Zaufanie w systemach informatycznych

Paweł Krawczyk

Kontakt z autorem:

pawel.krawczyk@hush.com
Tel. +48-602-776959

Konspekt

- Kryteria zaufania
- Analiza ryzyka
- Funkcje bezpieczeństwa
- Zaufanie oparte o reputację
- Etyka bezpieczeństwa

Zaufanie do systemu informatycznego

- Zaufanie, wiarygodność systemu informatycznego
  - Przekonanie, że dany system spełnia swoje zadanie zgodnie z określonymi kryteriami – np. polityką bezpieczeństwa (PN-I-02000:2002 pkt 3.2.017)
- Warunek konieczny: **kryteria**

Jak opisać kryteria?

- Polityki (policies)
- Procedury (procedures)
- Standardy (standards)
- Minimalne wymagania (baselines)
- Wytyczne (guidelines)

Polityki bezpieczeństwa

Polityki bezpieczeństwa

- Wysokopoziomowe
- Strategiczne
- Wytyczają kierunek
- Stabilne
- Zawierają wynik decyzji politycznych
  - Np. *"Priorytetem organizacji jest..."*
    - ***albo*** *"...maksymalizacja zysku za cenę ryzyka"*
    - ***albo*** *"...bezpieczeństwo i stabilność"*

Implementacja polityk

- **Minimalne wymagania**
  - Określają ilościowo wymagany poziom siły mechanizmów bezpieczeństwa (długość hasła, długość kluczy szyfrujących, częstość zmiany haseł)
- **Wytyczne**
  - Mogą mieć charakter niewiążący, zawierają zalecenia (*recommendations*) i najlepsze praktyki postępowania (*best practices*)

Implementacja polityk

- **Standardy**
  - Opisują obecność konkretnych mechanizmów bezpieczeństwa (hasła, szyfrowanie danych, zapory sieciowe)
- **Procedury**
  - Krok po kroku opisują sposób wykonywania określonych zadań w sposób bezpieczny (np. postępowanie z dokumentami wrażliwymi)

Częste błędy w tworzeniu polityk

- Sprzeczne cele (oksymorony)
  - *"maksymalizacja zysku za cenę ryzyka, bezpieczeństwo oraz stabilność"*
- Przemieszanie polityk z procedurami i standardami
  - Trudność zmian lub zbyt częste zmiany
  - Zbyt obszerne, nieczytelne i nieprzyswajalne
- Tworzenie polityk "na zapas" i myślenie życzeniowe
  - Zbyt dużo priorytetów = brak priorytetów

Nierealne cele polityk

- Patologia pierwsza
  - Podniesienie poziomu bezpieczeństwa tak wysoko, że zanika zysk krótko- i długoterminowy
  - Przykład: e-faktury, podpis kwalifikowany
- Patologia druga
  - Ustalenie celów bezpieczeństwa tak wysoko, że mają one charakter "myślenia życzeniowego"

Czy więcej bezpieczeństwa to lepiej?

- Bezpieczeństwo służy maksymalizacji zysku
  - Poświęcamy krótkoterminowy zysk lub wydajność w celu uniknięcia długoterminowych strat
  - Dbamy o zysk długoterminowy
- Wartość graniczna bezpieczeństwa
  - 100% bezpieczeństwa = 0% działania
- Racjonalna polityka bezpieczeństwa
  - Jest dostosowana do profilu ryzyka tej konkretnej organizacji
  - Przyczynia się do realizacji jej celów

Metody racjonalizacji polityk

- Rozbudowa na podstawie
  - Potrzeb wewnętrznych
  - Wymagań zewnętrznych
    - Prawo, standardy branżowe, wymagania klientów, przewaga konkurencyjna
- Uporządkowanie przy pomocy analizy ryzyka
  - Jakościowa, ilościowa
- Racjonalizacja zabezpieczeń
  - Analiza kosztów i zysków (*cost-benefit*)
  - ROI = Return on Investment
  - ROSI = Return on Security Investment

Analiza ryzyka

Analiza ryzyka

- Racjonalny i obiektywny opis ryzyk organizacji
  - Umożliwia ich racjonalne **kontrolowanie**
- Analiza jakościowa (*qualitative*)
  - Wysokie/średnie/niskie
- Analiza ilościowa (*quantitative*)
  - Każde ryzyko ma wartość finansową

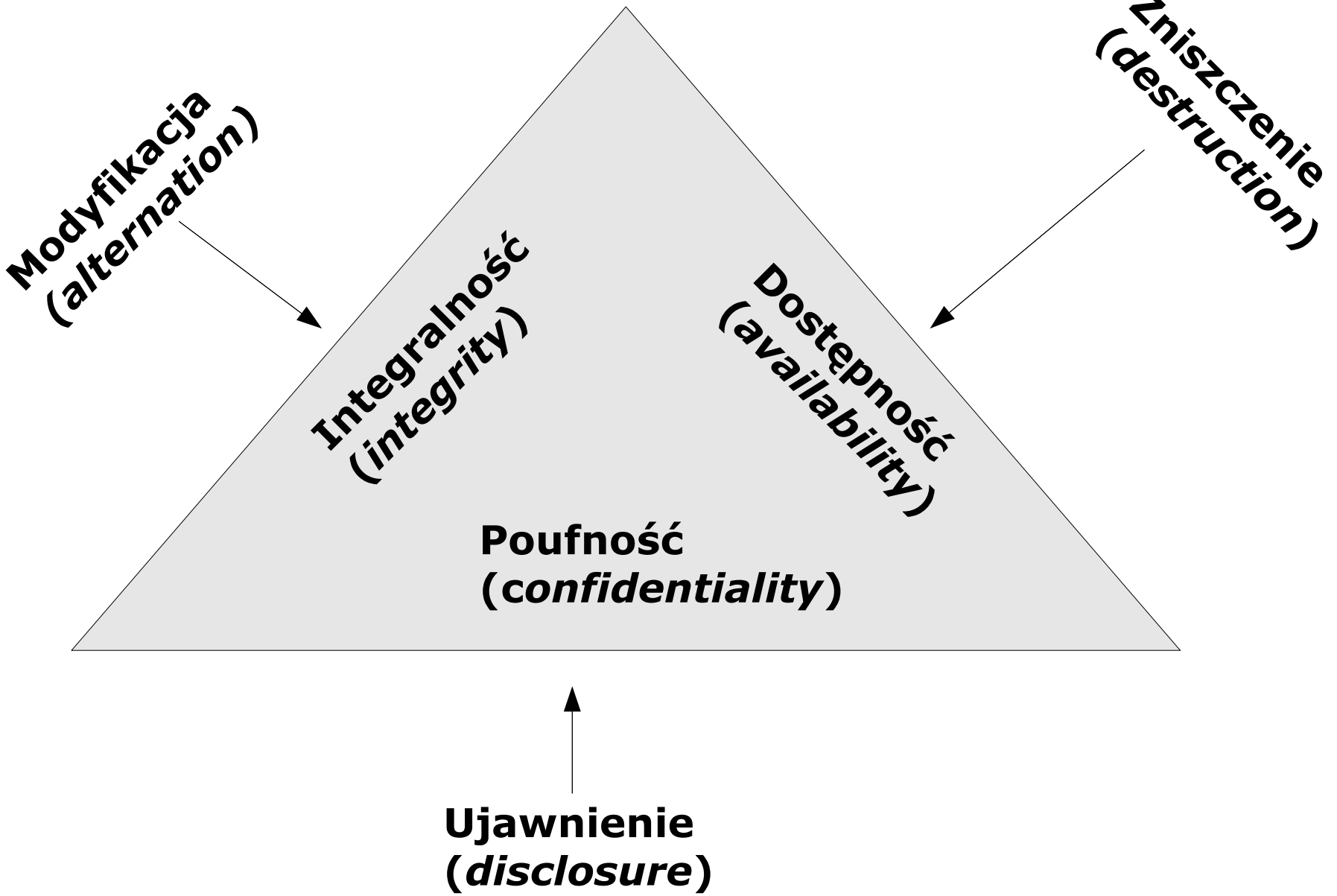
Terminologia

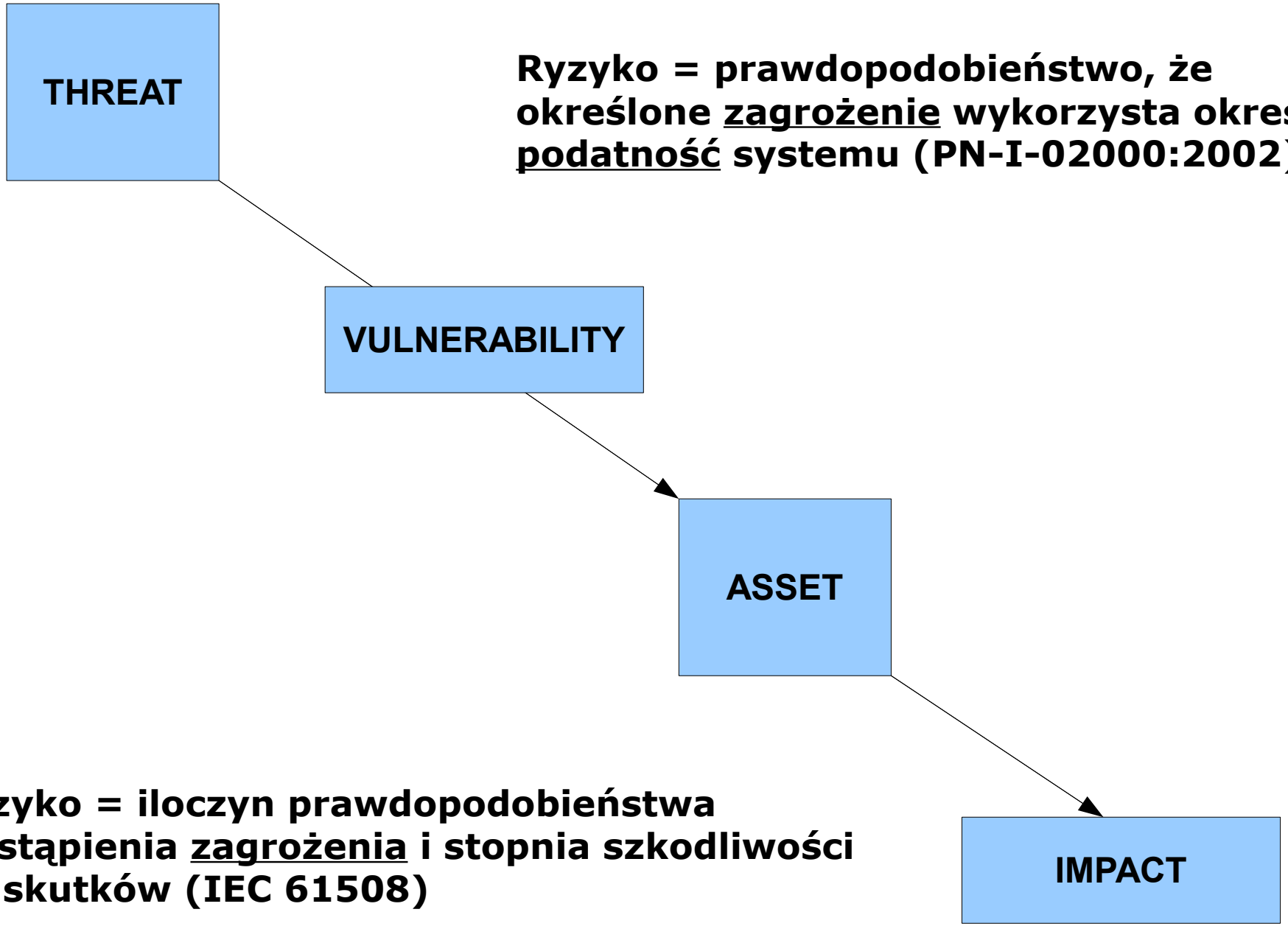
- Zasoby chronione, aktywa (*assets*)
- Zagrożenie (*threat*)
- Czynnik zagrożenia (*threat agent*)
- Podatność (*vulnerability*)
- Narażenie na ryzyko (*exposure to risk*)
- Ryzyko (*risk*)
- Środki bezpieczeństwa, zabezpieczenia (*countermeasures*)
- Szkoda (*impact*)

Wyjaśnienia terminologii

- Zagrożenia
  - Niezależne od nas, nie mamy na nie wpływu
  - Nie muszą nas dotyczyć, jeśli nie istnieje **czynnik** (*agent*)
- Podatność
  - Istnieje jeśli odpowiada **czynnikowi zagrożenia** i nie istnieje odpowiednie **zabezpieczenia**
  - Na podatność mamy wpływ
- Ryzyko
  - Istnieje, jeśli istnieje **podatność**

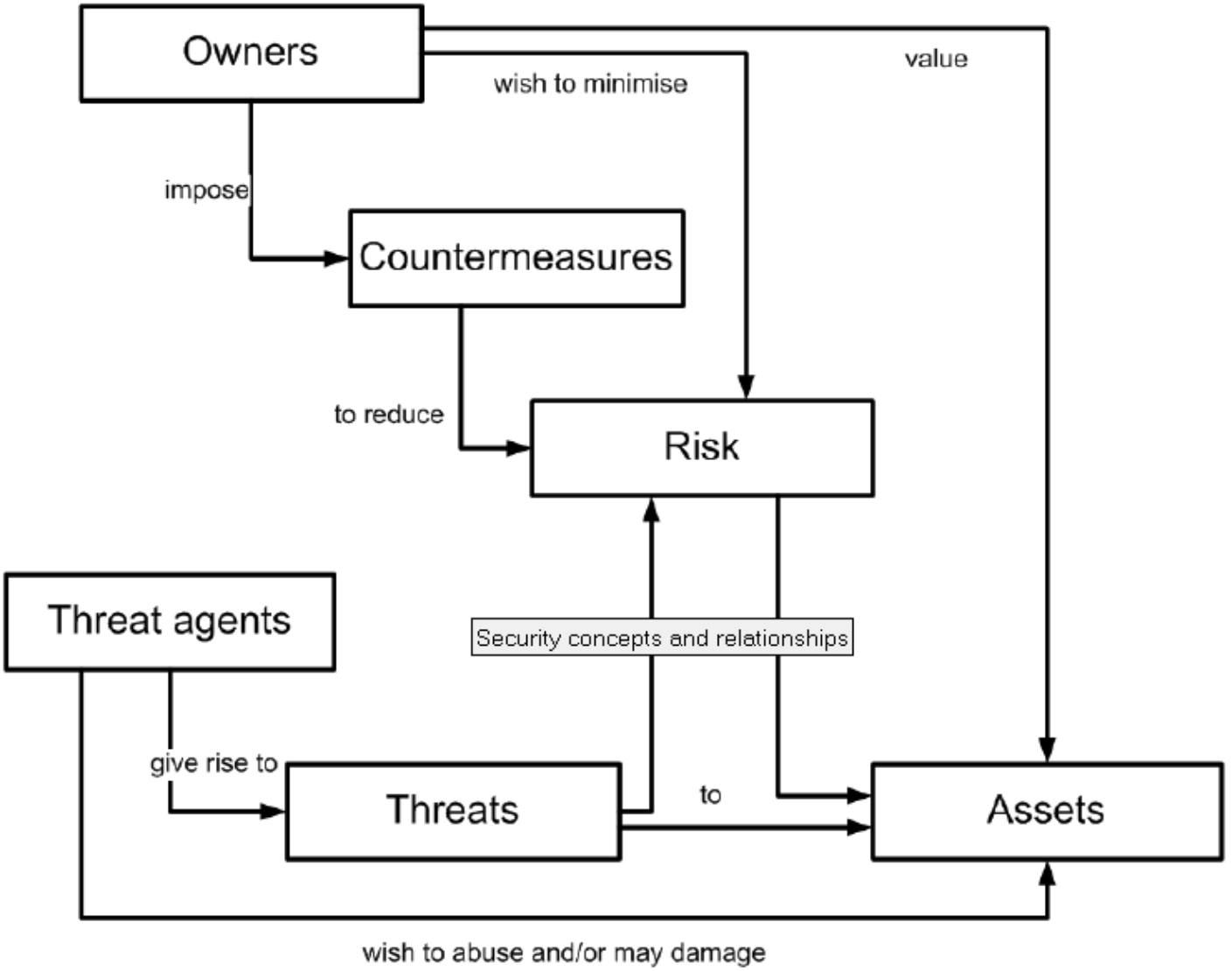
Trójkąt C.I.A.


Modyfikacja
(*alternation*)
Zniszczenie
(*destruction*)
Integralność
(*integrity*)
Dostępność
(*availability*)
Poufność
(*confidentiality*)
Ujawnienie
(*disclosure*)



Ryzyko = prawdopodobieństwo, że określone zagrożenie wykorzysta określoną podatność systemu (PN-I-02000:2002)

Ryzyko = iloczyn prawdopodobieństwa wystąpienia zagrożenia i stopnia szkodliwości jej skutków (IEC 61508)



Źródło: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009

Wycena ryzyka w praktyce #1

- Określenie SLE (*Single Loss Expectancy*)
  - SLE = AV x EF
    - AV (Asset Value) [$]
    - EF (Exposure Factor) [%]
- Przykład
  - Zysk z jednego dnia emisji reklam średnio 1000 zł
    - AV = 1000zł
  - Ciągłość pracy systemu 98%
    - To nie jest EF!
    - System przestaje działać → reklamy się nie wyświetlają → EF=100%

Wycena ryzyka w praktyce #2

- Agregacja w skali rocznej
  - AV_{roczny} = AV x 365 dni = 365'000 zł
- ARO (*Annual Rate of Occurence*)
  - ARO = 2% (100%-98%) = 7,3 dnia w roku
- ALE (Annual Loss Expectancy)
  - ALE = SLE x ARO = 7300 zł
- Obiektywna miara ryzyka w skali roku
  - Zagrożenie – 2% przerwa w pracy systemu

Wycena ryzyka w praktyce #3

- ALE jest wskazówką do dalszych decyzji
- Jak postąpić z danym ryzykiem?
  - Jeśli ograniczać, to ile wydać na zabezpieczenie?
    - Wartość zabezpieczenia: ALE – ALE_{zabezp} – $KOSZT_{zabezp}$
- Dodatkowe narzędzia – ROI i ROSI

$$ROSI = \frac{(E \cdot S_m) - S_c}{S_c} \qquad ROI = \frac{G - C}{C}$$

Postępowanie z ryzykiem

- Ograniczenie (reduction)
  - Zabezpieczenia (*safeguards, controls*)
- Akceptacja (acceptance)
  - Świadoma i racjonalna, oparta na przesłankach
- Przeniesienie (transfer)
  - Ubezpieczenie, outsourcing
- Unikanie (avoidance)
  - Zaprzestanie ryzykownego działania
- ~~Ignorowanie (ignorance)~~
  - Patologiczna forma akceptacji

Jak weryfikować zaufanie?

Zaufanie... co do czego?

- Czy dana osoba jest tą, za którą się podaje?
- Czy dany obiekt jest tym, jako który go opisano?
- Czy dana osoba ma prawo czytać dany plik?

Poufność

- Formalne modele poufności
- Środki prawne
  - Penalizacja ujawnienia informacji niejawnej
- Środki organizacyjne
  - Zasada wiedzy koniecznej (*need to know*)
- Środki techniczne
  - Szyfrowanie danych

Formalne modele dostępu do danych

- Wywodzą się z polityk wojskowych
- Realizują funkcje
  - Poufności – kto może czytać/kopiować dane
  - Integralności – kto może zapisywać/zmieniać dane
- Wymagają klasyfikacji informacji
  - Np. "tajne", "jawne"
  - Opisują relacje między klasami

Model Bell-LaPadula

- Model poufności (kontroli dostępu)
- Poziomy klasyfikacji poufności
  - "Niższy", "Taki sam jak mój", "Wyższy"
- "Read down – write up"
  - Mogę czytać dane tylko z "niższe" lub "takie same"
    - "simple security property"
  - Mogę zapisywać dane tylko "wyższe" lub "takie same"
    - "star security property" (*-property)

Integralność

- Dane są zmieniane tylko przez uprawnione osoby
  - Tylko uprawniona osoba ma prawo zmian
    - Kontrola dostępu do danych
      - Nie ma praw zapisu, nie można zmienić
  - Nieuprawnione zmiany są wykrywalne
    - Kontrola integralności za pomocą funkcji skrótu

Model Biba

- Model integralności ("czystości" danych)
- Poziomy klasyfikacji integralności j.w.
- "Read up – write down"
  - Mogę czytać tylko dane "czystsze" lub "takie same"
  - Mogę zapisywać tylko dane "brudniejsze" lub "takie same"
- Integralność danych
  - Np. precyzja pomiarów, zaokrągleń, skala map

Funkcje bezpieczeństwa

- **Poufność (*Confidentiality*)**
- **Integralność (*Integrity*)**
- **Dostępność (*Availability*)**
- Autentyczność (*Authenticity*)
- Niezaprzeczalność (*Non-repudiation*)
- Rozliczalność (*Accountability*)
- Anonimowość (*Anonymity*)

Model kratowy

- Krata (*security lattice*) – opis uprawnień
  - Obiekty sklasyfikowane jako {kategoria, poziom}
    - {Osobowe, służbowy}
    - {Osobowe, wrażliwe}
    - {Projekty, służbowy}
    - {Projekty, zastrzeżone}
  - Podmiot ma przypisany zakres dostępu
    - Pracownik HR – {Osobowe, *}
    - Pracownik finansów – {Osobowe, służbowy}
    - Inżynier – {Projekty, służbowy}
    - Menedżer – {Projekty, *}

Modele macierzowe

- Zbiory wejściowe
  - S (*subjects*) – podmioty (np. użytkownicy)
  - O (*objects*) – obiekty (np. Pliki)
- Uprawnienia
  - Odczyt, Zapis, Dopisanie, Wykonanie...
- Reprezentacja polityki bezpieczeństwa
  - A (*access*) – macierz dostępu
    - S1 → O → O1
    - S2 → O,Z → O2

Zastosowanie modeli kontroli dostępu

- Połączenie elementów wszystkich w/w modeli w systemach operacyjnych
  - Prawa dostępu do plików
- Discretionary vs Mandatory Access Control
  - DAC – właściciel decyduje o uprawnieniach
  - MAC – administrator decyduje o uprawnieniach
- W praktyce
  - Security Enhanced Linux, AppArmor
  - Windows Vista – Mandatory Integrity Control
    - Internet Explorer Protected Mode

Autentyczność

- Podstawa kontroli dostępu
  - Autentyczność podmiotów i obiektów
- Przykłady
  - Wiadomości (*message*)
  - Kanału łączności (*peer entity*)
  - Pochodzenia danych (*data origin*)
  - Tożsamości osoby (*identity*)

Uwierzytelnianie

- Identyfikacja
  - Tożsamość deklarowana
- Uwierzytelnianie
  - Weryfikacja i potwierdzenie tożsamości
- Wiele metod weryfikacji
  - Różne poziomy pewności = różny koszt
  - Wynik – potwierdzenie tożsamości
  - Wybór poziomu wystarczającego na podstawie analizy ryzyka

Klasyfikacja metod uwierzytelniania

- Coś, co wiesz (*something you know*)
  - Hasło, kod PIN
- Coś, co masz (*something you have*)
  - Token, identyfikator RFID, karta kryptograficzna
- Coś, czym jesteś (*something you are*)
  - Techniki biometryczne
- Techniki kombinowane
  - Uwierzytelnienie dwuskładnikowe (*two-factor authentication*)

Strona techniczna

- Hasła (*password, pass-phrase*)
- Hasła jednorazowe
  - Pregenerowane - TAN (*Transaction Authentication Numbers*), "zdrapki", OTP (*One-time password*)
  - Generowane – RSA SecurID, SafeWord, YubiKey, CERB, sToken, SMS...
- Identyfikatory zbliżeniowe (RFID)
  - Samo posiadanie identyfikatora, ewentualnie z PIN

Kryptografia asymetryczna

- Dowód posiadania klucza prywatnego
  - SSL/TLS, ISAKMP/IKE (IPSec), SSH – uwierzytelnienie kanału łączności
  - Podpis elektroniczny - PGP, S/MIME – uwierzytelnienie pochodzenia wiadomości
- Lokalizacja klucza prywatnego
  - Program, system operacyjny
  - Karta kryptograficzna
  - W obu przypadkach dodatkowe hasło (PIN)

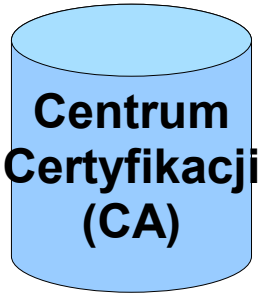
Strona organizacyjna

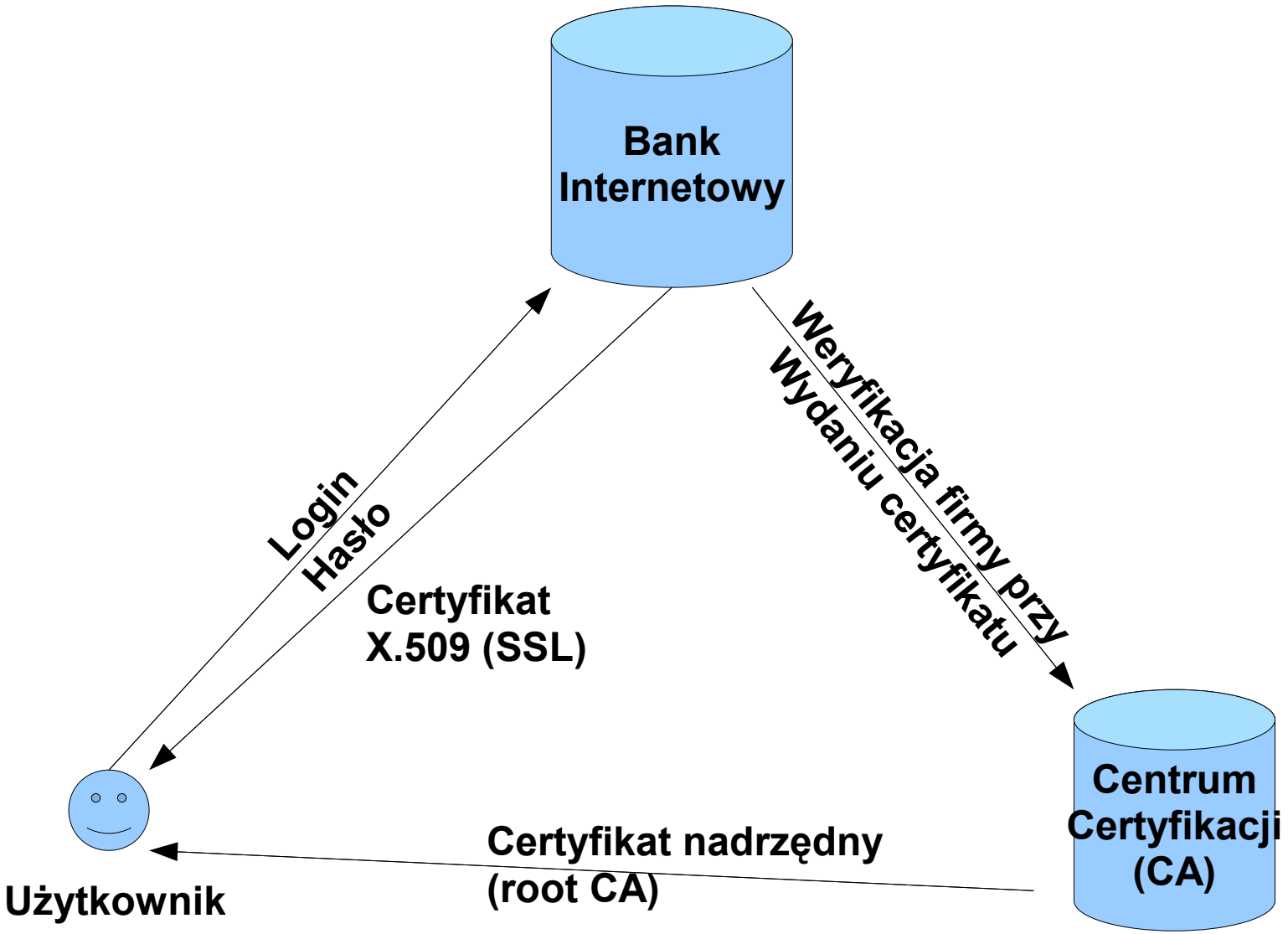
- Identyfikator, hasło, klucz, token, karta...
  - Komu wydać?
  - Jak przywiązać je do tożsamości?
  - Na jakiej podstawie?
- Środowisko instytucjonalne i korporacyjne
  - Wydzielony dział z odpowiednimi uprawnieniami
- Środowiska heterogeniczne
  - B2B, B2C, G2C
  - Znacznie bardziej złożony problem

Zaufana trzecia strona

- Architektury zaufania
  - "Każdy ufa każdemu" (*mesh, web of trust*)
    - Każdy weryfikuje tożsamość i swoje zaufanie do każdego
    - Problematyczna skalowalność
  - Wszyscy ufamy jednemu podmiotowi
    - Zaufana trzecia strona (TTP) poświadcza tożsamość wszystkich uczestników
    - Usługom TTP towarzyszą zobowiązania formalne (umowy cywilno-prawne) dotyczące zakresu gwarancji

Użytkownik




Bank
Internetowy
Login
Hasło
Certyfikat
X.509 (SSL)
Weryfikacja firmy przy
Wydaniu certyfikatu
Centrum
Certyfikacji
(CA)
Certyfikat nadrzędny
(root CA)
Użytkownik

Niezaprzeczalność

- Ochrona przed wyparciem się danej operacji
  - Podpisanie umowy, dokonanie zakupu, złożenie zlecenia przelewu, zrzeczenie się praw, zgoda na...
- Wyprzeć się można zawsze...
  - Przesłanki, że wyparcie jest nieuzasadnione
  - Mogą być one gromadzone środkami prawnymi lub technicznymi

Niezaprzeczalność #1

- Uzależnienie usługi od poświadczenia deklaracji
  - "Tak, wyrażam zgodę na otrzymywanie reklam..."
  - "Tak, przeczytałem i akceptuję regulamin..."
- W razie wyparcia
  - Klient zaznaczył kratkę "Tak..."
  - Bez tego realizacja usługi nie była możliwa
  - Musiał być więc świadomy treści deklaracji

Niezaprzeczalność #2

- Podpis elektroniczny składany kluczem prywatnym
  - Zakaz tworzenia kopii klucza prywatnego (prawny)
  - Niemożność skopiowania klucza prywanego (techniczny)
  - Dostęp do klucza po podaniu PIN (techniczny)
  - Zakaz udostępniania PIN innym osobom (prawny)
- Wnioski
  - Tylko właściciel może złożyć podpis
    - Lub złamać prawo, lub zostać do tego zmuszonym...

Dostępność

- Kontrola dostępu
  - Nieautoryzowane osoby nie mogą zmienić lub usunąć danych
- Środki techniczne
  - Replikacja, kopie zapasowe, kolokacja
- Środki organizacyjne
  - Plany awaryjne, delegacja odpowiedzialności, testowanie środków technicznych

Rozliczalność

- Mozliwość przypisania działań podmiotom
  - Funkcja audytu (*audit*)
  - Zależy od skutecznego potwierdzenia tożsamości
- Środki techniczno-organizacyjne
  - Obligatoryjne dzienniki
    - Systemowe (logi), wejścia-wyjścia (pomieszczenia)
  - Ochrona integralności dzienników

Anonimowość

- Dostęp do obiektu bez ujawniania tożsamości podmiotu
  - Ochrona prywatności
- Pozorna sprzeczność z rozliczalnością i kontrolą dostępu
  - W praktyce – poufność informacji o tożsamości

Anonimowa kontrola dostępu

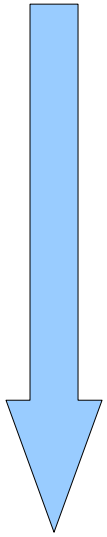
- Model tradycyjny
  - Identyfikacja → Uwierzytelnienie → Uprawnienia
- Ograniczone udostępnianie informacji (*limited disclosure*)
  - "Uprawnienia na okaziciela" (Microsoft U-Prove)
  - Dowód wiedzy zerowej (*zero knowledge proof*)
  - Anonymizacja danych (*anonymisation*)
    - Tokenizacja (tokenisation),

Gradacja siły mechanizmów bezpieczeństwa

- Koszt użycia jest funkcją siły zabezpieczenia
  - Najmniejsza, wystarczająca siła mechanizmów
  - Racjonalizacja kosztów i optymalizacja procesu
- Pułapka unifikacji ("one size fits all")
  - Konieczność dostosowania do procesu o najwyższych wymaganiach
  - Paraliż procesów o niższych wymaganiach

Przykłady

- Bankowość elektroniczna
- IDA (Interchange of Data between Administrations) Authentication Policy
  1) Hasła lub kody PIN
  2) Hasła jednorazowe
  3) Klucze kryptograficzne przechowywane programowo
  4) Klucze kryptograficzne przechowywane sprzętowo
- FIPS 200 (NIST)



Zaufanie oparte o reputację

Zaufanie oparte o reputację

- W odniesieniu do osób
  - Systemy aukcyjne, mikropożyczkowe...
  - Systemy oceny sklepów, prawników, lekarzy...
  - Systemy historii kredytowej, bazy dłużników...
- W odniesieniu do sieci
  - Czarne listy adresów IP
    - DNSBL (DNS Blocklist)
  - Klasyfikacja treści
    - WCF (Web Content Filtering)

Reputacja a funkcje bezpieczeństwa

- Reputacja może być przywiązana do mniej lub bardziej anonimowego identyfikatora
  - "marysia123" – w serwisach aukcyjnych
  - 10.2.3.4 – w czarnych listach adresów IP
  - http://www.casino124.net/ - w systemach klasyfikacji stron
- Potwierdzenie tożsamości stron nie jest kluczowe
  - *"Czy chcę z nim rozmawiać"* zamiast *"kim on jest?"*

Reputacja osób

- Odpowiedź na anonimowość drobnego handlu elektronicznego
  - "Czy chcę kupić/sprzedać coś tej osobie na odległość?"
  - "Jaki jest poziom ryzyka tej transakcji?"
- Ułatwia podjęcie decyzji
- Poprawia konkurencję
- Ogranicza nadużycia
- Nie jest doskonała

Reputacja osób

- Przykładowe kryteria
  - Działający adres email → email z kodem
  - Działający adres pocztowy → list z kodem
  - Telefon komórkowy → SMS
  - Konto bankowe → przelew na 0,01 zł
  - Historia w KRD, BIK, InfoMonitor, ERIF
  - Jest zatrudniony → kontakt z pracodawcą
  - Co o nim myślą inni użytkownicy → komentarze

Reputacja domen i adresów IP

- Odpowiedź na patologie takie jak spam, włamania do serwerów i phishing
  - Serwer: "Czy chcę przyjąć połączenie z tego IP?"
  - Klient: "Czy chcę wejść na tą stronę?"
- Często oparte o DNS (DNSBL)
  - Szybka, rozproszona, replikowalna baza danych

Czarne listy IP

- Spammerzy
  - "Z tych IP otrzymaliśmy spam"
- Open proxy/open relay
  - "Te serwery są niedostatecznie zabezpieczone"
- Podsieci konsumenckie
  - "Te adresy są przydzielane konsumentom i nie powinny na nich działać serwery"
- Prognozujące (predictive)
  - "Te adresy należą do firm spammerskich"

Klasyfikacja stron WWW

- Reputacja strony WWW
  - Przynależność do określonej kategorii
    - Systemy WCF- kilkadziesiąt kategorii i kilkaset podkategorii
    - "Czarne listy" (OpenDNS, Google Safe Browsing, Microsoft Smart Screen)
  - Wg adresu URL
- Polityka bezpieczeństwa określa dopuszczalny dostęp

Zaufanie w branży bezpieczeństwa

Zaufanie do branży

- Szczególne oczekiwania wobec branży bezpieczeństwa
  - Por. tajemnica lekarska, adwokacka, maklerska, spowiedzi...
  - Bezpieczeństwo – nie tylko dochowanie tajemnicy
- Jak buduje się zaufanie do branży i ekspertów
  - Certyfikacje zawodowe
  - Kodeksy etyki zawodowej

Kompetencje zawodowe

- Systemy certyfikacji zawodowej
  - Certyfikaty ogólne – CISSP, CISA, CISM
- Wymóg rozwoju zawodowego
  - CPE – publikacje, konferencje, wykłady...
- Udokumentowane doświadczenie
- Kodeks etyczny
- Certyfikaty produktowe
  - Microsoft, Cisco...

Etyka w bezpieczeństwie

- Zaufanie do ekspertów i branży
- Dylematy moralne i prawne
  - Prowizje od producentów
  - Korupcja
- Branżowe kodeksy etyczne
  - (ISC)2 Code of Ethics
  - ISACA Code of Professional Ethics
  - RFC 1087 "Ethics and the Internet"

Przykład - (ISC)2

- Kanon kodeksu (ISC)2
  - Protect society, the commonwealth, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.
- Kolejność istotna!

Kontakt z autorem:

pawel.krawczyk@hush.com
Tel. +48-602-776959

Zaufanie w systemach informatycznych

Paweł Krawczyk

Kontakt z autorem:

pawel.krawczyk@hush.com
Tel. +48-602-776959

Literatura:

http://ipsec.pl/
http://securitystandard.pl/

Krzysztof Liderman, "Podręcznik administratora bezpieczeństwa teleinformatycznego"

Konspekt

- Kryteria zaufania
- Analiza ryzyka
- Funkcje bezpieczeństwa
- Zaufanie oparte o reputację
- Etyka bezpieczeństwa

Zaufanie do systemu informatycznego

- Zaufanie, wiarygodność systemu informatycznego
  - Przekonanie, że dany system spełnia swoje zadanie zgodnie z określonymi kryteriami – np. polityką bezpieczeństwa (PN-I-02000:2002 pkt 3.2.017)
- Warunek konieczny: **kryteria**

Jak opisać kryteria?

- Polityki (policies)
- Procedury (procedures)
- Standardy (standards)
- Minimalne wymagania (baselines)
- Wytyczne (guidelines)

Polityki bezpieczeństwa

Polityki bezpieczeństwa

- Wysokopoziomowe
- Strategiczne
- Wytyczają kierunek
- Stabilne
- Zawierają wynik decyzji politycznych
  - Np. *"Priorytetem organizacji jest..."*
    - ***albo*** *"...maksymalizacja zysku za cenę ryzyka"*
    - ***albo*** *"...bezpieczeństwo i stabilność"*

Implementacja polityk

- **Minimalne wymagania**
  - Określają ilościowo wymagany poziom siły mechanizmów bezpieczeństwa (długość hasła, długość kluczy szyfrujących, częstość zmiany haseł)
- **Wytyczne**
  - Mogą mieć charakter niewiążący, zawierają zalecenia (*recommendations*) i najlepsze praktyki postępowania (*best practices*)

Implementacja polityk

- **Standardy**
  - Opisują obecność konkretnych mechanizmów bezpieczeństwa (hasła, szyfrowanie danych, zapory sieciowe)
- **Procedury**
  - Krok po kroku opisują sposób wykonywania określonych zadań w sposób bezpieczny (np. postępowanie z dokumentami wrażliwymi)

Częste błędy w tworzeniu polityk

- Sprzeczne cele (oksymorony)
  - *"maksymalizacja zysku za cenę ryzyka, bezpieczeństwo oraz stabilność"*
- Przemieszanie polityk z procedurami i standardami
  - Trudność zmian lub zbyt częste zmiany
  - Zbyt obszerne, nieczytelne i nieprzyswajalne
- Tworzenie polityk "na zapas" i myślenie życzeniowe
  - Zbyt dużo priorytetów = brak priorytetów

Nierealne cele polityk

- Patologia pierwsza
  - Podniesienie poziomu bezpieczeństwa tak wysoko, że zanika zysk krótko- i długoterminowy
  - Przykład: e-faktury, podpis kwalifikowany
- Patologia druga
  - Ustalenie celów bezpieczeństwa tak wysoko, że mają one charakter "myślenia życzeniowego"

Z patologią pierwszą można się zetknąć w przypadku mechanizmów, które miały oryginalnie służyć optymalizacji pewnych procesów, ułatwieniu dostępu do usług lub obniżeniu kosztów. Podniesienie wymagań bezpieczeństwa na poziom nieuzasadniony analizą ryzyka powoduje, że ich stosowanie staje się nieracjonalne – i w konsekwencji nie są one stosowane. Z taką sytuacją mamy do czynienia w przypadku podpisu kwalifikowanego w większości Państw Członkowskich UE oraz z fakturami elektronicznymi w Polsce.

Patologię drugą można spotkać w organizacjach, które z różnych powodów wdrażają polityki bezpieczeństwa ale robią to w sposób mechaniczny, np. przez skopiowanie polityk modelowych. W rezultacie otrzymują polityki niedostosowane do swojego profilu ryzyka. Jeśli nakładane przez nie wymagania są zbyt wysokie i kolidowałyby z działalnością tych organizacji to po prostu są powszechnie ignorowane i stan taki jest tolerowany. Taka fikcja zachęca jednak do selektywnego traktowania wszystkich reguł postępowania w danej organizacji i prowadzi do specyficznego "dwójmyślenia".

Czy więcej bezpieczeństwa to lepiej?

- Bezpieczeństwo służy maksymalizacji zysku
  - Poświęcamy krótkoterminowy zysk lub wydajność w celu uniknięcia długoterminowych strat
  - Dbamy o zysk długoterminowy
- Wartość graniczna bezpieczeństwa
  - 100% bezpieczeństwa = 0% działania
- Racjonalna polityka bezpieczeństwa
  - Jest dostosowana do profilu ryzyka tej konkretnej organizacji
  - Przyczynia się do realizacji jej celów

Teoria bezpieczeństwa informacji wywodzi się ze środowisk wojskowych, które mają szczególny profil ryzyka (risk aversive). W środowiskach tych priorytetem jest unikanie ryzyka lub ograniczanie go niemal do zera. Jest to jednak bardzo kosztowne.

Stosowanie tej samej miary do większości współczesnych zastosowań komercyjnych prowadziłoby do paraliżowania gospodarki elektronicznej, zamiast jest stymulowania.

Stąd działalność komercyjna w znacznie większym stopniu skupia się na "życiu z ryzykiem" przez jego ograniczanie tylko w takim stopniu, w jakim jest to uzasadnione względami biznesowymi.

Racjonalna analiza ryzyka pozwala na wyznaczenie optymalnego – czyli wystarczającego, ale ani zbyt małego ani nadmiernego – poziomu kontroli ryzyka.

Metody racjonalizacji polityk

- Rozbudowa na podstawie
  - Potrzeb wewnętrznych
  - Wymagań zewnętrznych
    - Prawo, standardy branżowe, wymagania klientów, przewaga konkurencyjna
- Uporządkowanie przy pomocy analizy ryzyka
  - Jakościowa, ilościowa
- Racjonalizacja zabezpieczeń
  - Analiza kosztów i zysków (*cost-benefit*)
  - ROI = Return on Investment
  - ROSI = Return on Security Investment

Analiza ryzyka

Analiza ryzyka

- Racjonalny i obiektywny opis ryzyk organizacji
  - Umożliwia ich racjonalne **kontrolowanie**
- Analiza jakościowa (*qualitative*)
  - Wysokie/średnie/niskie
- Analiza ilościowa (*quantitative*)
  - Każde ryzyko ma wartość finansową

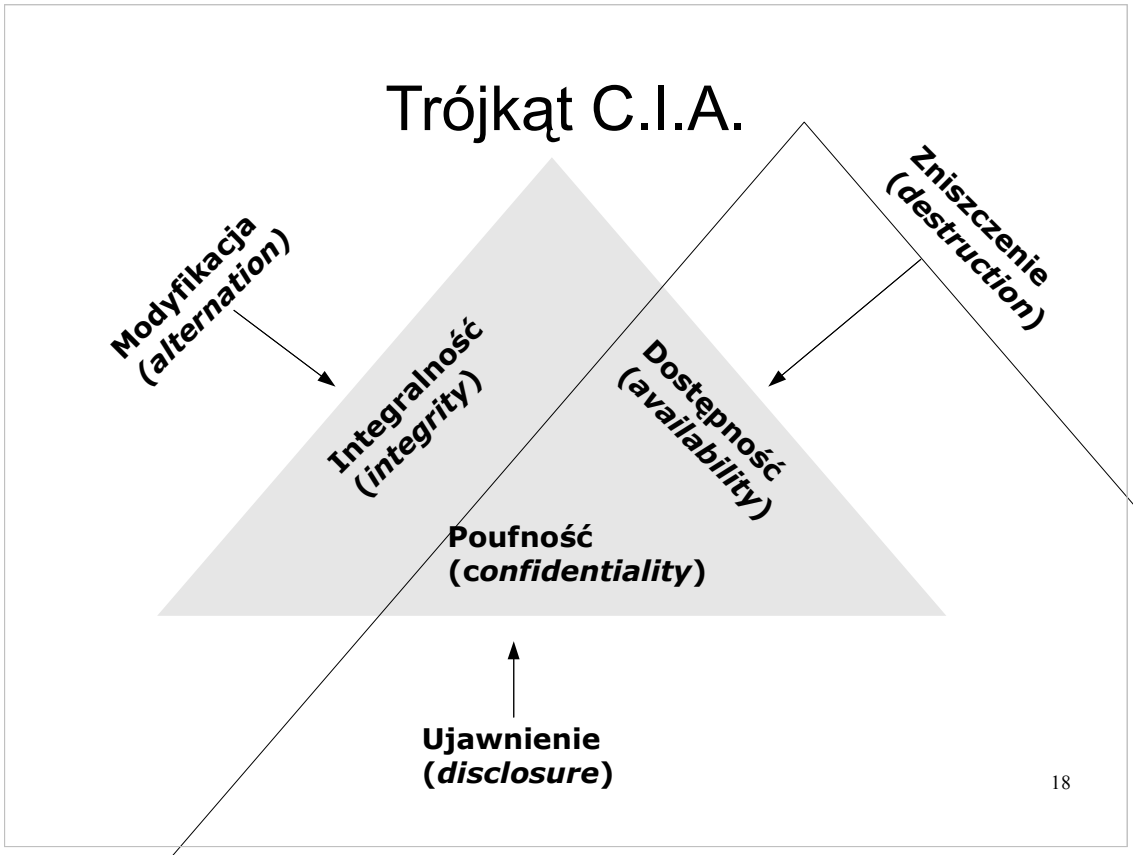
Rekomendacje i standardy:
NIST SP 800-30 "Risk Management Guide for Information Technology Systems"
ISO 27005

Terminologia

- Zasoby chronione, aktywa (*assets*)
- Zagrożenie (*threat*)
- Czynnik zagrożenia (*threat agent*)
- Podatność (*vulnerability*)
- Narażenie na ryzyko (*exposure to risk*)
- Ryzyko (*risk*)
- Środki bezpieczeństwa, zabezpieczenia (*countermeasures*)
- Szkoda (*impact*)

Wyjaśnienia terminologii

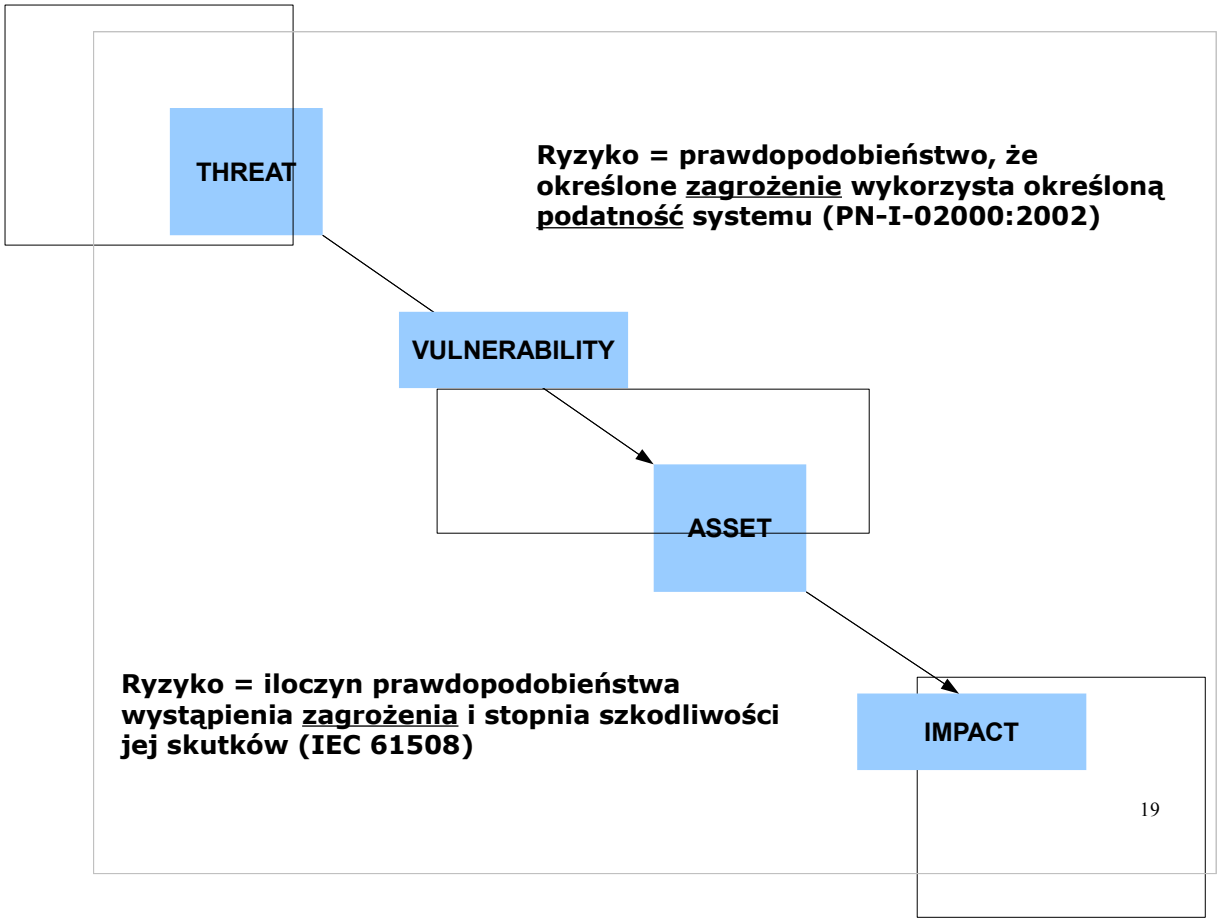
- Zagrożenia
  - Niezależne od nas, nie mamy na nie wpływu
  - Nie muszą nas dotyczyć, jeśli nie istnieje **czynnik** (*agent*)
- Podatność
  - Istnieje jeśli odpowiada **czynnikowi zagrożenia** i nie istnieje odpowiednie **zabezpieczenia**
  - Na podatność mamy wpływ
- Ryzyko
  - Istnieje, jeśli istnieje **podatność**

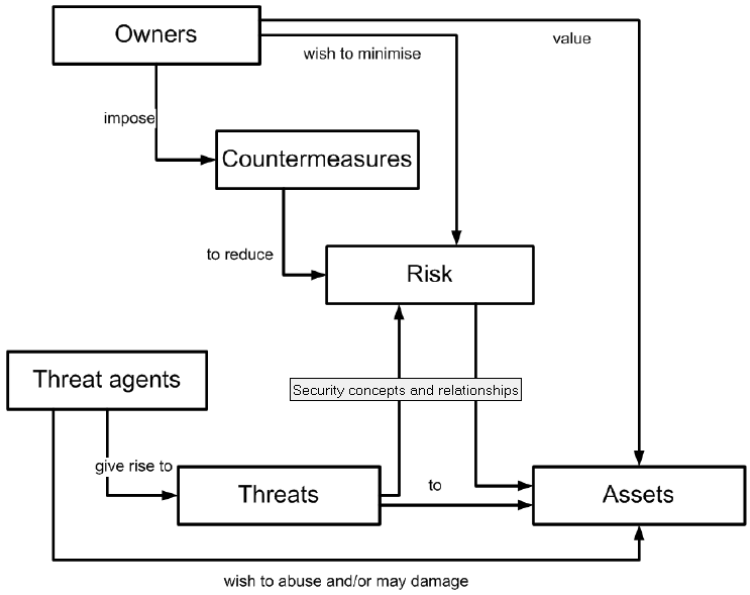


Poufność – dostęp do informacji mają wyłącznie osoby uprawnione, a osoby nieuprawnione nie mają do niej dostępu.

Integralność – informacja nie może być zmodyfikowana, dodana lub usunięta bez możliwości wykrycia ingerencji.

Dostępność – upoważnione osoby mogą uzyskać dostęp do informacji w wymaganym miejscu, czasie i zakresie.


THREAT
Ryzyko = prawdopodobieństwo, że określone zagrożenie wykorzysta określoną podatność systemu (PN-I-02000:2002)
VULNERABILITY
ASSET
Ryzyko = iloczyn prawdopodobieństwa wystąpienia zagrożenia i stopnia szkodliwości jej skutków (IEC 61508)
IMPACT
19



Źródło: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009

Wycena ryzyka w praktyce #1

- Określenie SLE (*Single Loss Expectancy*)
  - SLE = AV x EF
    - AV (Asset Value) [$]
    - EF (Exposure Factor) [%]
- Przykład
  - Zysk z jednego dnia emisji reklam średnio 1000 zł
    - AV = 1000zł
  - Ciągłość pracy systemu 98%
    - To nie jest EF!
    - System przestaje działać → reklamy się nie wyświetlają → EF=100%

Wycena ryzyka w praktyce #2

- Agregacja w skali rocznej
  - AV_{roczny} = AV x 365 dni = 365'000 zł
- ARO (*Annual Rate of Occurence*)
  - ARO = 2% (100%-98%) = 7,3 dnia w roku
- ALE (Annual Loss Expectancy)
  - ALE = SLE x ARO = 7300 zł
- Obiektywna miara ryzyka w skali roku
  - Zagrożenie – 2% przerwa w pracy systemu

Wycena ryzyka w praktyce #3

- ALE jest wskazówką do dalszych decyzji
- Jak postąpić z danym ryzykiem?
  - Jeśli ograniczać, to ile wydać na zabezpieczenie?
    - Wartość zabezpieczenia: ALE – ALE_{zabezp} – $KOSZT_{zabezp}$
- Dodatkowe narzędzia – ROI i ROSI

$$ROSI = \frac{(E \cdot S_m) - S_c}{S_c} \qquad ROI = \frac{G - C}{C}$$

ROI
G = Gain from investment
C = Cost of investment

ROSI
E = Risk exposure before safeguard
Sm = Risk mitigated by solution (90% = 10% residual)
Sc = Total solution cost

Postępowanie z ryzykiem

- Ograniczenie (reduction)
  - Zabezpieczenia (*safeguards, controls*)
- Akceptacja (acceptance)
  - Świadoma i racjonalna, oparta na przesłankach
- Przeniesienie (transfer)
  - Ubezpieczenie, outsourcing
- Unikanie (avoidance)
  - Zaprzestanie ryzykownego działania
- ~~Ignorowanie (ignorance)~~
  - Patologiczna forma akceptacji

Jak weryfikować zaufanie?

Zaufanie... co do czego?

- Czy dana osoba jest tą, za którą się podaje?
- Czy dany obiekt jest tym, jako który go opisano?
- Czy dana osoba ma prawo czytać dany plik?

Poufność

- Formalne modele poufności
- Środki prawne
  - Penalizacja ujawnienia informacji niejawnej
- Środki organizacyjne
  - Zasada wiedzy koniecznej (*need to know*)
- Środki techniczne
  - Szyfrowanie danych

Formalne modele dostępu do danych

- Wywodzą się z polityk wojskowych
- Realizują funkcje
  - Poufności – kto może czytać/kopiować dane
  - Integralności – kto może zapisywać/zmieniać dane
- Wymagają klasyfikacji informacji
  - Np. "tajne", "jawne"
  - Opisują relacje między klasami

Literatura:

Krzysztof Liderman, "Podręcznik administratora bezpieczeństwa teleinformatycznego", 2003

Model Bell-LaPadula

- Model poufności (kontroli dostępu)
- Poziomy klasyfikacji poufności
  - "Niższy", "Taki sam jak mój", "Wyższy"
- "Read down – write up"
  - Mogę czytać dane tylko z "niższe" lub "takie same"
    - "simple security property"
  - Mogę zapisywać dane tylko "wyższe" lub "takie same"
    - "star security property" (*-property)

Model BLP (Bell-LaPadula) jest modelem teoretycznym, opisującym wyłacznie problem kontroli dostępu do danych.

Osoba posiadająca poświadczenie na poziom "2" może czytać dokumenty z poziomu "1" lub "2", ale żaden dokument, który stworzy nie może być sklasyfikowany jako "1".

Ponieważ posiada ona wiedzę z poziomu "2", blokada tworzenia dokumentów na niższym poziomie uniemożliwia wyciek informacji.

Równocześnie synteza dwóch dokumentów klasy "2" lub "1" może prowadzić do wniosków, które muszą być sklasyfikowane wyżej ("3") stąd dopuszczalność "write up".

Integralność

- Dane są zmieniane tylko przez uprawnione osoby
  - Tylko uprawniona osoba ma prawo zmian
    - Kontrola dostępu do danych
      - Nie ma praw zapisu, nie można zmienić
  - Nieuprawnione zmiany są wykrywalne
    - Kontrola integralności za pomocą funkcji skrótu

Ochrona integralności może być realizowana dwiema drogami – po pierwsze, uniemożliwiając modyfikację danych osobom nieuprawnionym za pomocą kontroli dostępu. Opisujemy to dalej na przykładzie modelu Biba.

Po drugie, długoterminową ochronę integralności zapewniamy przez wykrywanie nieuprawnionych zmian – za kryptograficznych kodów kontrolnych, podpisu elektronicznego itd.

Przykładem bardzo rozbudowanej i długoterminowej ochrony integralności i autentyczności dokumentów są usługi notariatu elektronicznego LTANS (Long-Term Archiving and Notary Services).

Model Biba

- Model integralności ("czystości" danych)
- Poziomy klasyfikacji integralności j.w.
- "Read up – write down"
  - Mogę czytać tylko dane "czystsze" lub "takie same"
  - Mogę zapisywać tylko dane "brudniejsze" lub "takie same"
- Integralność danych
  - Np. precyzja pomiarów, zaokrągleń, skala map

Połączenie Biba z BLP skutkuje nową istotną restrykcją tzw. "strong star property"- jeśli mam prawo i zapisu i odczytu, to mogę pisać i czytać tylko na swoim poziomie.

Wynika to z połączenia restrykcji obu modeli w celu ochrony zarówno poufności jak i integralności.

Funkcje bezpieczeństwa

- **Poufność (*Confidentiality*)**
- **Integralność (*Integrity*)**
- **Dostępność (*Availability*)**
- Autentyczność (*Authenticity*)
- Niezaprzeczalność (*Non-repudiation*)
- Rozliczalność (*Accountability*)
- Anonimowość (*Anonymity*)

Autentyczność – pewność, że dany podmiot jest tym, za który się podaje a obiekt tym, jako który został opisany.

Niezaprzeczalność – możliwość wykazania z dużym prawdopodobieństwem, że dany podmiot wykonał daną czynność w sytuacji, gdy się tego wypiera.

Rozliczalność – możliwość jednoznacznego przypisania danego działania określonemu podmiotowi.

Anonimowość – niemożność przypisania danego obiektu lub działania do określonego podmiotu.

Model kratowy

- Krata (*security lattice*) – opis uprawnień
  - Obiekty sklasyfikowane jako {kategoria, poziom}
    - {Osobowe, służbowy}
    - {Osobowe, wrażliwe}
    - {Projekty, służbowy}
    - {Projekty, zastrzeżone}
  - Podmiot ma przypisany zakres dostępu
    - Pracownik HR – {Osobowe, *}
    - Pracownik finansów – {Osobowe, służbowy}
    - Inżynier – {Projekty, służbowy}
    - Menedżer – {Projekty, *}

Modele macierzowe

- Zbiory wejściowe
  - S (*subjects*) – podmioty (np. użytkownicy)
  - O (*objects*) – obiekty (np. Pliki)
- Uprawnienia
  - Odczyt, Zapis, Dopisanie, Wykonanie...
- Reprezentacja polityki bezpieczeństwa
  - A (*access*) – macierz dostępu
    - S1 → O → O1
    - S2 → O,Z → O2

Zastosowanie modeli kontroli dostępu

- Połączenie elementów wszystkich w/w modeli w systemach operacyjnych
  - Prawa dostępu do plików
- Discretionary vs Mandatory Access Control
  - DAC – właściciel decyduje o uprawnieniach
  - MAC – administrator decyduje o uprawnieniach
- W praktyce
  - Security Enhanced Linux, AppArmor
  - Windows Vista – Mandatory Integrity Control
    - Internet Explorer Protected Mode

Autentyczność

- Podstawa kontroli dostępu
  - Autentyczność podmiotów i obiektów
- Przykłady
  - Wiadomości (*message*)
  - Kanału łączności (*peer entity*)
  - Pochodzenia danych (*data origin*)
  - Tożsamości osoby (*identity*)

Uwierzytelnianie

- Identyfikacja
  - Tożsamość deklarowana
- Uwierzytelnianie
  - Weryfikacja i potwierdzenie tożsamości
- Wiele metod weryfikacji
  - Różne poziomy pewności = różny koszt
  - Wynik – potwierdzenie tożsamości
  - Wybór poziomu wystarczającego na podstawie analizy ryzyka

NIST SP 800-63 Electronic Authentication Guideline

Klasyfikacja metod uwierzytelniania

- Coś, co wiesz (*something you know*)
  - Hasło, kod PIN
- Coś, co masz (*something you have*)
  - Token, identyfikator RFID, karta kryptograficzna
- Coś, czym jesteś (*something you are*)
  - Techniki biometryczne
- Techniki kombinowane
  - Uwierzytelnienie dwuskładnikowe (*two-factor authentication*)

"Coś co wiesz" – mają charakter niematerialny, są informacjami. Zaletą jest wysoka dostępność, wadą – łatwość kradziezy przez skopiowanie bez świadomości osoby uprawnionej.

"Coś co masz" – są spersonalizowanymi przedmiotami. Zaletą jest trudność kradzieży bez świadomości posiadacza, wadą – brak dostępności w razie awarii lub zgubienia. Stą konieczność zapewnienia kanałów awaryjnych!

"Coś czym jesteś" – unikalne cechy danej osoby (cechy biometryczne). Trudne do skopiowania, pomiar może być uciążliwy oraz obarczony błędem (False Acceptance/Rejection Ration). Zdeterminowany atakujący może zniszczyć oryginał w celu uzyskania kopii.

Strona techniczna

- Hasła (*password, pass-phrase*)
- Hasła jednorazowe
  - Pregenerowane - TAN (*Transaction Authentication Numbers*), "zdrapki", OTP (*One-time password*)
  - Generowane – RSA SecurID, SafeWord, YubiKey, CERB, sToken, SMS...
- Identyfikatory zbliżeniowe (RFID)
  - Samo posiadanie identyfikatora, ewentualnie z PIN

Hasła nadal są najbardziej rozpowszechnioną techniką uwierzytelnienia. Wymagają najprostszego z możliwych interefejsu czyli klawiatury i ekranu.

Problem łatwej kradzieży haseł rozwiązują hasła jednorazowe. Hasła pregenerowane również mogą być wyłudzane lub kradzione.

Sprzętowe generatory mogą zostać zgubione lub skradzione. Dodatkowe hasło (PIN) do tokenu rozwiązuje problem kradzieży, ale nie rozwiązuje problemu dostępności w razie zgubienia.

Kryptografia asymetryczna

- Dowód posiadania klucza prywatnego
  - SSL/TLS, ISAKMP/IKE (IPSec), SSH – uwierzytelnienie kanału łączności
  - Podpis elektroniczny - PGP, S/MIME – uwierzytelnienie pochodzenia wiadomości
- Lokalizacja klucza prywatnego
  - Program, system operacyjny
  - Karta kryptograficzna
  - W obu przypadkach dodatkowe hasło (PIN)

Klucz prywatny – reprezentacja "wyłącznej kontroli posiadacza" (pojęcie *"sole control of owner"* z Dyrektywy 1999/93 EC), zgodnie z logiką kryptografii z kluczem publicznym.

Poziom pewności, że kontrola jest "wyłączna" może być sterowany dodatkowymi środkami takimi jak kod PIN oraz karta kryptograficzna.

Odbiorca wiadomości lub strona komunikacji weryfikuje posiadanie klucza prywatnego przy pomocy klucza publicznego nadawcy. Musi go oczywiście uprzednio posiadać i mieć pewność, co do jego autentyczności.

Strona organizacyjna

- Identyfikator, hasło, klucz, token, karta...
  - Komu wydać?
  - Jak przywiązać je do tożsamości?
  - Na jakiej podstawie?
- Środowisko instytucjonalne i korporacyjne
  - Wydzielony dział z odpowiednimi uprawnieniami
- Środowiska heterogeniczne
  - B2B, B2C, G2C
  - Znacznie bardziej złożony problem

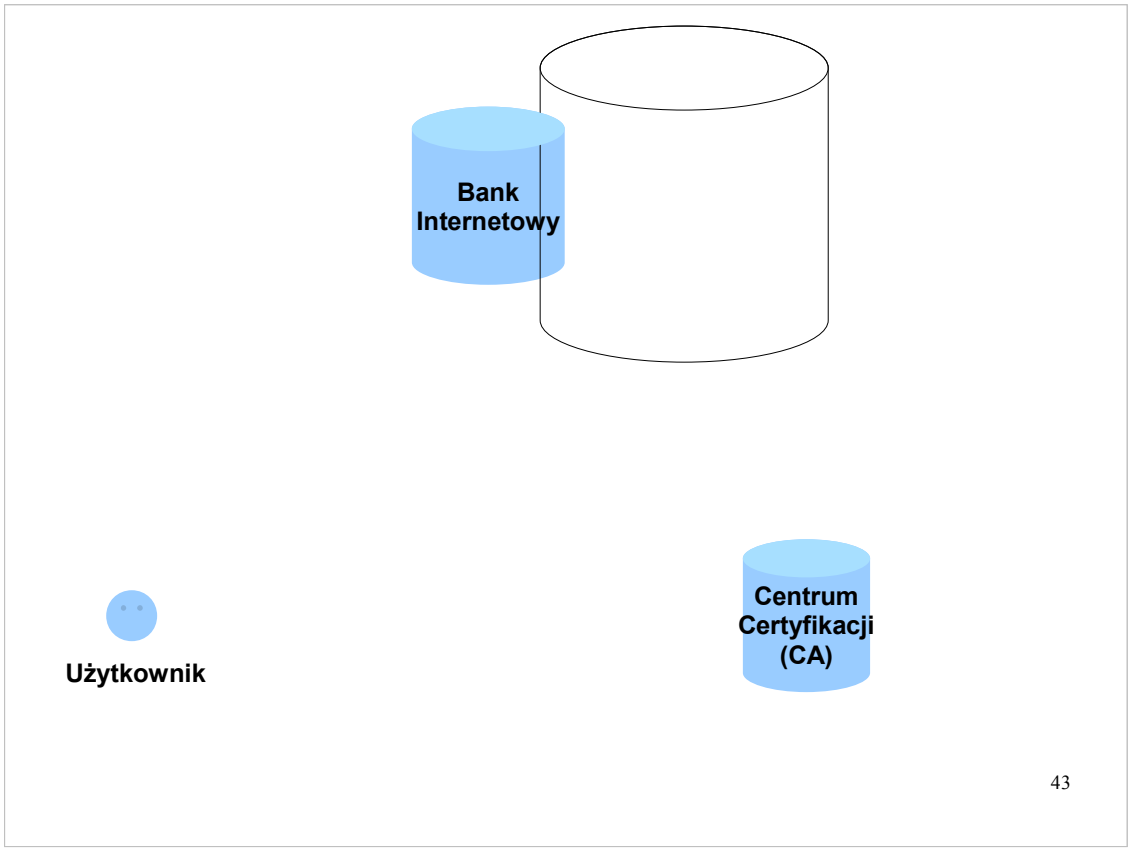
Zaufana trzecia strona

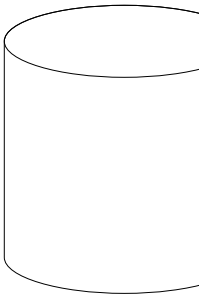
- Architektury zaufania
  - "Każdy ufa każdemu" (*mesh, web of trust*)
    - Każdy weryfikuje tożsamość i swoje zaufanie do każdego
    - Problematyczna skalowalność
  - Wszyscy ufamy jednemu podmiotowi
    - Zaufana trzecia strona (TTP) poświadcza tożsamość wszystkich uczestników
    - Usługom TTP towarzyszą zobowiązania formalne (umowy cywilno-prawne) dotyczące zakresu gwarancji

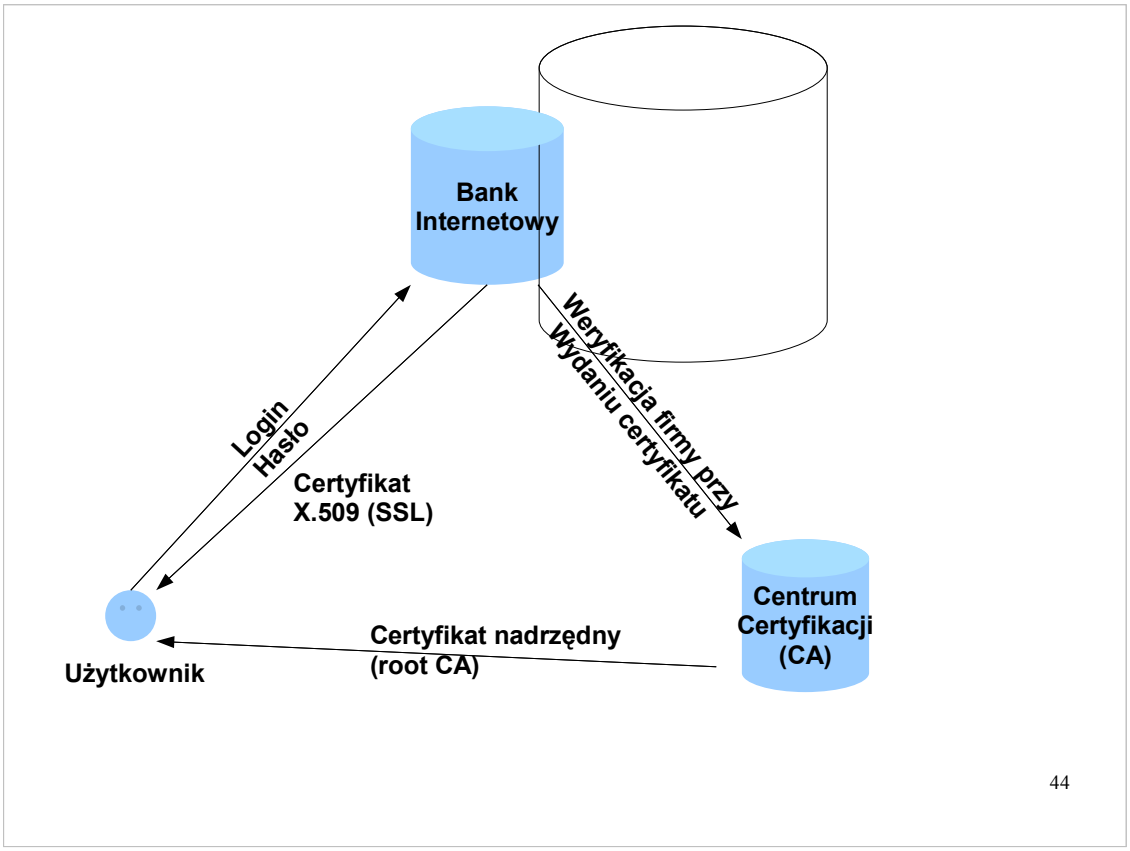
Model mesh jest pierwszym i naturalnym modelem w kontaktach społecznych i biznesowych. Każdemu uczestnikowi zapewnia pełną kontrolę nad procesem weryfikacji tożsamości oraz kryteriami zaufania.

Równocześnie jednak oczekiwania większości podmiotów odpowiadają możliwym do ustandardyzowania zbiorom kryteriów, ze względu na wykładniczy wzrost ilości relacji w modelu mesh jego skalowalność nastręcza problemy.

W związku z tym rynek wykształcił również usługi weryfikacji i poświadczania tożsamości. Robią to niezależne podmioty, które wszyscy uczestnicy procesu traktują jako zaufaną trzecią stronę – TTP (Trusted Third Party).


Bank
Internetowy
Centrum
Certyfikacji
(CA)
Użytkownik
43





Proszę zwrócić uwagę na asymetrię uwierzytelnienia banku wobec klienta (certyfikat X.509) oraz klienta wobec banku (login+hasło).

Bank uwierzytelnia się klientowi by ten miał pewność, komu podaje swój login i hasło.

Login i hasło zapewniają wystarczającą siłę uwierzytelnienia klienta. Intuicyjnie najbardziej oczywista technika – certyfikat X.509 klienta – bardzo ograniczałaby interoperacyjność, stąd bankowość unika ich stosowania. Podnoszenie poziomu pewności osiąga się technikami takimi jak hasła jednorazowe czy kody SMS.

CA uwierzytelnia się wobec klienta za pomocą preinstalowania swojego certyfikatu (root certificate) w przeglądarce lub systemie operacyjnym klienta (WebTrust).

Bank uwierzytelnia się wobec CA przedstawiając odpowiednie dokumenty.

Niezaprzeczalność

- Ochrona przed wyparciem się danej operacji
  - Podpisanie umowy, dokonanie zakupu, złożenie zlecenia przelewu, zrzeczenie się praw, zgoda na...
- Wyprzeć się można zawsze...
  - Przesłanki, że wyparcie jest nieuzasadnione
  - Mogą być one gromadzone środkami prawnymi lub technicznymi

45

Niektóre sposoby gromadzenia materiału dowodowego na potrzeby niezaprzeczalności opisuje norma PN ISO/IEC 13881-3.

Niezaprzeczalność pochodzenia – NRO (non-repudiaton of origin)

Podmiot utworzył wiadomość i ją nadał

„Wiadomość" odnosi się do podpisu, a nie samej wiadomości

Osoba lub podmiot nadający nie musi znać lub zgadzać się z treścią wiadomości

Przykład: dokument opublikowany na BIP z podpisem pracownika technicznego

Niezaprzeczalność znajomości (wiedzy) – NRK (non-repudiation of knowledge)

Podmiot jest świadomy treści podpisywanej wiadomości

Przykłady: wymóg przewinięcia umowy licencyjnej do końca lub zaznaczenia kratki

Niezaprzeczalność #1

- Uzależnienie usługi od poświadczenia deklaracji
  - "Tak, wyrażam zgodę na otrzymywanie reklam..."
  - "Tak, przeczytałem i akceptuję regulamin..."
- W razie wyparcia
  - Klient zaznaczył kratkę "Tak..."
  - Bez tego realizacja usługi nie była możliwa
  - Musiał być więc świadomy treści deklaracji

Niezaprzeczalność dostarczenia – **NRD** (non-repudiation of delivery)
odbiorca odebrał wiadomość i zapoznał się z jej treścią.
Niezaprzeczalność przedłożenia – **NRS** (non-repudiation of submission)
przeznaczone dla nadawcy wiadomości poświadczenie, że została ona przyjęta do przesłania przez organ pośredniczący w jej dostarczeniu (np. poczta, kurier, elektroniczna skrzynka podawcza)
Niezaprzeczalność nadania – **NRST** (non-repudiation of sending)
podmiot nadał wiadomość.
Niezaprzeczalność przesłania – **NRT** (non-repudiation of transmission)
przeznaczone dla nadawcy wiadomości poświadczenie faktu jej dostarczenia adresatowi przez organ pośredniczący w dostarczeniu.
Niezaprzeczalność utworzenia – **NRC** (non-repudiation of creation)
podmiot utworzył wiadomość.
Niezaprzeczalność odbioru – **NRR** (non-repudiation of receipt)
podmiot odebrał wiadomość
ale niekoniecznie się z nią zapoznał (np. Return-Receipt - RFC 3798)

Niezaprzeczalność #2

- Podpis elektroniczny składany kluczem prywatnym
  - Zakaz tworzenia kopii klucza prywatnego (prawny)
  - Niemożność skopiowania klucza prywanego (techniczny)
  - Dostęp do klucza po podaniu PIN (techniczny)
  - Zakaz udostępniania PIN innym osobom (prawny)
- Wnioski
  - Tylko właściciel może złożyć podpis
    - Lub złamać prawo, lub zostać do tego zmuszonym...

Zapotrzebowanie na tego typu funkcje pojawia się np. w elektronicznych serwisach maklerskich lub inwestycyjnych.

Ze względu na znaczne ryzyko operacji finansowych wyparcie się zlecenia danej operacji może być sposobem na uniknięcie strat lub odpowiedzialności za błędne decyzje.

Stąd serwisy tego typu są jednymi z nielicznych na rynku komercyjnym, gdzie rzeczywiście istnieje silna potrzeba biznesowa zapewnienia niezaprzeczalności.

Dostępność

- Kontrola dostępu
  - Nieautoryzowane osoby nie mogą zmienić lub usunąć danych
- Środki techniczne
  - Replikacja, kopie zapasowe, kolokacja
- Środki organizacyjne
  - Plany awaryjne, delegacja odpowiedzialności, testowanie środków technicznych

Rozliczalność

- Mozliwość przypisania działań podmiotom
  - Funkcja audytu (*audit*)
  - Zależy od skutecznego potwierdzenia tożsamości
- Środki techniczno-organizacyjne
  - Obligatoryjne dzienniki
    - Systemowe (logi), wejścia-wyjścia (pomieszczenia)
  - Ochrona integralności dzienników

Anonimowość

- Dostęp do obiektu bez ujawniania tożsamości podmiotu
  - Ochrona prywatności
- Pozorna sprzeczność z rozliczalnością i kontrolą dostępu
  - W praktyce – poufność informacji o tożsamości

Anonimowa kontrola dostępu

- Model tradycyjny
  - Identyfikacja → Uwierzytelnienie → Uprawnienia
- Ograniczone udostępnianie informacji (*limited disclosure*)
  - "Uprawnienia na okaziciela" (Microsoft U-Prove)
  - Dowód wiedzy zerowej (*zero knowledge proof*)
  - Anonymizacja danych (*anonymisation*)
    - Tokenizacja (tokenisation),

Gradacja siły mechanizmów bezpieczeństwa

- Koszt użycia jest funkcją siły zabezpieczenia
  - Najmniejsza, wystarczająca siła mechanizmów
  - Racjonalizacja kosztów i optymalizacja procesu
- Pułapka unifikacji ("one size fits all")
  - Konieczność dostosowania do procesu o najwyższych wymaganiach
  - Paraliż procesów o niższych wymaganiach

Gradacja siły mechanizmów bezpieczeństwa jest konieczna ze względu na ich różny koszt – co do zasady wyższy poziom bezpieczeństwa wiąże się z wyższymi kosztami wdrożenia i stosowania.

Żądanie zbyt wysokiego poziomu bezpieczeństwa przy dostępie do informacji może utrudnić dostęp osobom uprawnionym – jest więc przeciwieństwem funkcji dostępności (*availability*).

Obie funkcje należy więc rozważne balansować – pomaga w tym analiza ryzyka oraz analiza kosztów i zysków.

Przykłady

- Bankowość elektroniczna
- IDA (Interchange of Data between Administrations) Authentication Policy
  1)Hasła lub kody PIN
  2)Hasła jednorazowe
  3)Klucze kryptograficzne przechowywane programowo
  4)Klucze kryptograficzne przechowywane sprzętowo
- FIPS 200 (NIST)

Praktycznym przykładem skutecznej gradacji poziomów bezpieczeństwa jest autoryzacja transakcji w bankowych serwisach transakcyjnych – w Polsce stosowanych jest prawie 15 różnych technik pokrywających szeroki przedział siły uwierzytelnienia, od haseł jednorazowych po "sprzętowy" podpis elektroniczny.

Warto zwrócić uwagę na poziom minimalny – to hasła jednorazowe, a do autoryzacji transakcji od dawna nie są stosowane hasła statyczne. Równocześnie najsilniejsze mechanizmy są stosowane prawie wyłącznie tam, gdzie ma to uzasadnienie biznesowe (patrz "Niezaprzeczalność").

Patrz: "Najbezpieczniejsze banki internetowe w Polsce", raport Bankier.pl, 2009

Zaufanie oparte o reputację

Zaufanie oparte o reputację

- W odniesieniu do osób
  - Systemy aukcyjne, mikropożyczkowe...
  - Systemy oceny sklepów, prawników, lekarzy...
  - Systemy historii kredytowej, bazy dłużników...
- W odniesieniu do sieci
  - Czarne listy adresów IP
    - DNSBL (DNS Blocklist)
  - Klasyfikacja treści
    - WCF (Web Content Filtering)

Reputacja a funkcje bezpieczeństwa

- Reputacja może być przywiązana do mniej lub bardziej anonimowego identyfikatora
  - "marysia123" – w serwisach aukcyjnych
  - 10.2.3.4 – w czarnych listach adresów IP
  - http://www.casino124.net/ - w systemach klasyfikacji stron
- Potwierdzenie tożsamości stron nie jest kluczowe
  - *"Czy chcę z nim rozmawiać"* zamiast *"kim on jest?"*

Reputacja osób

- Odpowiedź na anonimowość drobnego handlu elektronicznego
  - "Czy chcę kupić/sprzedać coś tej osobie na odległość?"
  - "Jaki jest poziom ryzyka tej transakcji?"
- Ułatwia podjęcie decyzji
- Poprawia konkurencję
- Ogranicza nadużycia
- Nie jest doskonała

Reputacja osób

- Przykładowe kryteria
  - Działający adres email → email z kodem
  - Działający adres pocztowy → list z kodem
  - Telefon komórkowy → SMS
  - Konto bankowe → przelew na 0,01 zł
  - Historia w KRD, BIK, InfoMonitor, ERIF
  - Jest zatrudniony → kontakt z pracodawcą
  - Co o nim myślą inni użytkownicy → komentarze

KRD – Krajowy Rejestr Długów, BIK – Biuro Informacji Kredytowej, Biuro Informacji Gospodarczej InfoMonitor (windykacja), ERIF – Europejski Rejestr Informacji Finansowej

Przykłady:
Kokos.pl (mikropożyczki) – wszystkie z w/w
Allegro.pl (aukcje) – przelew 1,01 zł na konto Allegro lub wpisanie kodu wysłanego pocztą tradycyjną
Swistak.pl (aukcje) – przelew bankowy

Wszystkie serwisy budują reputację na komentarzach innych osób handlujących z ocenianymi osobami – liczone są komentarze pozytywne, negatywne i neutralne.

Serwisy aukcyjne stosują również kategorie użytkowników - zarówno pozytywne "Zaufany Sprzedawca" w Swistak.pl, "SuperSprzedawca" w Allegro, jak i negatywne np. "użytkownik niezweryfikowany"

Reputacja domen i adresów IP

- Odpowiedź na patologie takie jak spam, włamania do serwerów i phishing
  - Serwer: "Czy chcę przyjąć połączenie z tego IP?"
  - Klient: "Czy chcę wejść na tą stronę?"
- Często oparte o DNS (DNSBL)
  - Szybka, rozproszona, replikowalna baza danych

Czarne listy IP

- Spammerzy
  - "Z tych IP otrzymaliśmy spam"
- Open proxy/open relay
  - "Te serwery są niedostatecznie zabezpieczone"
- Podsieci konsumenckie
  - "Te adresy są przydzielane konsumentom i nie powinny na nich działać serwery"
- Prognozujące (predictive)
  - "Te adresy należą do firm spammerskich"

Na świecie działa kilkadziesiąt dużych baz typu DNSBL, zarówno darmowych jak i komercyjnych. Często jeden podmiot udostępnia kilka baz, z których każda zawiera adresy z jednej z w/w kategorii. Historycznie najbardziej znane były bazy MAPS i ORBS.

Większość z nich zawiera adresy IP wysyłające spam w poczcie elektronicznej (SMTP). Baza http:BL zawiera kilka kategorii adresów IP, z których wychodzą różnego rodzaju ataki HTTP.

Do baz prognozujących można zaliczyć systemy SPEWS oraz Dshield HPB (Highly Predictive Blacklist).

Bazy te mogą być aktualizowane ręcznie (na podstawie zgłoszeń) lub automatycznie – na podstawie informacji z systemów IDS lub pułapek (honeypot, spam bait).

Klasyfikacja stron WWW

- Reputacja strony WWW
  - Przynależność do określonej kategorii
    - Systemy WCF- kilkadziesiąt kategorii i kilkaset podkategorii
    - "Czarne listy" (OpenDNS, Google Safe Browsing, Microsoft Smart Screen)
  - Wg adresu URL
- Polityka bezpieczeństwa określa dopuszczalny dostęp

Współczesne produkty WCF (Web Content Filtering) klasy korporacyjnej (enterprise) korzystają z często aktualizowanych baz zawierających klasyfikację milionów stron. Każda strona ma przypisaną jedną lub więcej kategorii i w odróżnieniu od prostych produktów "rodzinnych" (family filter) mogą to być kategorie tak rożnorodne jak "Travel", "Job search", "Hacking", "News", "Social networking" itd.

Klasyfikacja stron jest prowadzona zarówno ręcznie (ocena przez człowieka) jak i w sposób automatyczny (słowa kluczowe).

Istotne parametry filtrów treści to wielkość bazy, sposób klasyfikacji, ilość kategorii, częstotliwość aktualizacji, możliwość dodawania wyjątków oraz możliwość reklamowania stron błędnie sklasyfikowanych.

Zaufanie w branży bezpieczeństwa

Zaufanie do branży

- Szczególne oczekiwania wobec branży bezpieczeństwa
  - Por. tajemnica lekarska, adwokacka, maklerska, spowiedzi...
  - Bezpieczeństwo – nie tylko dochowanie tajemnicy
- Jak buduje się zaufanie do branży i ekspertów
  - Certyfikacje zawodowe
  - Kodeksy etyki zawodowej

Kompetencje zawodowe

- Systemy certyfikacji zawodowej
  - Certyfikaty ogólne – CISSP, CISA, CISM
- Wymóg rozwoju zawodowego
  - CPE – publikacje, konferencje, wykłady...
- Udokumentowane doświadczenie
- Kodeks etyczny
- Certyfikaty produktowe
  - Microsoft, Cisco...

Etyka w bezpieczeństwie

- Zaufanie do ekspertów i branży
- Dylematy moralne i prawne
  - Prowizje od producentów
  - Korupcja
- Branżowe kodeksy etyczne
  - (ISC)2 Code of Ethics
  - ISACA Code of Professional Ethics
  - RFC 1087 "Ethics and the Internet"

Przykład - (ISC)2

- Kanon kodeksu (ISC)2
  - Protect society, the commonwealth, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.
- Kolejność istotna!

Kontakt z autorem:

pawel.krawczyk@hush.com
Tel. +48-602-776959

Literatura:

http://ipsec.pl/
http://securitystandard.pl/

Krzysztof Liderman, "Podręcznik administratora bezpieczeństwa teleinformatycznego"