Bezpieczeństwo informacji – zagrożenia

dr inż. Bolesław Szomański
bolkosz@wit.edu.pl

Przykładowe straty

- **wg. Computer Security Institute (CSI)**
  - **w publikacji "2000 Computer Crime and Security Survey"**
- **90% respondentów (głównie wielkie korporacje i agencje rządowe) w ostatnich 12 miesiącach wykryły włamania komputerowe.**
- **70% odnotowało różne poważne przełamania zabezpieczeń inne niż te powszechnie znane jak wirusy, kradzież laptopów czy niewłaściwe używanie sieci przez pracowników.**
  - **Są to kradzieże ważnych informacji, oszustwa finansowe, penetracja systemów z zewnątrz, ataki powodujące utratę możliwości pracy (denial of service) i sabotaż skierowany na dane lub sieci.**
- **71% przyznało się do strat finansowych spowodowanych włamaniami komputerowymi.**
- **41% zgodziło się i/lub byli w stanie ocenić swoje straty finansowe.**
- **Straty całkowite tych 273 respondentów wyniosły $265,589,940 (średnia całkowita strata roczna w ciągu ostatnich trzech lat wynosiła $120,240,180).**

Rodzaje zagrożeń ze względu na skutki

- **Utrata informacji**
  - **Przypadkowe skasowanie**
  - **Wywołana awarią sprzętu lub błędem oprogramowania**
  - **Celowa (skasowanie, kradzież sprzętu)**
- **Kradzież informacji**
- **Modyfikacja informacji**
  - **Błąd ludzki lub usterka oprogramowania (rzadko sprzętu)**
  - **Zamierzona (zwykle w celu ukrycia nadużyć)**
- **Zniszczenie zasobów i informacji**
  - **Klęska żywiołowa**
  - **Sabotaż lub terroryzm**

Przykłady Zagrożeń

Ludzkie		**Środowiskowe**
Rozmyślne	*Przypadkowe*	
Podsłuch	Pomyłki i pominięcia	Trzęsienie ziemi
Modyfikacja informacji	Skasowanie pliku	Piorun
Włamania do systemu	Nieprawidłowe skierowanie	Powódź
Złośliwy kod	Wypadki fizyczne	Pożar
Kradzież		

Zagrożenia wg sposobu wystąpienia

- **Zagrożenia związane z nieuprawnionym dostępem do systemu**
  - **Przypadkowe wejście**
  - **Umyślny atak**
  - **Nieuprawniony dostęp od wewnątrz**
  - **Złośliwy kod**
- **Zagrożenia związane z przenikaniem elekromagnetycznym**
- **Zagrożenia związane z jakością sprzętu komputerowego**
- **Zagrożenia zawiązane z awarią oprogramowania**
- **Zagrożenia związane z atakiem fizycznym**

Źródła zagrożeń

- **brak mechanizmów lub nieskuteczne mechanizmy kontroli dostępu do sprzętu oprogramowania i danych (nieuprawniony dostęp do zasobów systemu),**
- **niewłaściwa administracja systemem informatycznym,**
- **zaniedbania i błędy użytkowników,**
- **niezadowolenie pracowników (mających dostęp do istotnych informacji) z warunków pracy,**
- **programy wirusowe, bomby logiczne, konie trojańskie, robaki komputerowe**
- **ingerencja intruzów specjalizujących się w przełamywaniu zabezpieczeń (tzw hakerów),**
- **możliwość podsłuchu aktywnego i pasywnego,**
- **retransmisja informacji**

Rodzaje zagrożeń

- nieuprawniona modyfikacja informacji
- kradzież istotnych informacji: cenne i poufne informacje trafiają w niepowołane ręce
- zniszczenie fizyczne: np. kopii bezpieczeństwa czy sprzętu
- powielenie komunikatu: np. przelewu
- podszycie się pod inną osobę
- zaprzeczenie wykonania operacji
- sabotaż zasobów: kradzież sprzętu , obciążenie sieci w celu uniemożliwienia przesyłania danych
- niedbalstwo użytkowników

- **...szantaż: haker zażądał od jednego z banków niemieckich (Verbraucherbank) miliona marek za nie ujawnianie danych o kontach klientów..**
- **...wysuwane są również żądania okupu za nie ujawnianie ukrytych programów, mogących siać spustoszenie w systemach należących do ofiary.**
- **...sabotaż przemysłowy ...ataki mające na celu obniżenie sprawności funkcjonowania infrastruktury informatycznej konkurenta lub spadek zaufania do firmy, nie mogącej zapewnić bezpieczeństwa danych klientów**
- **Najgroźniejsi okazują się pracownicy firmy (np. chowający urazę za złe traktowanie): programista jednej z amerykańskich firm odchodząc od swego dotychczasowego pracodawcy pozostawił program (bombę cyfrową), regularnie niszczący nowe projekty.**
  Firma poniosła straty w wysokości 10 mln $

Kod złośliwy

- Bomba logiczna
- Backdoor
- Wirus
- Robak internetowy
- Koń trojański
- keylogger
- rootkit

Spam

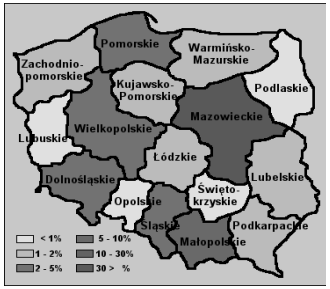
- Niechciana i nie zamawiana poczta e-mail
- Skutecznie blokuje łącza i skrzynki pocztowe
- Około 85% przysyłanych wiadomości stanowi spam (cyberatlas.com)
- Spam powoduje globalne koszty w wysokości około 20,5 miliarda $ (MessageLabs) 2008
- Coraz częściej istnieją porozumieniach między twórcami wirusów a spamerami...
- Nowe technologie: robak rozsyłający spam na telefony komórkowe

Programy antyspamowe

- Coraz częściej poczta nie dociera bo jest traktowana jako spam
- Bywają kłopoty z połączeniem
- Ważne wiadomości nie docierają lub są oznaczane jako spam
- W ramach walki ze spamem czytane są listy
- i kasowane zaszyfrowane pliki lub załączniki
- np.
  - Z konferencji BiN wrzesień 2004
  - *80% spamu nasz program likwiduje*
  - *Zaszyfrowane załączniki i maile kasujemy*
  - *Resztę korespondencji czytamy żeby wiedzieć czy to nie spam*
- *Obecnie coraz więcej maili nie dociera przykład to miejsce*

Penetracje systemów

http://arakis.cert.pl/



- Exploity wykorzystujące znane podatności
- Coraz krótszy czas na przygotowanie „łatki”
- Automatyzacja ataków (komputery „zombie”)
- Nowe rodzaje ataków (Wi-Fi, Bluetooth)

Inżynieria społeczna

- „Insiders” – szpiedzy podstępnie wprowadzani do firm
- Podszywanie się pod inne osoby (praktykant, nowy administrator, laik komputerowy…)
- Biały Wywiad, Dump Diving

83% brytyjskich użytkowników komputerów zgodziło by się podać swoje hasło w zamian za Snickersa (RSA Security)

Oszustwa

- Kradzieże tożsamości
- Fałszywe e-maile z prośbą o podanie haseł, kodów PIN
- Poszukiwanie informacji poprzez czaty, listy dyskusyjne, strony prywatne
- Oszustwa na aukcjach internetowych
- Liczba oszustw systematycznie rośnie

Obraźliwa i nielegalna treść

- Pornografia & pedofilia
- Promowanie brutalności, terroryzmu, rasizmu a nawet anoreksji
- Edukacja anarchistyczna (jak zaatakować strony, zbudować bombę itp.)
- Nielegalne transakcje (paserstwo, broń, narkotyki, ale też handel ludźmi czy organami...)

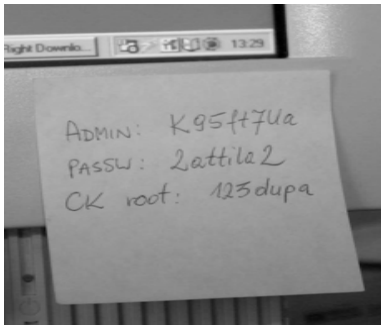
Największe włamania...

są oraz pozostaną tajemnicą, lecz wiadomo że:

- Wiele banków znajduje w swoich systemach konie trojańskie
- e-przedsiębiorstwa niespodziewanie tracą informacje o swoich klientach (np. numery kart kredytowych) czy też całe kontrakty
- Codziennie wiele witryn zostaje zaatakowanych
- Wiele komputerów jest wykorzystywanych bez wiedzy właścicieli (komputery zombie)
- wykryto próbę włamania na 700mln funtów
- Wykradziono bazę danych Rosyjskiego banku centralnego (50GB)

Przyczyny

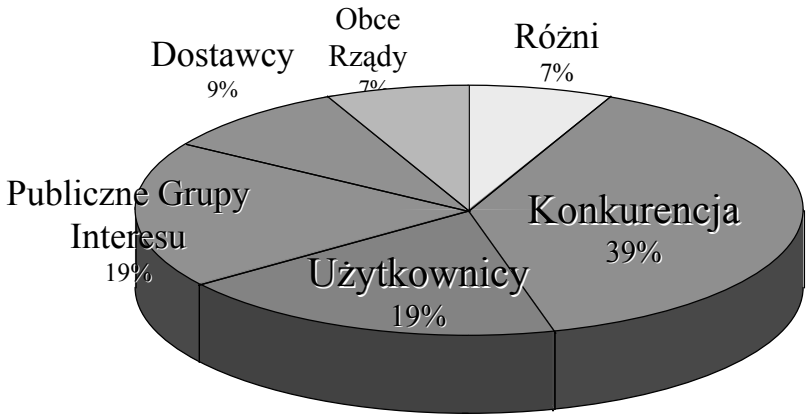
- Luki w wiedzy nt. bezpieczeństwa informacji większości użytkowników
- Brak środków na zabezpieczenia
- Setki nowych podatności
- Exploit „dnia zerowego”
- Nowe technologie
- Niska jakość oprogramowania
- Brak odpowiedzialności za produkty
- Walka konkurencyjna



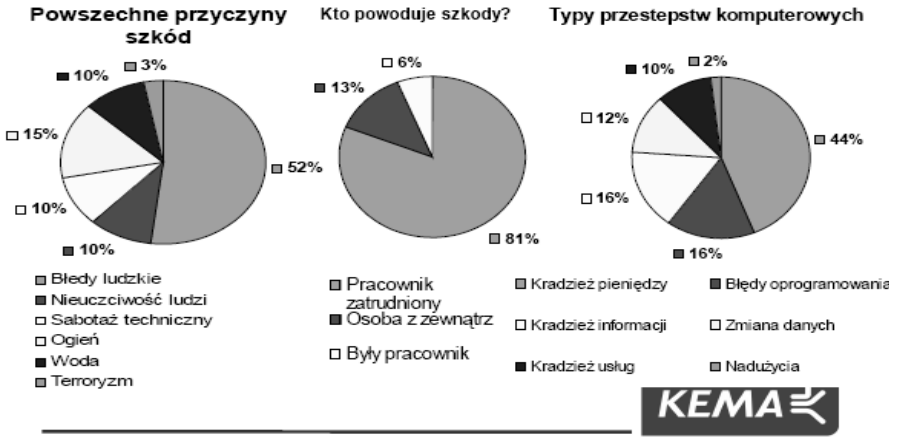
Kto dokonuje nadużyć ?

- Zewnętrzny uprawniony 15%
- Zewnętrzny nieuprawniony 10%
- Wewnętrzny nieuprawniony 17%
- Wewnętrzny uprawniony 58%

Ataki zewnętrzne dokonywane są z wielu stron



Typowe straty



2007 CSI Computer Crime Survey

- 350mln $ strat przyrost prawie 200mln $
- 18% respondentów poddanych celowemu atakowi
- Nadużycia finansowe większe spowodowały większe straty niż wirusy
- Pewne zmniejszenie liczby incydentów (46% wobec 53% rok wcześniej)
- Liczba wtargnięć do komputerów wzrosła do 29% z 25% przypadków

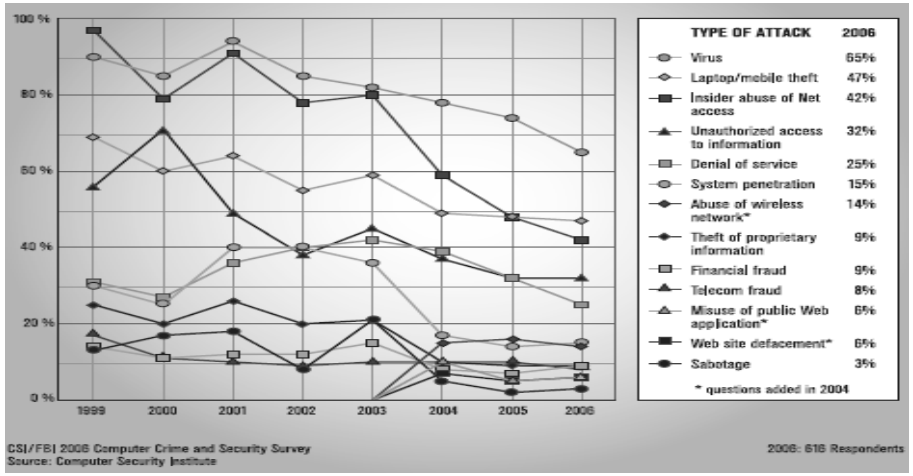
Liczba incydentów

- 2007 41 11 26 23

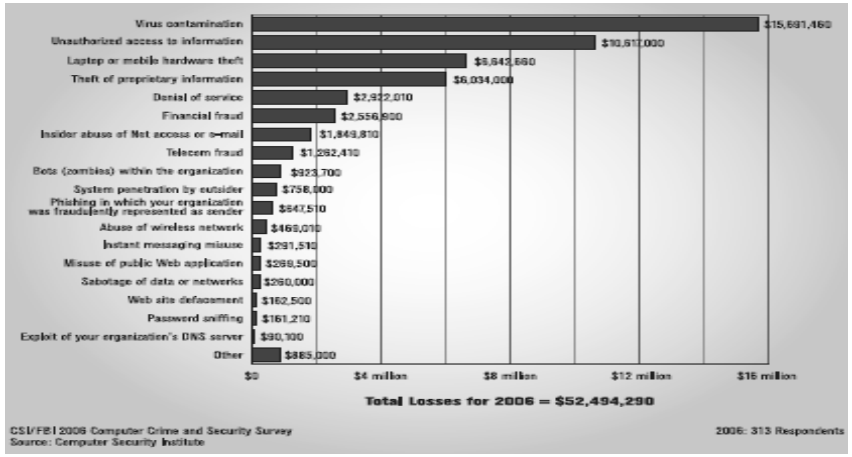
How many incidents, by % of respondents	1–5	6–10	>10	Don't know
2006	48	15	9	28
2005	43	19	9	28
2004	47	20	12	22
2003	38	20	16	26
2002	42	20	15	23
2001	33	24	11	31
2000	33	23	13	31
1999	34	22	14	29

CSI/FBI 2006 Computer Crime and Security Survey 2006: 341 Respondents
Source: Computer Security Institute

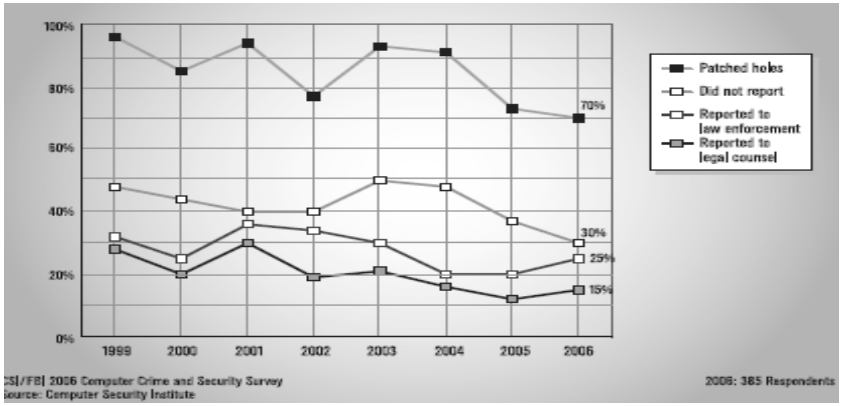
Typy ataków



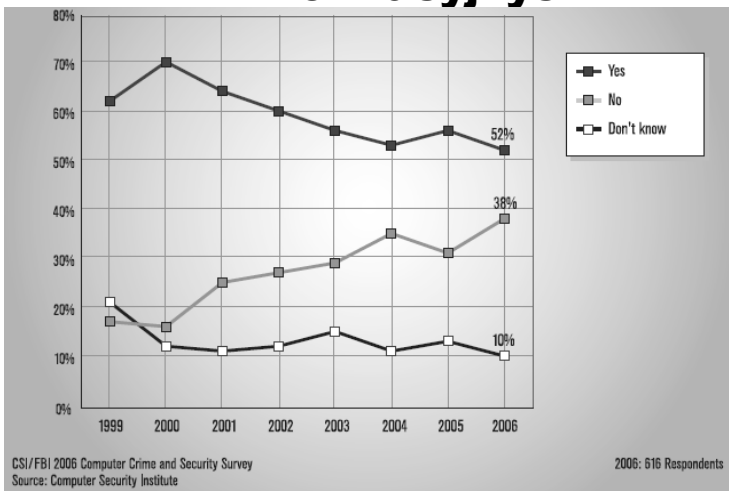
Wielkość strat



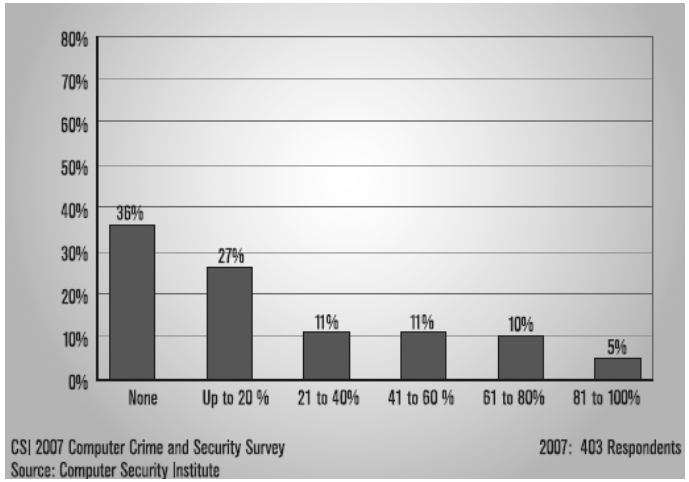
Podejmowane akcje po ataku



Nieautoryzowane użycie systemów informacyjnych



Straty od wewnętrznych zagrożeń



Wycieki informacji 2006

- **1. Gratis Internet Company zgromadziła poprzez internet dane osobowe 7 milionów Amerykanów, a następnie odsprzedała je osobom trzecim.**
- **2. Wyciek danych osobowych weteranów i żołnierzy amerykańskiej armii. maj**
- **3. Jeden z podwykonawców Texas Guaranteed zgubił laptop z danymi osobowymi klientów firmy. maj**
- **4. Skradziono laptop pracownika Nationwide Building Society zawierający dane osobowe 11 milionów członków stowarzyszenia. sierpień**
- **5. Z biura Affiliated Computer Services (ACS) skradziono przenośny komputer zawierający dane osobowe pracowników firmy. październik.**

Problemy z Bezpieczeństwem informacji 2007, 2008

- 13 wypadków w Wielkiej Brytanii
  - Utrata danych 20mln podatników
  - 9 miesięcy opóźnienia w ściganiu pedofilów
  - Zgubienie kodów dostępu do systemu zawierającego dane 10mln obywateli
- Przerwanie kabla podmorskiego koło Sycylii
- Ataki hackerów na sieci energetyczne
- Problem z Visą a właściwie 2 razy problem
- Ataki fishingowe
- Awaria energetyczna w Szczecinie
- Ataki na strony rządowe
- Whaling
- Wojny w internecie (Estonia, Gruzja)

Wpadki w Bankach w Polsce 2008

- Problemy z fuzją PKO S.A. i BPH
- Życiorysy i listy motywacyjne kandydatów do pracy PKO S.A
- BRE 3mln zł – kradzież tradycyjna z wrzutni
  - (ale pewnie był przeciek)
- Fishing (WZB, PKO ....)
- Karta VISA problemy 2 razy w roku
- Nieuznawanie reklamacji (rekordzista Lukas Bank)
- Zniknięcie 500tys L.Wałęsy z Multibanku?
- 50tys. Pobranych z kont w czasie awarii połączenia do bankomatu

A co w roku 2009

- 10 mln $ z jednego banku przez kilkadziesiąt bankomatów
- Penetracje ambasad kilkudziesięciu krajów,
- Dostęp do serwerów myśliwca F35
- Awaria serwerów autoryzacji bankowej
- Awaria google – złe uaktualnienie
- Awaria sieci T-Mobile
- Problem Microsoftu z Zumi (nie istniejący dzień)
- 75% zwolnionych pracowników wynosi dane (ankieta)
- Sprytniejsi donoszą na nielegalne oprogramowanie
  - BSA się cieszy
- Ostatnio w jednym z banków w Polsce na godzinę konta zostały wyzerowane

Najbardziej krytyczne sprawy

Ochrona danych (klasyfikacja, identyfikacja i szyfrowanie) i zarządzanie podatnościami oprogramowania	73
Zgodność z politykami i przepisami prawa	63
Kradzieże tożsamości i wyciek prywatnych informacji	58
Wirusy i robaki	52
Udział kierownictwa, zarządzanie ryzykiem, lub wspomagające zasoby (ludzkie i finansowe)	47
Kontrola dostępu	43

Najbardziej krytyczne sprawy[2]

Nauczanie, szkolenie i uświadamianie użytkowników	43
Bezpieczeństwo sieci bezprzewodowych	41
Wewnętrzne bezpieczeństwo sieciowe	38
Oprogramowanie szpiegowskie (spyware)	34
Inżynieria społeczna	33

Najbardziej krytyczne sprawy [3]

Przenośne urządzenia (palmtopy)	27
Oszustwa i oszukańczy kod	20
Uaktualnienia	16
Atak dnia zerowego	16
IDS (systemy wykrywania intruzów)	15

Najbardziej krytyczne sprawy [4]

Komunikatory	15
Ataki pocztowe (e-mail) – spam	15
Nadużycia pracowników	12
Bezpieczeństwo fizyczne	10
Ataki sieciowe	9

Najbardziej krytyczne sprawy [5]

Autentyfikacja dwu składnikowa	9
Bots i botnets	7
Odzyskiwanie po katastrofie (disaster recovery)	7
Ataki DoS	7
Bezpieczeństwo końcowego użytkownika	6

Najbardziej krytyczne sprawy [6]

Zarządzanie usługami bezpieczeństwa (cybersecurity provider)	5
Wdrażanie PKI	4
Rootkits	3
Sniffing	3
Zarządzanie konfiguracją i standaryzacja	3

Zagrożenia sieciowe 2009

- Ataki na portale społecznościowe
  - 19%
- Technologie
  - SQL Injection
  - Cross site scripting XSS worms
    - Np., na Twitterze udało się przejąć hasło prezydenta Obamy
- Przyczyny
  - Nie sprawdzanie danych wejściowych
  - Zła konfiguracja baz danych
  - Dodawanie niepotrzebnych funkcjonalności i nie sprawdzanie ich bezpieczeństwa
  - Technologia web2
  - Udostępnianie baz na zewnątrz
  - Brak przeszkolenia w tworzeniu bezpiecznych aplikacji

Zagrożenia sieciowe to nie wszystko!

- Sprawcy
  - Kryminaliści głównie chodzi o pieniądze
  - Ataki ideologiczne na przeciwników politycznych
  - Agencje rządowe?
  - Tradycyjnych hackerów już prawie nie ma
    - No może script kids
- A ostatnio
  - Awarie energetyczne (Chile 90% kraju)
  - Pobranie 5 mln zł na podrobionych dokumentach (Polska)
  - Złamanie bezpieczeństwa kart chipowych w czytnikach → na stronie
  - Robak stuxnet – ataki na infrastrukturę przemysłową