CYBERPRZESTĘPCA

KTO TO JEST…

Prelegent:
Starszy Specjalista w Zespole Łączności i Informatyki
Komendy Miejskiej Policji w Zabrzu
inż. Krystian ŚLUSAREK
krystian.slusarek@slaska.policja.gov.pl
krystian.slusarek@gmail.com

WSTĘP

„Cyberprzestępczość już dojrzała i przekształciła się w ogromny biznes. Przestępcy mogą szybko zarobić ponosząc minimalne ryzyko, przez co ich szeregi cały czas rosną. Wraz z rozwojem technologii wzrasta też liczba okazji dla przestępców - okazji mających globalny charakter, nieograniczony geograficznie zasięg i nie znających barier językowych.”

Greg DAY, analityk ds. bezpieczeństwa w firmie McAfee

PRZYCZYNY i SKUTKI

Przyczyny

- niska świadomość problemu
- lekceważenie problematyki bezpieczeństwa
- nieprzystosowanie i niedostosowanie społeczne potencjalnych ofiar
- globalna recesja
  - ✓ rozproszenie uwagi instytucji rządowych
  - ✓ niedobór specjalistów, zwolnienia
  - ✓ bariera granic – możliwość wykorzystania różnic w regulacjach prawnych
- różnice poglądów politycznych (działania cyberterrorystyczne)
- gospodarcze (budowanie stref wpływów)
- osobiste (złe relacje międzyludzkie, konflikty, rozpad rodzin)
- chęć szybkiego i łatwego zysku

PRZYCZYNY i SKUTKI

Skutki

- społeczne
  - ✓ budowa / prowokowanie określonych zachowań określonych grup
- zdrowotne
- gospodarcze
  - ✓ przechwytywanie rozwiązań
  - ✓ wprowadzanie przedsiębiorstw w określone stany finansowe
  - ✓ spowalnianie rozwoju naukowego / gospodarczego
- polityczne
  - ✓ skutkujące wobec jednostek
  - ✓ skutkujące wobec ugrupowań / państw
- militarne

http://mrmgr.pl/index.php/2009/09/spoleczno-ekonomicze-skutki-piractwa-komputerowego/

ALE JAK…?

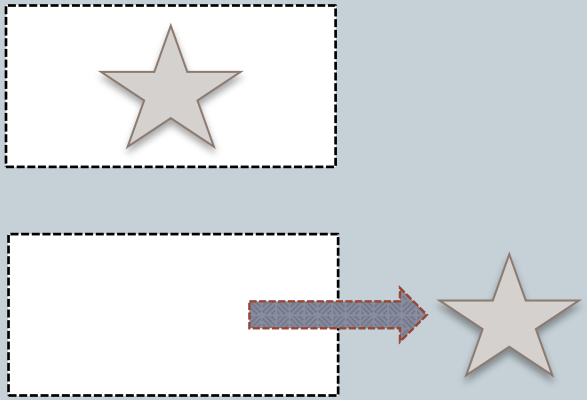
Czy cyberprzestępstwo
można popełnić
tylko przy użyciu komputera?

… I ZNÓW SKUTKI!

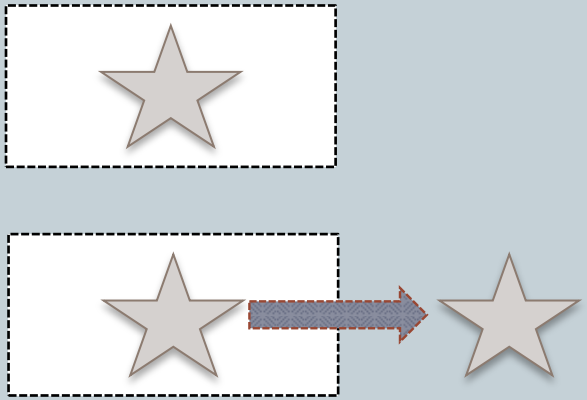
Efekt Wertera – znaczący wzrost samobójstw spowodowany nagłośnieniem w mediach samobójstwa znanej osoby. Efekt Wertera to po prostu fakt związany z "zaraźliwością" samobójstw. Dotyczy to także małych społeczności (np. szkół) i rodzin.

LEGALNOŚĆ OPROGRAMOWANIA

KRADZIEŻ



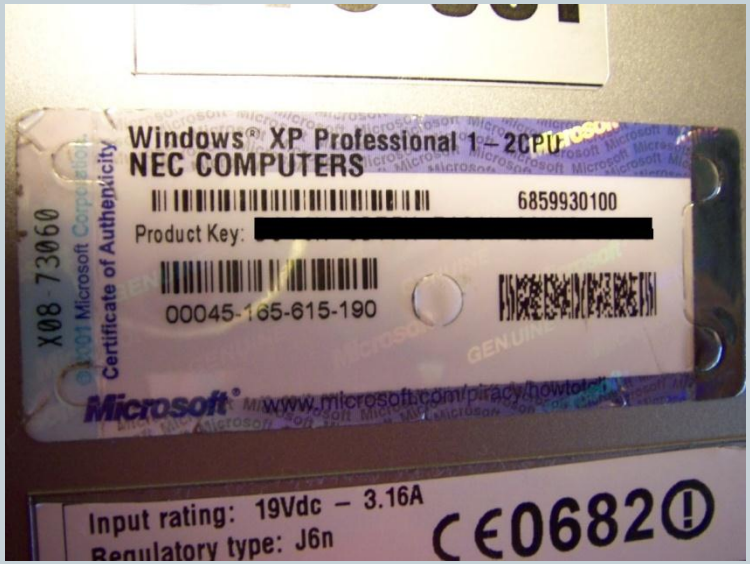
PIRACTWO



LEGALNOŚĆ OPROGRAMOWANIA

Jak rozpoznać legalne...?

- instrukcje załączone do leganie zakupionego oprogramowania
- sprzedawcy oprogramowania
- strony producentów oprogramowania
  - ✓ http://www.microsoft.com/poland/sam/partnerguide/licencje/strona_04.mspx



LEGALNOŚĆ OPROGRAMOWANIA

Przykłady licencji na użytkowanie oprogramowania

- zamknięte
  - OEM
  - BOX
- otwarte
  - GNU GPL (GNU General Public License – Powszechna Licencja Publiczna GNU)
    - ✓ wolność uruchamiania programu w dowolnym celu
    - ✓ wolność analizowania, jak program działa i dostosowywania go do swoich potrzeb
    - ✓ wolność rozpowszechniania niezmodyfikowanej kopii programu
    - ✓ wolność udoskonalania programu i publicznego rozpowszechniania własnych ulepszeń, dzięki czemu może z nich korzystać cała społeczność
  - Affero GPL – gdy oprogramowanie uruchamiane jest po stronie serwera
  - BSD

ZAGROŻENIA

- wirusy [przykłady]
  - ✓ pasożytnicze
  - ✓ towarzyszące
  - ✓ polimorficzne i metamorficzne
  - ✓ robaki
  - ✓ króliki
  - ✓ bakterie
  - ✓ bomby logiczne
  - ✓ bootnet
  - ✓ i wiele innych…

Po co mi ten program antywirusowy?

„Leczenie” – trudne, często niemożliwe – obecność wirusa niemal w 100% wypadków pociąga za sobą straty…

A Twoje dane… jak bardzo są ważne?!

ZAGROŻENIA

- kradzież tożsamości

  Kradzież tożsamości (ściślej fałszerstwo tożsamości) jest to celowe używanie danych osobowych innej osoby, adresu zameldowania, numeru PESEL, danych logowania do określonych systemów itp. w celu uzyskania nieuprawnionego dostępu do pewnych usług lub zasobów. Najczęściej celem uzyskania takiego dostępu jest chęć zdobycia korzyści – najczęściej majątkowych – kosztem ofiary której tożsamość została skradziona (sfałszowana).

Często traktowana jako błahostka. Nic gorszego. Podszywający się pod tożsamość realnej osoby przestępca potrafi spowodować nie tylko nieprzyjemności w kontaktach z rodziną i znajomymi ale również narazić nas na poważne straty finansowe...

ZAGROŻENIA

- stalking

  złośliwe i powtarzające się nagabywanie, naprzykrzanie się, czy prześladowanie, zagrażające czyjemuś bezpieczeństwu

- zapobieganie
  - ✓ nie ujawnianie swoich prawdziwych danych osobowych
  - ✓ analizowanie treści (w tym zdjęć) umieszczanych na portalach społecznościowych
  - ✓ uświadamianie dzieci – rozmowa → informowanie rodziców → reagowanie
  - ✓ potwierdzanie wiarygodności otrzymywanych drogą elektroniczną informacji
  - ✓ spotkania z osobami poznanymi w sieci… - poważne zagrożenie zwłaszcza dla nieletnich…
  - ✓ ostrożne postępowanie z pocztą elektroniczną (załączniki, łącza itp.)
  - ✓ hasła – po coś je wymyślono…

ZAGROŻENIA

- spam

  Spam to inaczej określenie niechcianych lub niepotrzebnych wiadomości elektronicznych najczęściej rozpowszechnianych za pomocą poczty elektronicznej.

- skutki
  - ✓ zatyka łącza
  - ✓ pochłania czas
  - ✓ generuje koszty
  - ✓ przenosi wirusy i… inne złośliwe oprogramowanie

- zapobieganie…
  - ✓ stosowanie oprogramowania antywirusowego mającego możliwość współpracy z klientem poczty elektronicznej
  - ✓ filtrowanie wiadomości
  - ✓ aktualizowanie oprogramowania do obsługi poczty (i nie tylko)
  - ✓ „pozytywne” nie reagowanie na spam
  - ✓ wyłączanie funkcji oprogramowania pocztowego podatnych na spam

ZAGROŻENIA

- zapobieganie c.d.
  - ✓ rozważne podejmowanie decyzji o rejestracji w serwisie internetowym
  - ✓ antyspamowy zapis adresu e-mail (krystian.slusarek@gmail.wytnijtoito.com)
  - ✓ stosowanie klientów poczty elektronicznej o małej popularności (np. Sylpheed)

ZAGROŻENIA

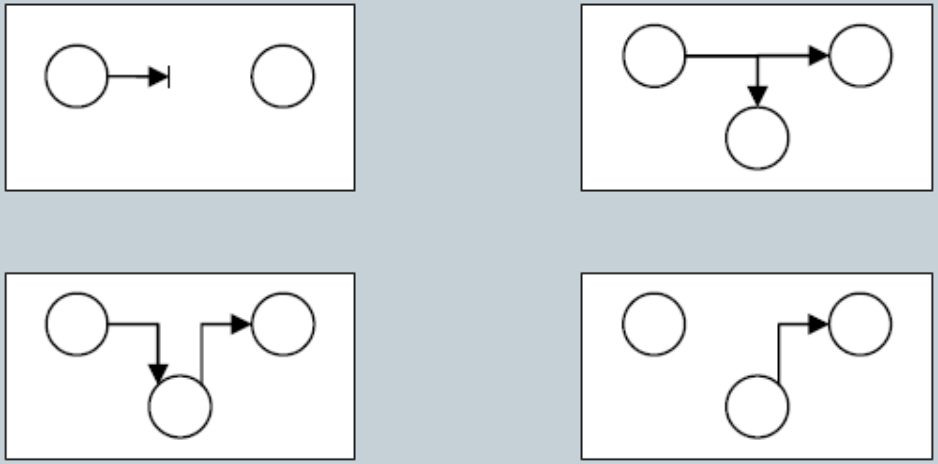
- pornografia
  - ✓ filtrowanie zawartości – specjalistyczne oprogramowanie
  - ✓ blokowanie dostępu do serwisów prezentujących twardą pornografię o z góry znanych adresach sieciowych,
  - ✓ reagowanie – kontakt z administratorami poczty elektronicznej

Przekazywanie treści pornograficznym może odbywać się różnymi kanałami. Może to być:

- poczta internetowa
- banery reklamowe
- komunikatory internetowe
- popularne portale społecznościowe lub…
- …ich pornograficzne odpowiedniki!
- i wiele innych…

ZAGROŻENIA

- ataki z sieci
  - ✓ zróżnicowane cele oraz typy



  - ✓ zróżnicowane skutki
    - niewielki dyskomfort, małe straty, łatwe przywrócenie sprawności systemu
    - gigantyczne straty, utrata danych, trudne lub niemożliwe przywrócenie sprawności systemu

ZAGROŻENIA

- ataki z sieci
  - ✓ obrona
    - firewall
    - IPS
    - IDS
    - NAT
    - obrona przed warfaringiem – WPA, WPA/PSK, WEP
    - szyfrowanie danych
      - TrueCrypt
      - Keyparc
      - Enigma 2003
      - DiskCryptor

ANONIMOWOŚĆ

Czy anonimowość w sieci jest realna?

Jak zachować możliwie wysoki stopień anonimowości i co cebula ma wspólnego z Internetem