

Przestępstwa komputerowe



**KOMPUTER JEST JEDNOCZEŚNIE NARZĘDZIEM I CELEM ATAKU
(PRZESTĘPSTWA)**

Kinga Dzedzic

Definicja przestępstwa komputerowego



Przestępstwo komputerowe – pospolita nazwa przestępstw, których narzędziem lub przedmiotem sprawczym jest komputer lub inne urządzenie elektroniczne.

Wykorzystanie komputerów w celu, np. kradzieży pieniędzy, towarów, programów, danych, szpiegostwa gospodarczego bądź technologicznego, może wypełniać znamiona przestępstw zbiorczo zwanych komputerowymi, właśnie ze względu na wykorzystanie urządzeń elektronicznych.

**Za przestępstwa komputerowe grozi od 3
miesiący do 5 lat lub nawet 10 lat
wiezienia.**



Traktat Rady Europy ds. zagrożenia cyberprzestępczością

Definiuje pojęcie „przestępstwa komputerowe” jako działalność przestępczą przeciwko zawartości danych oraz łamaniu praw autorskich



Przykłady przestępstw komputerowych

Przestępstwa komputerowe uregulowane w Ustawie z dnia 6 czerwca 1997 r. Kodeks karny.

- **falszerstwa komputerowe**
- **uniemożliwianie lub utrudnianie dostępu do informacji, w tym *hacking***
- **przestępstwa karne skarbowe**
- **oszustwa komputerowe**
- **szpiegostwo komputerowe**
- **niszczenie danych lub programów komputerowych**

Na mocy ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

- **piractwo komputerowe**

Falszerstwa komputerowe

Występują w postaci:

- falszerstwa dokumentów klasycznych dokonywanych z wykorzystaniem komputera, oprogramowania i urządzeń Peryferyjnych
- falszerstw dokumentów elektronicznych polegających na wprowadzaniu zmian w bazie danych (kartoteki pojazdów, ewidencje magazynowe, księgi podatkowe itp.)

Przestępstwa przeciw ochronie informacji.

Regulacje dotyczące tych przestępstw ustawodawca zamieścił w rozdziale XXXIII k.k. „Przestępstwa przeciw ochronie informacji” (art. 265-269).



Przestępstwa przeciw ochronie informacji.

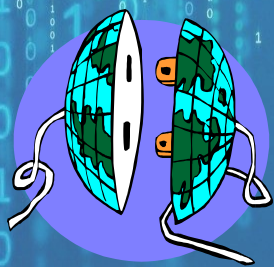
Wyróżnić możemy tutaj:

- ❖ **hacking komputerowy**
- ❖ **nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych**
- ❖ **naruszenie integralności komputerowego zapisu informacji**
- ❖ **Sabotaż komputerowy**

Hacking komputerowy (włamanie)

Nieuprawnione wejście do sieci komputerowej poprzez pokonanie zabezpieczenia w postaci kodów i haseł broniących dostępu do nagromadzonych i przetworzonych informacji.

(grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat 2.)



Nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych

Polega na zakładaniu lub posługiwaniu się urządzeniami podsłuchowymi, wizualnymi albo innymi urządzeniami specjalnymi w celu uzyskania informacji, do której nie jest się uprawnionym.
(grzywna lub kara ograniczenia bądź pozbawienia wolności do dwóch lat.)

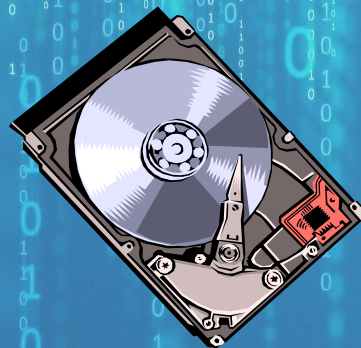


**(grzywna lub kara ograniczenia bądź
pozbawienia wolności do dwóch lat)**



Naruszenie integralności komputerowego zapisu informacji (art. 268 § 2 k.k.).

Chodzi tutaj o naruszenie integralności komputerowego zapisu informacji, które może nastąpić wskutek bezprawnego niszczenia, uszkodzania, usuwania lub zmiany zapisu istotnej informacji albo udaremniania czy utrudniania osobie uprawnionej zapoznanie się z nią. Takie działanie zagrożone jest karą pozbawienia wolności do lat 3.



Sabotaż komputerowy

Ostatnie z przestępstw rozdziału XXXIII, które polega na doprowadzeniu do sparaliżowania systemu komputerowego, zakłócaniu lub paraliżowaniu funkcjonowania systemów informatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli.

Sabotaż komputerowy może wystąpić również w formie niszczenia lub wymiany nośnika informacji, niszczenia albo uszkodzenia urządzeń służących do automatycznego przetwarzania, gromadzenia bądź przesyłania informacji

Przestępstwa przeciwko mieniu

Do przestępstw przeciwko mieniu ustawodawca (w Rozdziale XXXV k.k.) zaliczył także cztery rodzaje przestępstw komputerowych.

Są to:

- oszustwo komputerowe,***
- kradzież programu komputerowego,***
- paserstwo komputerowe oraz***
- podłączenie się do urządzenia telekomunikacyjnego.***

Oszustwa komputerowe

Szeroko rozumiana ingerencja (manipulacja) w komputerowy nośnik informacji (wprowadzenie do systemu informatycznego nieprawdziwych danych) w celu uzyskania nienależnych korzyści majątkowych lub wyrządzenia innej osobie szkody.

Najczęstszymi formami popełnienia oszustwa komputerowego (rodzajami manipulacji) są:

Oszustwa komputerowe

➤ **manipulacja danymi (input manipulation) — sprawcą tego rodzaju przestępstwa jest najczęściej operator systemu lub inna osoba włamująca się do systemu komputerowego**

➤ **manipulacja programem (software manipulation) — jest możliwa po dokonaniu jego modyfikacji, w taki sposób, aby można było dokonywać określonych operacji niezależnie od woli obsługującego komputer (przykład: metoda salami)**

➤ **manipulowanie urządzeniami peryferyjno – systemowymi (czyli manipulowanie wynikiem – rezultatem np. wydrukiem).**

Kradzież programu komputerowego

Kradzież programu komputerowego ma miejsce wtedy, gdy przestępca w jakikolwiek sposób zdobywa program komputerowy (np. kopiowanie, zabranie dyskietki lub innego nośnika) nie mając na to wyraźnej zgody (np. licencji) osoby uprawnionej według prawa autorskiego (np. twórcy programu).



Przestępstwa przeciwko Rzeczypospolitej Polskiej

Kodeks karny w **Rozdziale XVII** reguluje dwa rodzaje przestępstw komputerowych, które ze względu na swój charakter mieszczą się w tym właśnie katalogu. Jest to uprzywilejowana forma szpiegostwa – **szpiegostwo komputerowe oraz szpiegostwo komputerowe na szkodę państwa sojuszniczego.**

W jednej i w drugiej formie **przedmiot** przestępstwa jest taki sam zmieniają się jedynie jego **podmioty.**

Regulację w tym zakresie zawiera art. 130 § 3 k.k.

Szpiegostwo komputerowe

Polega na pokonaniu zabezpieczeń i nieuprawnionym wejściu w system komputerowy w celu skopiowania danych zawartych w systemach komputerowych (kartoteki, wyniki badań, adresy klientów i inne).

Regulację w tym zakresie zawiera art. 130 § 3 k.k.

Niszczenie danych lub programów komputerowych.

Podział ze względu na rodzaj dokonania przestępstwa:

- **dokonane w sposób fizyczny (np. wysadzenie w powietrze komputera)**
- **dokonane za pomocą programów komputerowych, np.:**
 - **wirusy komputerowe**
 - **konie trojańskie**
 - **bomby logiczne**

Wirusy komputerowe

Programy komputerowe, które rozpowszechniają się na zasadzie porównywalnej z infekcją i wykonują określone funkcje

- ✓ mogą one oddziaływać na dowolny element systemu komputerowego
- ✓ usunięcie wirusa z jednego miejsca jest nieskuteczne
- ✓ krąg sprawców jest nieograniczony



ALERT
VIRUS DETECTED!!
ALERT



Konie trojańskie

Polega na umieszczeniu nielegalnych instrukcji komputerowych w programie użytkowym

- komputer wykonuje zamierzony cel programu i „wmontowane” operacje
- jest to najczęstsza i trudna do wykrycia metoda dokonywania oszustw i sabotażu oparta na programie komputerowym

Piractwo komputerowe

Na mocy Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i
prawach pokrewnych

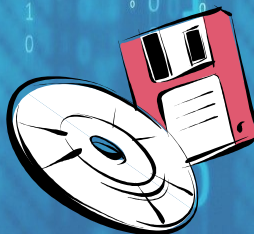
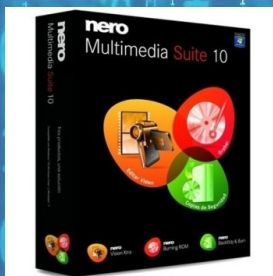
PRAWA AUTORA

do programu komputerowego są chronione jako

WŁASNOŚĆ INTELEKTUALNA.

Do najbardziej rozpowszechnionych przestępstw związanych
z technologią informatyczną bez wątpienia należy tzw.

„PIRACTWO KOMPUTEROWE”.



Piractwo komputerowe

Piractwo - to kopiowanie, reprodukcja, używanie i wytwarzanie bez zezwolenia produktu chronionego przez prawo autorskie.

Należy sobie zdać sprawę z tego, że tzw.

„piractwo komputerowe”

jest niczym innym jak charakterystyczną - ze względu na specyfikę programu komputerowego - kradzieżą.

Wykonywanie dodatkowych kopii oprogramowania,

Instalacja na twardym dysku (np. systemu od znajomego),

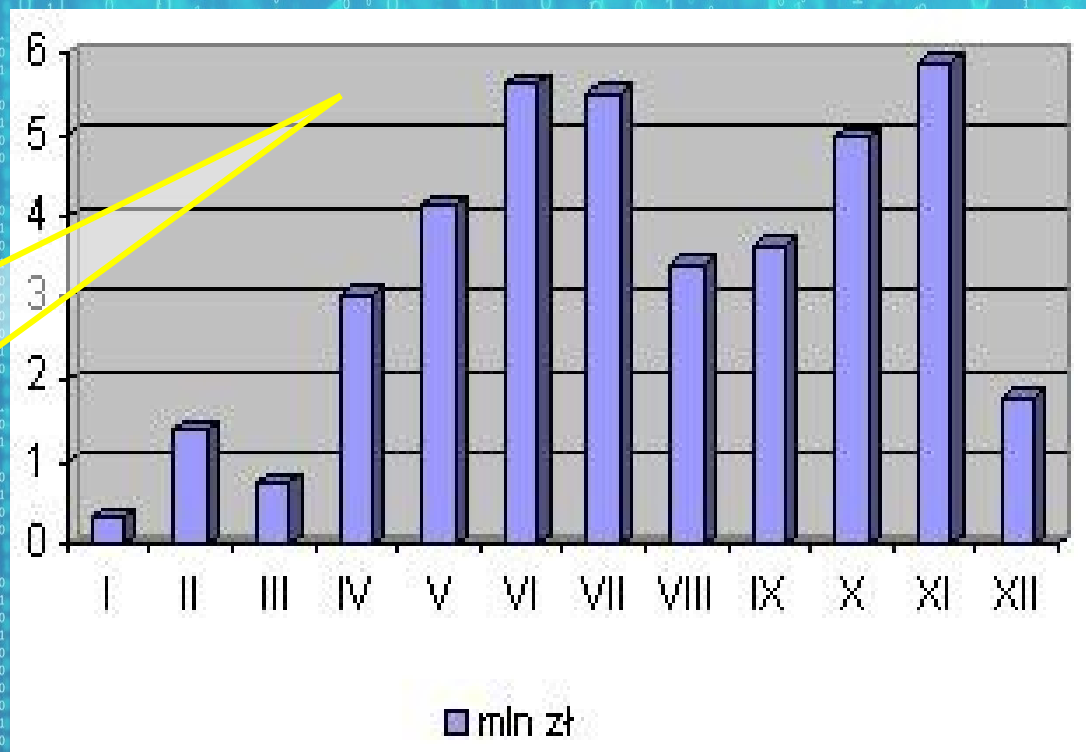
Fałszowanie (używanie cracków i nr seryjnych w celu uzyskania nieograniczonej wersji danego programu),

Umieszczanie na serwerach pełnych wersji oprogramowania w celu udostępniania innym – np. sieci p2p, Wynajem oprogramowania

Piractwo komputerowe

STRATY PRODUCENTÓW

Jak widzimy straty w skali roku są ogromne. Piractwo nasila się w okresie wakacyjnym oraz jesienią



Wykres przedstawia skalę strat producentów

w okresie od stycznia do grudnia 2010 r.

Zapobieganie przestępstwom komputerowym

Sposoby podnoszenia bezpieczeństwa wg FBI

1. Używanie mocnych haseł - trudnych do odgadnięcia
2. Regularne kopiowanie najważniejszych danych
3. Używanie oprogramowania antywirusowego
4. Używanie firewall między komputerem, a Internetem
5. Odłączanie nieużywanych komputerów od Internetu
6. Nie otwierać załączników pocztowych od nieznanomych
7. Regularna aktualizacja i uzupełnianie oprogramowania



Zwalczanie przestępstw komputerowych.

Spośród przestępstw komputerowych największe obawy wzbudzają działania w sieci, głównie w Internecie, którego ogrom i decentralizacja pozwala na dużą swobodę działań przestępczych.

Zgłoszenia dotyczące naruszeń bezpieczeństwa w Sieci przyjmuje organizacja CERT Polska.

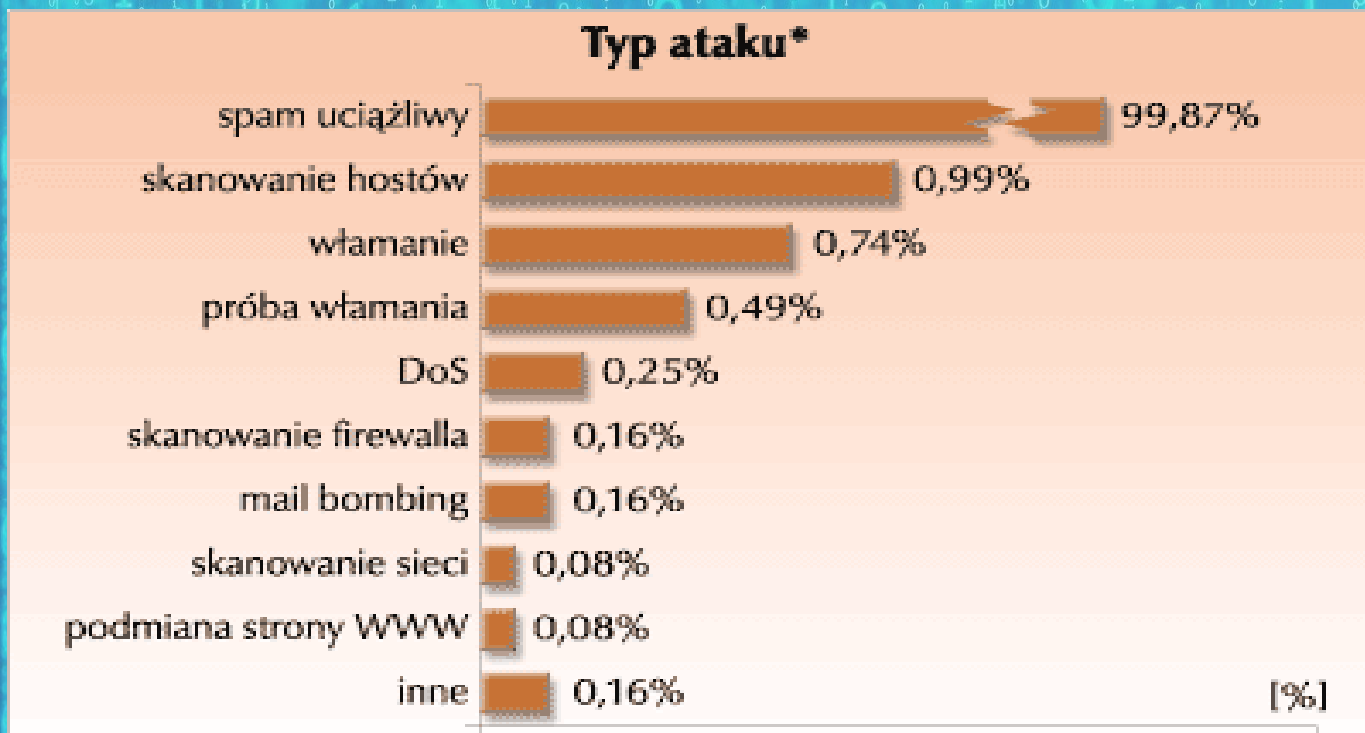


Zwalczanie przestępstw komputerowych.

Computer Emergency Response Team Polska – jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 r. Do głównych zadań zespołu należy rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo, alarmowanie użytkowników, prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu, testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

C
E
R
T

Zwalczanie przestępstw komputerowych.



Raport CERT NASK

- najczęściej występujące typy ataków komputerowych

Źródło

- <http://www.uplook.net/przestepstwa-komputerowe/>
- http://www.bryk.pl/wypracowania/pozosta%C5%82e/informatyka/15854-przest%C4%99pstwa_komputerowe.html
- http://pl.wikipedia.org/wiki/Przest%C4%99pstwo_komputerowe
- <http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe>
- <http://vagla.pl/skrypts/przestepstwa.htm>

Dziękuję za uwagę ;)