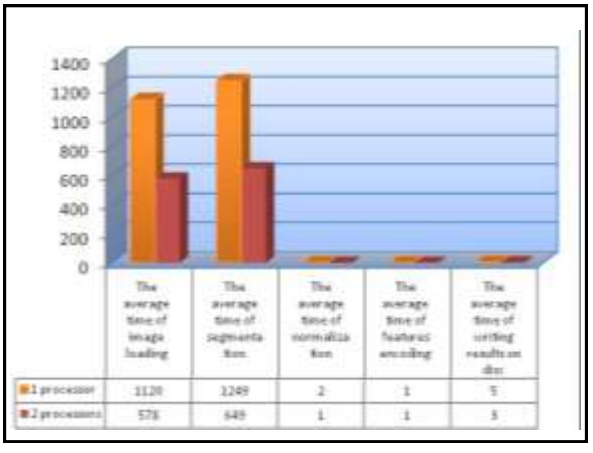
Niestety, opatrzył on swoją metodę („Iriscode") patentem , co zahamowało rozwój tej dziedziny na 10 lat.

Przetwarzanie wstępne

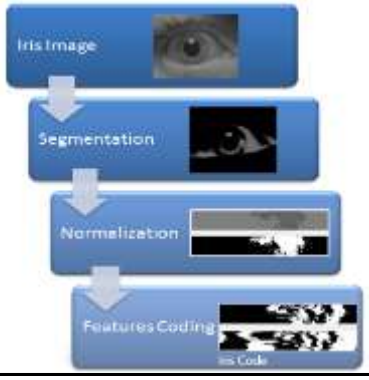


Większą część czasu zabierają czynności przygotowawcze

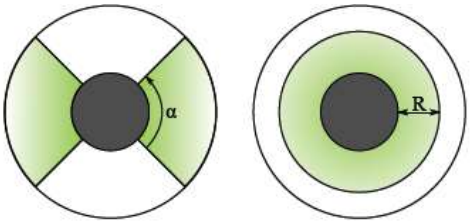




Etapy pozyskiwania kodu tęczówki oka

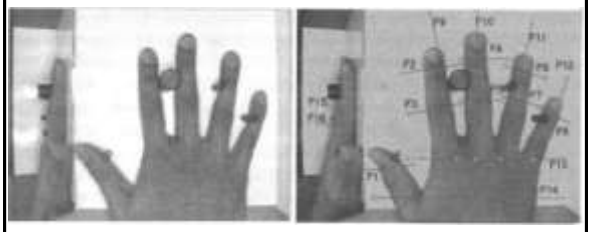


Konieczne jest wydzielenie fragmentu obrazu do analizy



Ustalanie kodu tęczówki oka

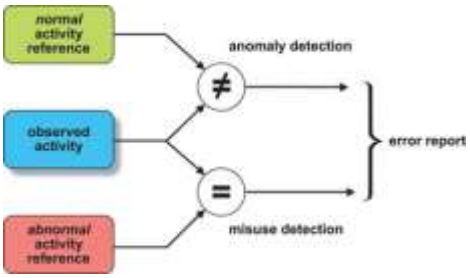
urządzenia do odczytu parametrów dłoni



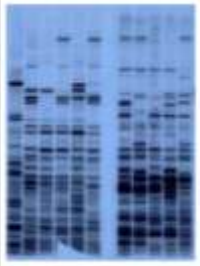
Kostki dłoni

- Jedną z rozwijających się metod jest biometria kostek dłoni (knuckle biometrics).
- Nazywana także **FKP** (finger-knuckle-print).
- Modalność ludzkiej dłoni

Identyfikacja na podstawie cech behawioralnych



Liczne zalety ma identyfikacja oparta o badanie DNA



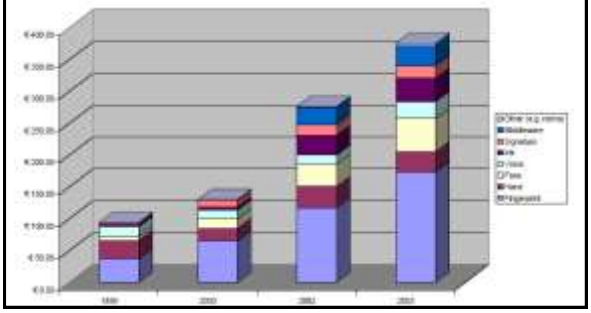
DNA fingerprint image

DNA profile representation

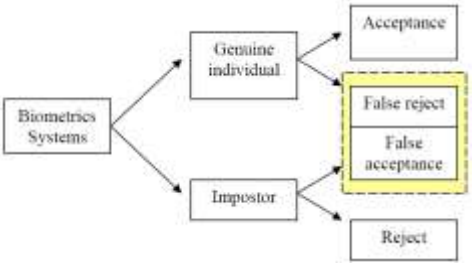
Biometryczne metody identyfikacji osób w systemach informatycznych o wysokich wymaganiach bezpieczeństwa ogólna charakterystyka

Biometric trait \ Pillars	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
DNA	H	H	H	L	H	L	L

Przychody z tytułu eksploatacji różnych biometrycznych metod identyfikacji



Przy pomiarach biometrycznych można się spodziewać dwojakiego rodzaju błędów



Popularność różnych metod

System kontroli bezpieczeństwa informatycznego dużej firmy

Bezpieczeństwo systemów informatycznych i prawo

Do podstawowych aktów prawnych, które mają wpływ na bezpieczeństwo i ochronę danych w systemach informatycznych polskich przedsiębiorstw należą:

- Ustawa *Kodeks Karny* [k.k. 1997],
- Ustawa o *rachunkowości* [1994],
- Ustawa o *ochronie danych osobowych* [ustawa ODO 1997],
- Ustawa o *ochronie informacji niejawnych* [ustawa OIN 1999],
- Ustawa o *prawie autorskim i prawach pokrewnych* [ustawa PAiPP 1994],
- Ustawa o *systemie ubezpieczeń społecznych* [ustawa SUS 1998],
- Ustawa o *podpisie elektronicznym* [ustawa PE 2001],
- Ustawa o *zwalczaniu nieuczciwej konkurencji* [ustawa ZNK 1993].

Czyn podlegający karze	Podstawa	Zagrożenie karą
Ujawnienie informacji wbrew zobowiązaniu	Art. 266 §1	Grzywna, ograniczenie lub pozbawienie wolności do lat 2
Niszczenie dokumentów	Art. 276	Grzywna, ograniczenie lub pozbawienie wolności do lat 2
Fałszerstwo dokumentów	Art. 270 §1	Grzywna, ograniczenie lub pozbawienie wolności od 3 m-cy do lat 5
Niszczenie lub zmiana istotnej informacji na nośniku papierowym	Art. 268 §1	Pozbawienie wolności do lat 3
Nieuprawnione uzyskanie i podsłuch informacji	Art. 267 §1-2	Grzywna, ograniczenie lub pozbawienie wolności do lat 2
Sabotaż komputerowy		
- skierowany przeciw bezpieczeństwu kraju	Art. 269 §1-2	Pozbawienie wolności od 6 m-cy do lat 8
- w celu osiągnięciu korzyści majątkowej	Art. 287 §1	Pozbawienie wolności od 3 m-cy do lat 5
Nielegalne uzyskanie programów	Art. 278 §1-2	Pozbawienie wolności od 3 m-cy do lat 5
Paserstwo programów	Art. 291 §1	Pozbawienie wolności od 3 m-cy do lat 5
Oszustwo komputerowe	Art. 287 §1	Pozbawienie wolności od 3 m-cy do lat 5
Oszustwo telekomunikacyjne	Art. 285 §1	Pozbawienie wolności do lat 3
Szpiegostwo przy użyciu komputera	Art. 130 §3	Pozbawienie wolności od 6 m-cy do lat 8

Analiza i projektowanie systemów informacyjnych

Problem bezpieczeństwa

informatyka stosowana