Normy prawne dotyczące rozpowszechniania programów komputerowych oraz ochrony praw autorskich. Rodzaje licencji.

Wprowadzenie do przestępczości komputerowej

Definicja i istota przestępczości komputerowej

Zakres przestępczości komputerowej

Obejmuje działania przestępcze związane z elektronicznym przetwarzaniem danych i naruszeniem systemów.

Przykłady działań przestępczych

Nieuprawnione przelewy, kradzież danych, niszczenie informacji i włamania do systemów informatycznych.

Znaczenie problemu

Dynamiczny wzrost zagrożeń wymaga szczególnej uwagi w ochronie cyberprzestrzeni.

Wstępne omówienie istoty przestępczości komputerowej

DEFINICJA

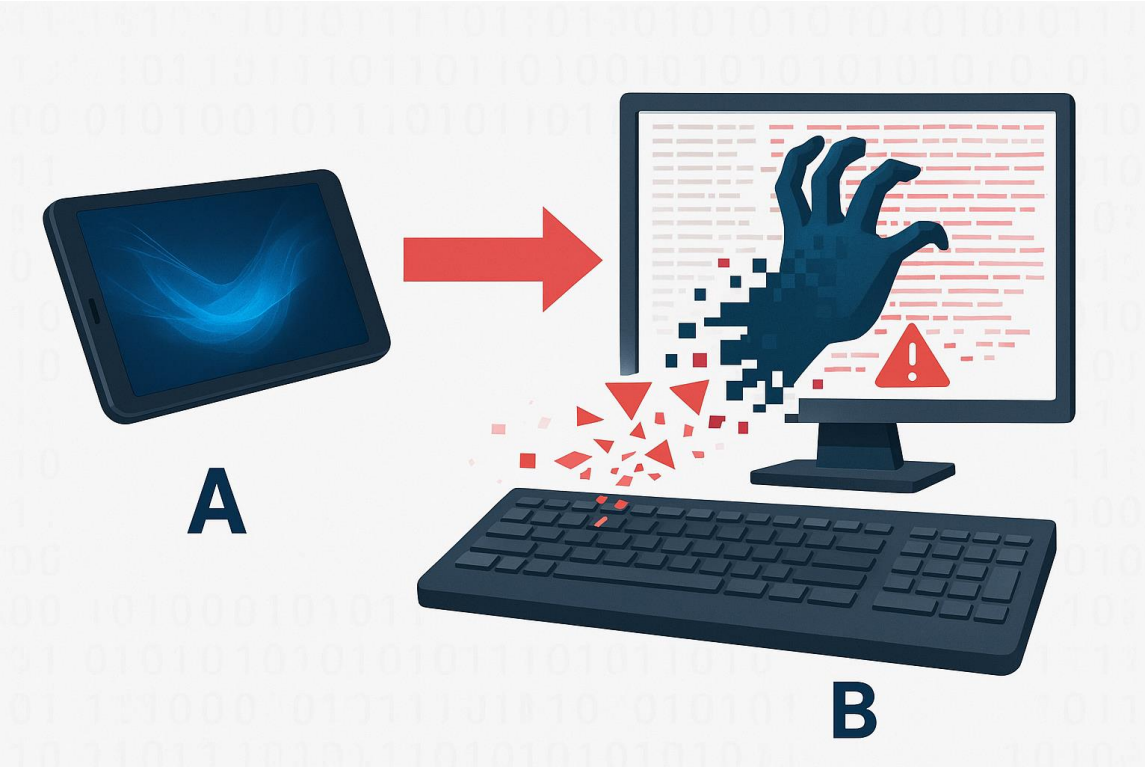
Przestępstwa komputerowe to wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer.

Wstępne omówienie istoty przestępczości komputerowej

Komputer A za pośrednictwem sieci Internet, wkrada się na komputer B (serwer banku) i dokonuje nieuprawnionego przelewu środków pieniężnych na swoje (lub inne) konto, bądź dokonuje zakupów w internetowym sklepie – komputer jest narzędziem służącym popełnieniu przestępstwa.

Wstępne omówienie istoty przestępczości komputerowej

Tablet A wkrada się do komputera B i niszczy znajdujące się tam informacje (dane) – celem ataku jest konkretny system komputerowy i znajdujące się tam informacje.



Rodzaje przestępstw komputerowych

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

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

Hacking komputerowy

Hacking to nieuprawnione uzyskanie informacji przez przełamanie zabezpieczeń systemów komputerowych.

Naruszenie integralności danych

Naruszenie integralności to bezprawne niszczenie, usuwanie lub zmiana danych zapisanych w systemach.

Podsłuch i inwigilacja

Podsłuch i inwigilacja wykorzystują urządzenia techniczne do nielegalnego pozyskiwania informacji.

Sabotaż komputerowy

Sabotaż komputerowy paraliżuje strategiczne systemy informatyczne, zagrażając bezpieczeństwu państwa.

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

<u>Wyróżnić możemy tutaj</u>:

- **<u>hacking komputerowy</u>** – to takie działanie sprawcy, który bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie.

(grzywna, kara ograniczenia wolności

albo pozbawienia wolności do lat 2.)

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

naruszenie integralności komputerowego zapisu informacji

(art. 268 § 2 k.k.). Naruszenie integralności komputerowego zapisu informacji, które może nastąpić wskutek bezprawnego niszczenia, uszkadzania, usuwania lub zmiany zapisu istotnej informacji albo udaremniania czy utrudniania osobie uprawnionej zapoznanie się z nią. Działanie zagrożone jest karą pozbawienia wolności do lat 3.

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

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).

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

Regulacja ta dotyczy przede wszystkim sytuacji podsłuchiwania rozmów telefonicznych oraz codziennych rozmów w pomieszczeniach. Ustawodawca, mówiąc o „innych urządzeniach specjalnych”, ma na myśli m.in.: mikrofony kierunkowe o wysokiej czułości, kamery, urządzenia podłączane do linii telefonicznej w celu przechwytywania danych.

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

Sabotaż komputerowy – to 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.

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

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

Podmieniona strona internetowa

Defacement to atak polegający na podmianie treści strony internetowej przez cyberprzestępców.
Najczęściej celem są serwisy z lukami w zabezpieczeniach (np. brak aktualizacji CMS, słabe hasła, brak firewalli aplikacyjnych).
Atakujący umieszczają własne komunikaty, grafiki lub propagandowe treści.

Przestępstwa przeciw wiarygodności dokumentów i obrotowi gospodarczemu

Fałszerstwo dokumentów komputerowych

Polega na podrobieniu lub przerobieniu dokumentów i użyciu ich jako autentycznych, co jest przestępstwem.

Niszczenie lub ukrywanie dokumentów

Nieuprawnione niszczenie lub ukrywanie dokumentów jest karalne i zagraża transparentności obrotu gospodarczego.

Fałszerstwo kart płatniczych

Obejmuje kradzież danych, manipulacje chipem lub ścieżką magnetyczną oraz kopiowanie informacji z kart płatniczych.

Konsekwencje prawne

Przestępstwa te są regulowane przez Kodeks karny i zagrożone kar pozbawienia wolności.

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

- **Przestępstwa przeciw wiarygodności dokumentów, obrotowi gospodarczemu i pieniężnemu.**

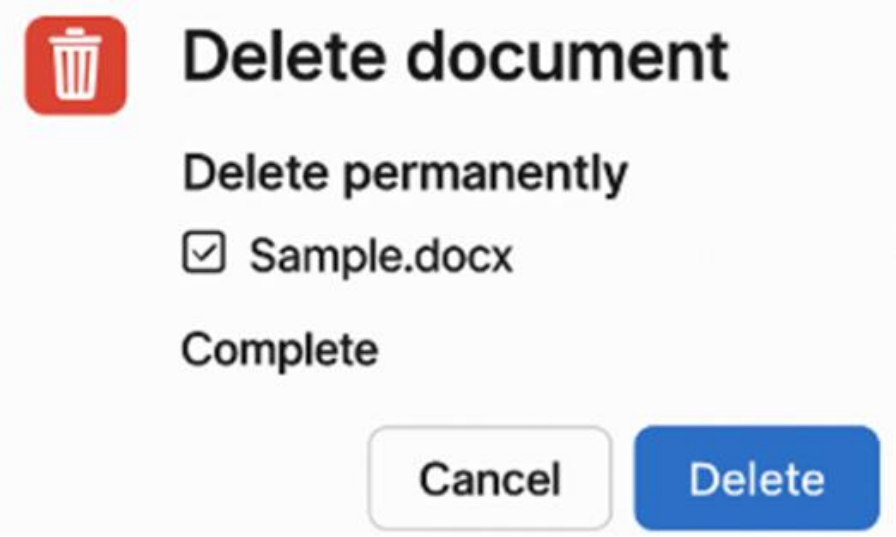
Przestępstwa tej kategorii ustawodawca zawarł w Rozdziale XXXIV k.k. :

Fałszerstwo dokumentu (sankcjonuje je art. 270 § 1 k.k.) dokonane przez osobę, która podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa (od 3 miesięcy do lat 5). **Jest to fałszerstwo komputerowego zapisu informacji stanowiącego dokument.**

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

Zniszczenie, uszkodzenie, ukrycie lub usunięcie dokumentu

(...) jest kolejnym przestępstwem przeciwko wiarygodności dokumentów. Polega na niszczeniu, uszkadzaniu, ukryciu lub usunięciu dokumentu przez osobę, która nie ma prawa nim rozporządzać.



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

Do przestępstw w tej kategorii, ze względu na jego przedmiot należy również zaliczyć przestępstwo z **Rozdziału XXXVI k.k**. „**Przestępstwa przeciwko obrotowi gospodarczemu**”. To: **Nierzetelne prowadzenie dokumentacji działalności gospodarczej** – art. 303 k.k.

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

Fałszerstwo kart płatniczych (Rozdział XXXVII) – art. 310 § 1 k.k.

Z reguły wiąże się z „kradzieżą” informacji, jaką jest numer karty i manipulowanie zapisem na jej ścieżce magnetycznej lub zapisem w „chipie”. Może ono przybrać postać podrobienia (np. skopiowanie zawartości ścieżki cudzej oryginalnej karty na czystą) lub przerobienia (zmiana zapisu danych).

Przestępstwa przeciwko mieniu

Kradzież programu komputerowego

Kradzież to bezprawne pozyskanie programu bez zgody jego właściciela, naruszające prawo autorskie.

Paserstwo komputerowe

Paserstwo może być umyślne lub nieumyślne, związane z handlem skradzionym oprogramowaniem.

Oszustwa komputerowe

Manipulacje w danych lub programach mające na celu korzyść majątkową lub wyrządzenie szkody.

Podłączenie do urządzenia telekomunikacyjnego

Nielegalne uruchomienie impulsów telefonicznych na cudzy rachunek jest formą przestępstwa telekomunikacyjnego.

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

- **Kradzież programu komputerowego**

Kradzież oprogramowania komputerowego ma miejsce wtedy, gdy osoba nieuprawniona pozyskuje, wykorzystuje lub rozpowszechnia program komputerowy bez zgody właściciela praw autorskich (np. twórcy, producenta lub licencjodawcy). Może to obejmować:

- Nielegalne kopiowanie oprogramowania z nośników fizycznych (np. pendrive, dysk zewnętrzny) lub cyfrowych (np. serwery, chmura),
- Nieautoryzowane pobieranie z internetu (np. z serwisów warez, torrentów),
- Ominięcie zabezpieczeń licencyjnych (np. crackowanie, użycie keygenów),

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

- **<u>Kradzież programu komputerowego</u>**

Kradzież oprogramowania komputerowego ma miejsce wtedy, gdy osoba nieuprawniona pozyskuje, wykorzystuje lub rozpowszechnia program komputerowy bez zgody właściciela praw autorskich (np. twórcy, producenta lub licencjodawcy).:

- Użycie oprogramowania bez ważnej licencji w środowisku komercyjnym lub edukacyjnym,
- Udostępnianie oprogramowania innym osobom bez prawa do sublicencjonowania. W świetle obowiązującego prawa (np. ustawy o prawie autorskim i prawach pokrewnych oraz międzynarodowych regulacji takich jak DMCA czy dyrektywy UE), takie działania są traktowane jako naruszenie praw autorskich i mogą skutkować odpowiedzialnością cywilną lub karną.

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

•**Paserstwo nieumyślne oprogramowania** występuje wtedy, gdy osoba nabywa, pomaga w zbyciu, ukryciu lub przyjmuje program komputerowy, nie mając świadomości, że pochodzi on z przestępstwa, ale powinna lub mogła przypuszczać, że został pozyskany nielegalnie. Przykłady takich sytuacji obejmują:

•Zakup oprogramowania z nieautoryzowanego źródła (np. giełda internetowa, portal aukcyjny) po rażąco zaniżonej cenie, bez dokumentacji licencyjnej,

•Instalacja programu z nośnika (np. pendrive, dysk zewnętrzny), którego pochodzenie jest niejasne lub podejrzane,

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

•**Paserstwo nieumyślne oprogramowania** występuje wtedy, gdy osoba nabywa, pomaga w zbyciu, ukryciu lub przyjmuje program komputerowy, nie mając świadomości, że pochodzi on z przestępstwa, ale powinna lub mogła przypuszczać, że został pozyskany nielegalnie. Przykłady takich sytuacji obejmują:

•Użycie oprogramowania udostępnionego przez osobę trzecią, która nie jest jego właścicielem ani licencjodawcą,

•Pobranie programu z serwisu oferującego pirackie wersje, bez weryfikacji legalności źródła.

W świetle prawa, brak świadomości co do przestępczego pochodzenia oprogramowania nie zwalnia z odpowiedzialności, jeśli można było przewidzieć, że program został pozyskany nielegalnie. Paserstwo nieumyślne może skutkować sankcjami cywilnymi lub karnymi, zwłaszcza w środowiskach zawodowych i edukacyjnych.

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

• **Paserstwo umyślne** oprogramowania występuje, gdy osoba świadomie nabywa, sprzedaje, ukrywa lub przechowuje program komputerowy, wiedząc, że pochodzi on z przestępstwa (np. został skradziony lub nielegalnie skopiowany). Przykłady:

•Sprzedaż w sklepie programu, o którym wiadomo, że jest piracki,

•Przyjęcie na przechowanie nielegalnego oprogramowania,

•Pomoc w ukryciu programu pochodzącego z kradzieży.

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

• **Oszustwa komputerowe.** polegają na celowym działaniu w celu uzyskania korzyści majątkowej lub wyrządzenia szkody poprzez nieuprawnioną ingerencję w:

•**Przetwarzanie danych** (np. manipulacja algorytmami),

•**Gromadzenie lub przesyłanie informacji**,

•**Zmianę, usunięcie lub dodanie danych** na nośniku lub w systemie.

Przykłady: fałszowanie zapisów w bazach danych, wprowadzanie nielegalnych transakcji, modyfikacja plików systemowych.
Kara: pozbawienie wolności od 3 miesięcy do 5 lat.

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

Oszustwa komputerowe polegają więc na szeroko rozumianej ingerencji (manipulacji) osób trzecich w komputerowy nośnik informacji, w celu

osiągnięcia korzyści majątkowej

lub

wyrządzenia innej osobie szkody.

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

W ramach oszustw komputerowych można wyróżnić trzy rodzaje manipulacji.

Będzie to:

- **manipulacja danymi** – wprowadzanie fałszywych informacji,
- **manipulacja programami** – ingerencja w kod programu,
- **manipulowanie urządzeniami peryferyjno – systemowymi**

(czyli manipulowanie wynikiem – rezultatem np. wydrukiem).

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

Mówi o tym art. 285 k.k.

- **<u>Podłączenie się do urządzenia telekomunikacyjnego</u>.**

Nielegalne uruchamianie impulsów telefonicznych polega na podłączeniu się do urządzenia telekomunikacyjnego (fizycznie lub systemowo) w celu obciążenia cudzym rachunkiem.
Może obejmować:

Podłączenie do linii lub aparatu telefonicznego,

Ingerencję w oprogramowanie urządzeń – dotyczy:

- Routerów, modemów LTE, urządzeń IoT.
- Ataków typu firmware injection, backdoor w urządzeniach sieciowych.

Sankcja: kara pozbawienia wolności do lat 3.

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

Mówi o tym art. 285 k.k.

- **Podłączenie się do urządzenia telekomunikacyjnego.**

Zagrożenie związane z modemami i podłączeniem do linii telefonicznej jest dziś w większości przypadków nieaktualne, ale nie całkowicie.: **Dlaczego jest w dużej mierze nieaktualne?** Klasyczne modemy analogowe (dial-up) praktycznie wyszły z użycia wraz z rozwojem szerokopasmowego internetu, LTE/5G i VoIP. Ataki polegające na wykorzystaniu numerów 0-800 do generowania kosztów były typowe dla lat 90 i początku 2000 r. **Kiedy może być nadal aktualne?** W środowiskach przemysłowych lub starszych systemach, gdzie modemy są używane do zdalnego dostępu (np. SCADA, urządzenia IoT w legacy systemach). W przypadku VoIP lub GSM bram, gdzie możliwe jest przekierowanie połączeń na numery premium (choć to bardziej fraud telekomunikacyjny niż klasyczny dial-up).

Sankcja: kara pozbawienia wolności do lat 3.

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

VoIP fraud i SIP trunk hijacking

VoIP fraud polega na przejęciu połączeń w systemach VoIP, umożliwiając obciążanie cudzych kont lub przekierowywanie rozmów.

SIM swapping

SIM swapping umożliwia przejęcie numeru telefonu przez zmianę karty SIM i dostęp do kont bankowych lub usług zabezpieczonych SMS.

Premium-rate fraud

Premium-rate fraud polega na przekierowywaniu połączeń na numery o wysokiej taryfie, generując znaczne koszty dla ofiary.

PBX hacking i nadużycia w chmurze

PBX hacking umożliwia manipulację centralami telefonicznymi, a cloud telephony abuse to podszywanie się pod użytkowników w telefonii IP.

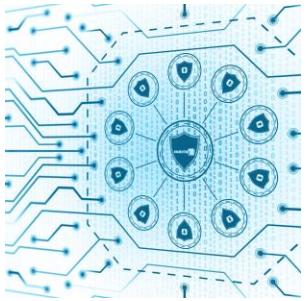
Szpiegostwo komputerowe

Definicja szpiegostwa komputerowego

Szpiegostwo komputerowe polega na nielegalnym zbieraniu i przekazywaniu strategicznych danych obcemu wywiadowi.

Regulacje prawne

Szpiegostwo komputerowe jest uregulowane w Kodeksie karnym, gwarantując surowe kary za takie działania.



Zagrożenie dla bezpieczeństwa

Działania szpiegowskie stanowią poważne zagrożenie dla bezpieczeństwa narodowego i są priorytetem służb specjalnych.

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

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**.

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

- **Szpiegostwo komputerowe.**

Szpiegostwo definiuje się jako działanie przestępne dokonywane na szkodę określonego państwa, polegające na wykonywaniu odpowiednich czynności na rzecz obcego wywiadu, a w szczególności na zbieraniu, przekazywaniu informacji organom obcego wywiadu lub na gromadzeniu i przechowywaniu informacji w celu przekazania obcemu wywiadowi.

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

Inne przestępstwa z wykorzystaniem komputerów

Rodzaje przestępstw komputerowych

Przestępstwa obejmują rozpowszechnianie zakazanych treści, groźby, zniesławienie i nawoływanie do przemocy z użyciem komputerów.

Przykłady działań nielegalnych

Publikowanie treści zakazanych i obraźliwych komentarzy w Internecie to przykłady wykorzystywania technologii do popełniania przestępstw.

Ściganie i sankcje prawne

Kodeks karny przewiduje sankcje za przestępstwa komputerowe, a organy ścigania współpracują z instytucjami monitorującymi cyberprzestrzeń.

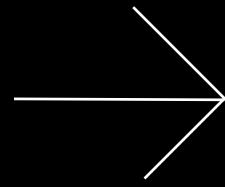
Przestępstwa komputerowe uregulowane w Ustawie z dnia 6 czerwca 1997 r. Kodeks karny.

- **Inne przestępstwa. W tej grupie wyróżnić można przestępstwa „pospolite” popełniane z wykorzystaniem komputerów. Poniższe wyliczenie jest przykładowe i nie obejmuje wszystkich możliwych przestępstw.**

<u>Nie jest to katalog zamknięty:</u>

1. rozpowszechnianie pornografii dziecięcej - art. 202 k.k.,
2. rozmaite formy rasizmu,
3. propagowanie stroju totalitarnego – art. 256 k.k.,
4. groźba karalna – art. 190 k.k.,
5. zniesławienie – art. 212 k.k.,
6. zniewaga – art. 216 k.k.,
7. podżeganie do popełnienia przestępstwa.

Piractwo komputerowe



Definicja i przykłady piractwa komputerowego

Definicja piractwa komputerowego

Piractwo komputerowe to nielegalne kopiowanie i używanie chronionych prawem autorskim produktów cyfrowych.

Przykłady piractwa

Obejmuje instalację od znajomego, cracki, numery seryjne oraz udostępnianie w sieciach p2p bez zgody właściciela.

Ochrona prawna

Ustawa z 1994 roku chroni prawa twórców oprogramowania jako własność intelektualną.

Konsekwencje piractwa

Piractwo prowadzi do strat finansowych i narusza prawa autorskie producentów oprogramowania.

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.

Piractwo komputerowe

Piractwo - to kopiowanie, reprodukowanie, używanie i wytwarzanie bez zezwolenia produktu chronionego przez prawo autorskie. Tzw. **„piractwo komputerowe”**

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

Piractwo komputerowe

Wykonywanie dodatkowych kopii oprogramowania,

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

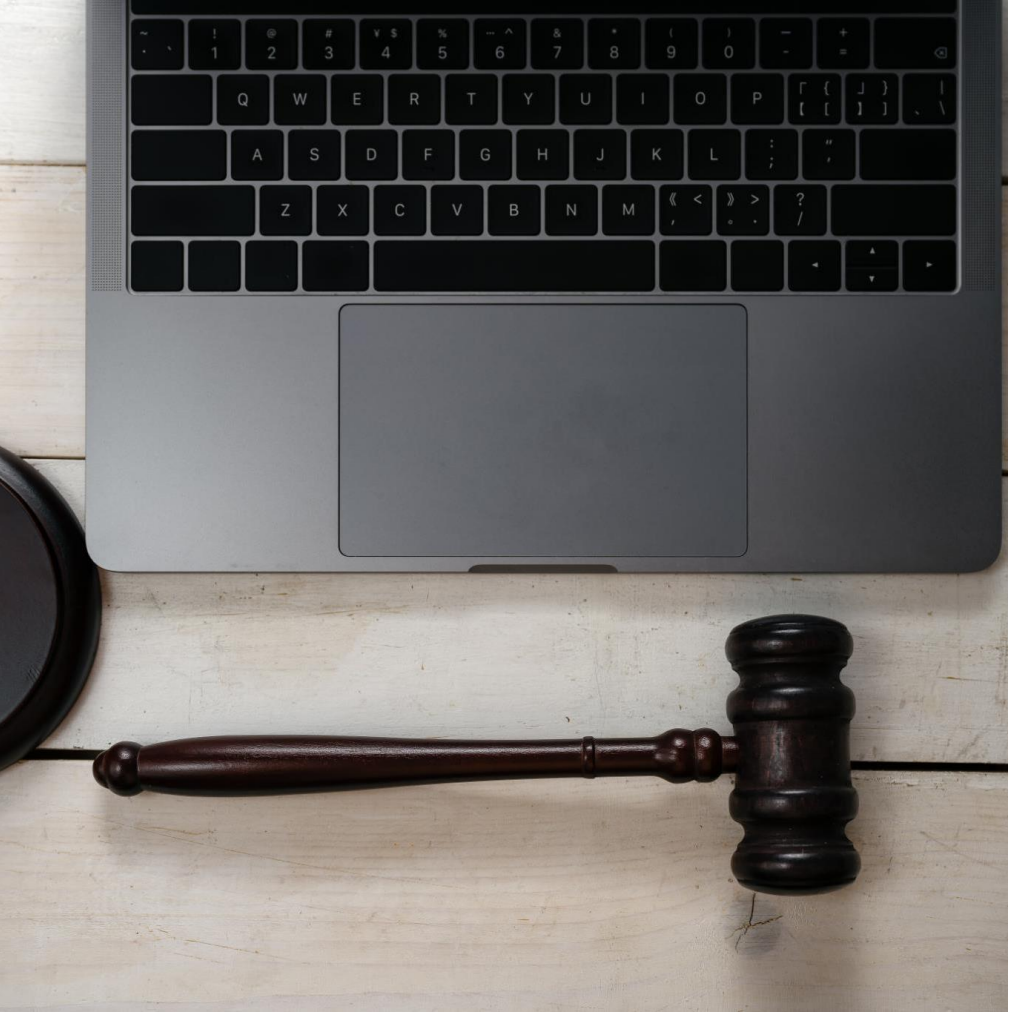
Fałszowanie (używanie cracków i nr seryjnych w celu uzyskania nieograniczonej wersji danego programu),

Umieszczanie na serwerach pełnych wersji

Oprogramowania w celu udostępniania innym – np. sieci p2p,

Wynajem oprogramowania.

Konsekwencje naruszeń prawa autorskiego



Odpowiedzialność cywilna i karna

Odpowiedzialność cywilna

Osoba naruszająca prawa autorskie może być zobowiązana do zapłaty odszkodowania oraz usunięcia skutków naruszenia.

Odpowiedzialność karna

Naruszenia prawa autorskiego mogą skutkować grzywną, ograniczeniem wolności lub więzieniem do 5 lat.

Przykłady naruszeń

Nielegalne kopiowanie oprogramowania i udostępnianie materiałów bez zgody autora to poważne wykroczenia.

Konsekwencje społeczne

Naruszenie prawa autorskiego może prowadzić do utraty reputacji i kosztów sądowych.

Regulacje Unii Europejskiej

Listy przestępstw komputerowych UE

Lista minimalna przestępstw

Lista minimalna obejmuje podstawowe przestępstwa komputerowe wymagające kryminalizacji we wszystkich krajach UE ze względu na ich powagę i charakter transgraniczny.

Lista fakultatywna przestępstw

Lista fakultatywna zawiera przestępstwa, których kryminalizacja pozostaje decyzją poszczególnych państw członkowskich Unii Europejskiej.

Zakres przestępstw minimalnych

Obejmuje oszustwa, fałszerstwa, włamania, niszczenie danych, sabotaż, piractwo i kopiowanie półprzewodników bez zgody.

Zakres przestępstw fakultatywnych

Zawiera modyfikacje danych, szpiegostwo komputerowe, nieautoryzowane użycie komputerów oraz korzystanie z chronionego oprogramowania.

Regulacje Unii Europejskiej

Rada Europy wdrożyła własny program badań nad przestępczością komputerową.

Stworzono dwie listy przestępstw komputerowych:

- minimalną, którą wszystkie kraje powinny adaptować;
- fakultatywną, której uwzględnienie powinno zostać rozważone indywidualnie przez każde z państw

Regulacje Unii Europejskiej

<u>Pierwsza lista obejmuje</u>:

- oszustwo komputerowe,
- fałszerstwo komputerowe,
- włamanie do systemu komputerowego,
- niszczenie danych lub programów,
- sabotaż komputerowy,
- piractwo komputerowe,
- bezprawne kopiowanie półprzewodników.

Regulacje Unii Europejskiej

<u>Drugą listą objęte zostały</u>:

- modyfikacje danych lub programów komputerowych,
- szpiegostwo komputerowe,
- używanie komputera bez zezwolenia,
- używanie prawnie chronionego programu komputerowego bez upoważnienia.

Regulacje Unii Europejskiej

Na liście „**minimalnej**” znalazły się czyny wymagające (według Komisji Ekspertów) kryminalizacji we wszystkich krajach członkowskich - przede wszystkim ze względu na znaczną szkodliwość oraz ponadgraniczny charakter.

Listą **fakultatywną** objęte zostały nadużycia, których kryminalizacja nie wymaga podejmowania skoordynowanych działań międzynarodowych i mogą o niej swobodnie decydować poszczególne państwa.

Zapobieganie i zwalczanie przestępczości komputerowej

Sposoby zapobiegania według FBI

Silne hasła i uwierzytelnianie wieloskładnikowe (Strong passwords and Multi-Factor Authentication)

* Używaj haseł o dużej złożoności (minimum 12 znaków, litery, cyfry, znaki specjalne).
* Włącz MFA (Multi-Factor Authentication – uwierzytelnianie wieloskładnikowe) wszędzie tam, gdzie to możliwe – szczególnie dla kont e-mail, bankowych i administracyjnych.

Kopie zapasowe i ochrona przed ransomware (Backups and Ransomware Protection)

* Twórz regularne kopie zapasowe (regular backups) danych na nośnikach offline lub w chmurze.
* Testuj możliwość odtworzenia backupu (restore backup).
* Stosuj zasadę 3-2-1 rule (zasada 3-2-1): 3 kopie danych, 2 różne nośniki, 1 kopia offline.

Oprogramowanie antywirusowe, EDR i aktualizacje (Antivirus, EDR and Updates)

* Używaj antywirusów (antivirus software) i rozwiązań EDR (Endpoint Detection & Response – wykrywanie i reagowanie na zagrożenia).
* Regularnie aktualizuj systemy operacyjne, aplikacje i firmware (regular updates).
* Włącz automatyczne aktualizacje (automatic updates) w celu minimalizacji ryzyka luk w zabezpieczeniach.

Sposoby zapobiegania według FBI

Bezpieczne korzystanie z Internetu (Safe Internet Practices)

* Nie otwieraj podejrzanych załączników ani linków z nieznanych źródeł (avoid suspicious attachments and links).
* Odłączaj nieużywane urządzenia i porty USB (disconnect unused devices).
* Korzystaj z VPN (Virtual Private Network – wirtualna sieć prywatna) w sieciach publicznych.
* Sprawdzaj adresy URL pod kątem phishingu (check URLs for phishing).

Edukacja i polityki bezpieczeństwa (Education and Security Policies)

* Regularnie szkol użytkowników w zakresie phishingu, socjotechniki i zasad cyberhigieny (phishing, social engineering, cyber hygiene).
* Wdrażaj polityki bezpieczeństwa: zarządzanie hasłami, dostępami, aktualizacjami (implement security policies).
* Monitoruj logi i konfiguruj alerty bezpieczeństwa (monitor logs and configure security alerts).

Dodatkowe zalecenia (Additional Recommendations)

* Włącz kontrolę dostępu opartą na zasadzie najmniejszych uprawnień (least privilege access control).
* Stosuj szyfrowanie danych w spoczynku i w transmisji (data encryption at rest and in transit).
* Rozważ wdrożenie LAPS (Local Administrator Password Solution) lub menedżera haseł (password manager).
* Używaj PowerShell w trybie ograniczonym (PowerShell constrained mode) i monitoruj jego użycie.

Rola CERT Polska

Reagowanie na incydenty

CERT Polska zajmuje się rejestrowaniem i obsługą zgłoszeń dotyczących naruszeń bezpieczeństwa w sieci Internet.

Współpraca z instytucjami

Organizacja współpracuje z krajowymi i międzynarodowymi instytucjami, zwalczając przestępczość komputerową.

Edukacja i wsparcie użytkowników

CERT Polska prowadzi kampanie edukacyjne i wspiera użytkowników w zabezpieczaniu systemów teleinformatycznych.

Zwalczanie przestępstw komputerowych.

C

E

R

T

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.

C

E

R

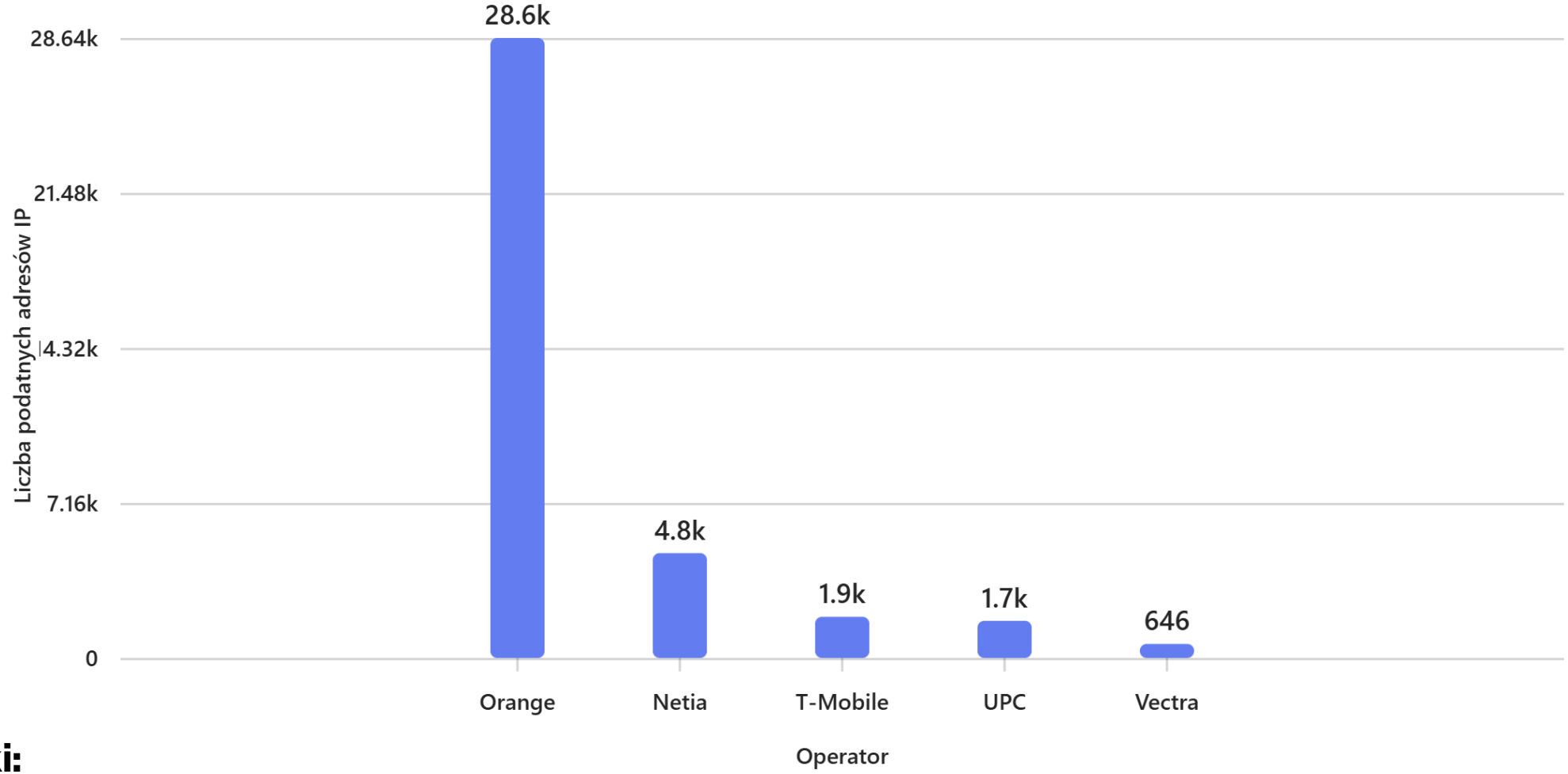
T

Computer Emergency Response Team Polska – jest powołane 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.

Zwalczanie przestępstw komputerowych.

Raport_CP_2024.pdf

Średnią dzienną liczbę podatnych adresów IP wg operatora w 2024 roku:



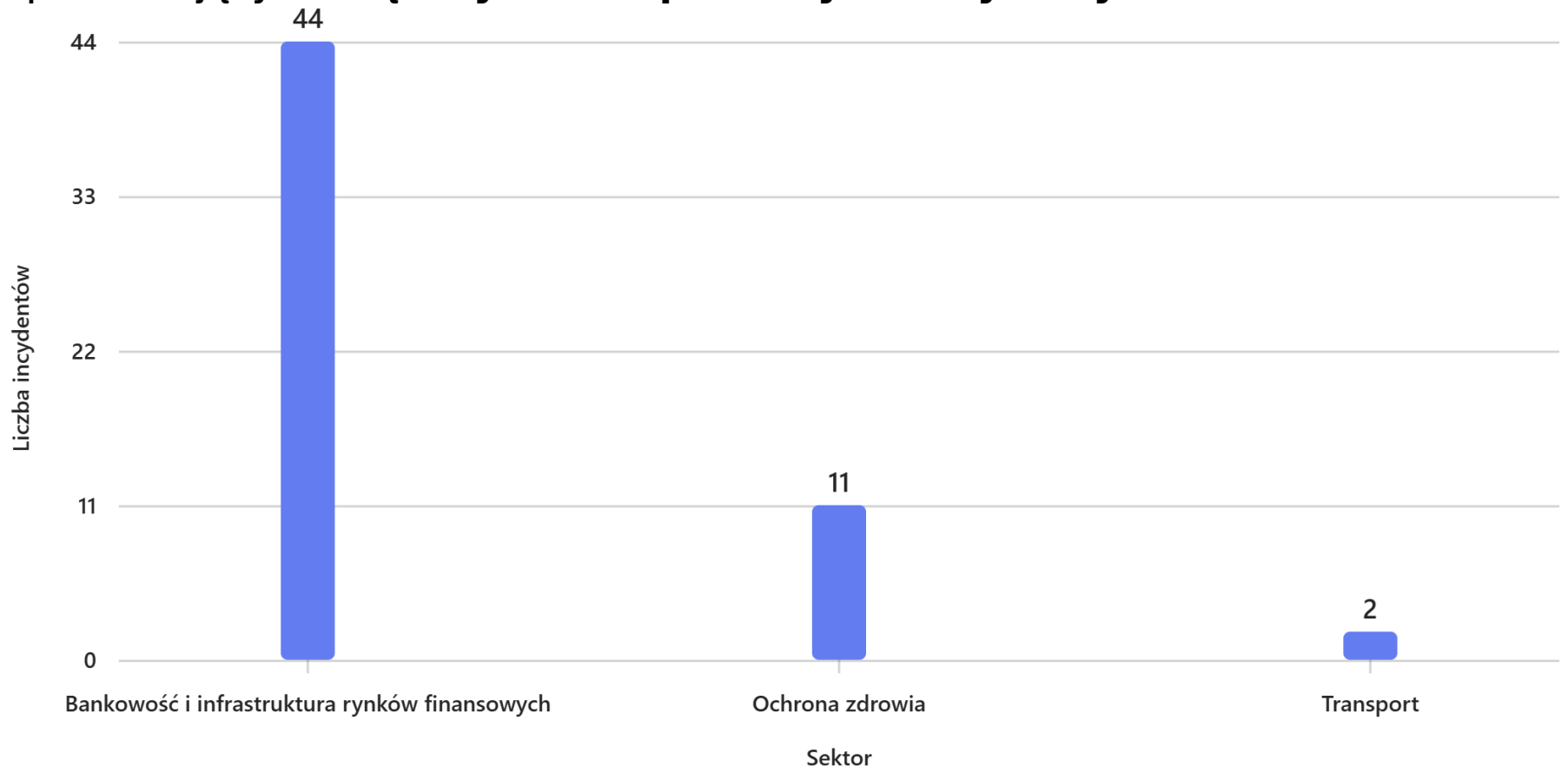
Wnioski:

- **Orange** zdecydowanie dominuje (ponad 28 tys. podatnych adresów IP dziennie).
- **Netia** jest na drugim miejscu (ok. 4,8 tys.).
- **T-Mobile**, **UPC** i **Vectra** mają znacznie niższe wartości, co może świadczyć o lepszej konfiguracji usług lub mniejszej skali infrastruktury.

Zwalczanie przestępstw komputerowych.

Raport_CP_2024.pdf

Wykres porównujący **liczbę incydentów poważnych w wybranych sektorach w Polsce w 2024 roku**:



Wnioski:

•**Bankowość i infrastruktura rynków finansowych** – zdecydowana większość (44 incydenty, czyli 77% wszystkich poważnych).

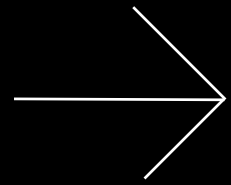
•**Ochrona zdrowia** – 11 incydentów (19%).

•**Transport** – tylko 2 incydenty (4%).

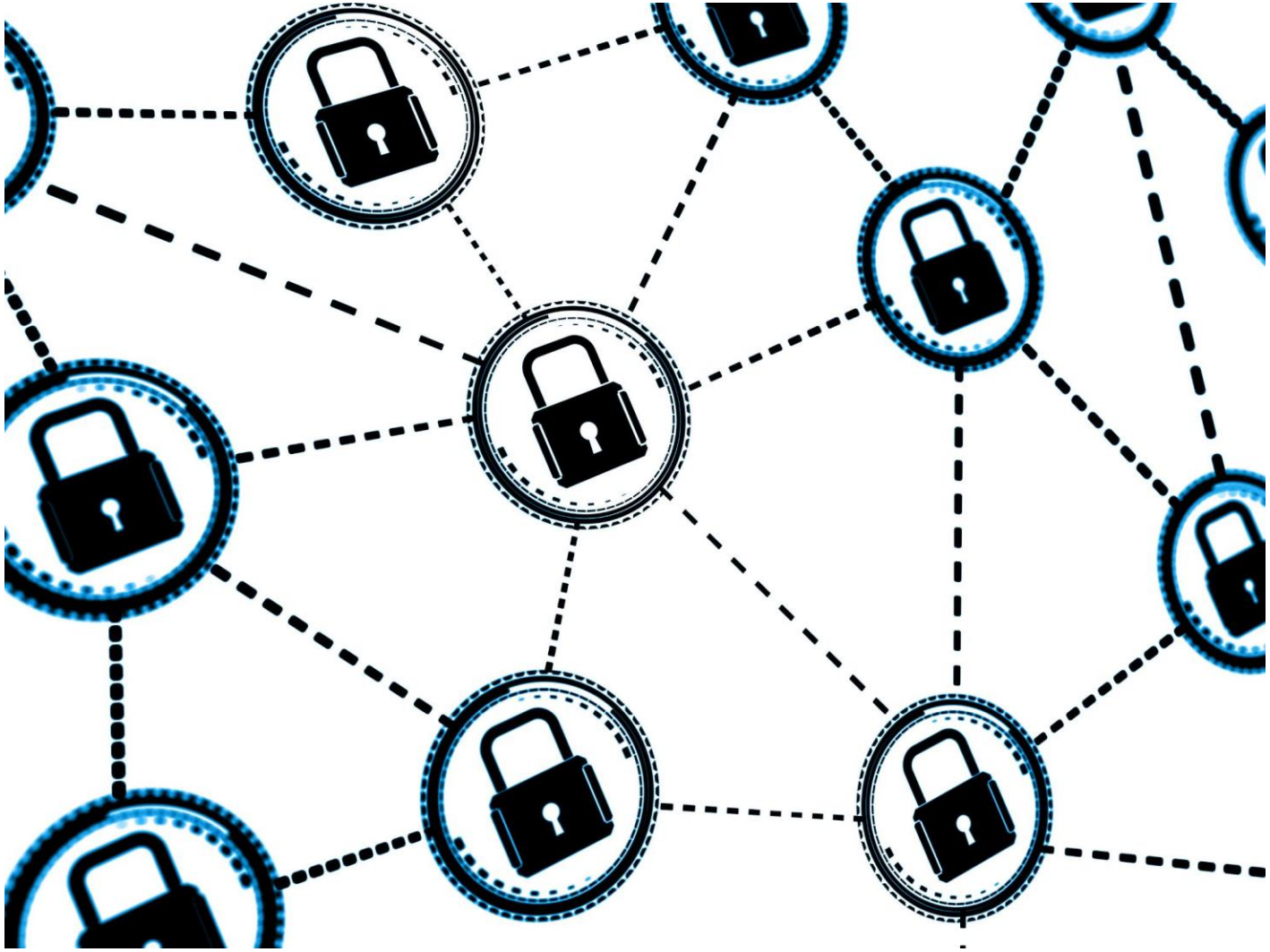
Zadanie

[2.3_cw1_ zwalczanie przestępczości komputerowej.pdf]

Podsumowanie



Pytania sprawdzające



Pytania sprawdzające

1. Co to jest przestępczość komputerowa?
2. Jakie są główne rodzaje przestępstw komputerowych według Kodeksu karnego?
3. Na czym polega fałszerstwo dokumentów elektronicznych?
4. Czym różni się paserstwo umyślne od nieumyślnego?
5. Jakie działania zalicza się do piractwa komputerowego?
6. Jakie przestępstwa znajdują się na liście minimalnej UE?
7. Jakie są zalecenia FBI dotyczące ochrony przed cyberprzestępczością?
8. Jakie zadania realizuje CERT Polska?

Odpowiedzi

1. To wszelkie działania przestępcze związane z elektronicznym przetwarzaniem danych, naruszaniem uprawnień do programów, ingerencją w informacje, ich nośniki, obieg w systemach komputerowych oraz w sprzęt komputerowy.
2. Przestępstwa przeciw ochronie informacji, przeciw wiarygodności dokumentów, przeciwko mieniu, szpiegostwo komputerowe oraz inne przestępstwa z wykorzystaniem komputerów (np. pornografia dziecięca, groźby karalne).
3. Polega na podrobieniu lub przerobieniu dokumentu elektronicznego oraz jego użyciu jako autentycznego, a także na niszczeniu, ukrywaniu lub usuwaniu dokumentu przez osobę nieuprawnioną.
4. Umyślne – sprawca wie, że program został skradziony lub nielegalnie skopiowany; nieumyślne – sprawca powinien przypuszczać, że program pochodzi z przestępstwa.
5. Kopiowanie i rozpowszechnianie oprogramowania bez zgody właściciela, instalacja nielegalnych kopii, używanie cracków i numerów seryjnych, udostępnianie pełnych wersji w sieciach P2P, wynajem oprogramowania bez zgody właściciela.
6. Oszustwo komputerowe, fałszerstwo komputerowe, włamanie do systemu komputerowego, niszczenie danych lub programów, sabotaż komputerowy, piractwo komputerowe, bezprawne kopiowanie półprzewodników.
7. Używanie silnych haseł, regularne tworzenie kopii zapasowych, instalacja antywirusa i zapór sieciowych, odłączanie nieużywanych komputerów od Internetu, nieotwieranie załączników od nieznanych nadawców, regularne aktualizacje oprogramowania.
8. Rejestrowanie i obsługa incydentów naruszających bezpieczeństwo sieci, alarmowanie użytkowników o zagrożeniach, prowadzenie badań i publikowanie raportów, współpraca z instytucjami krajowymi i międzynarodowymi, edukacja i kampanie informacyjne.

Źródła

•**Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny**
Rozdziały: XXXIII (przestępstwa przeciw ochronie informacji), XXXIV, XXXV, XXXVI, XXXVII, XVII.
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf
•**Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych**
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19940240083/U/D19940083Lj.pdf
•**CERT Polska – Raporty i zalecenia**
https://cert.pl
•**FBI Cybersecurity Recommendations**
https://www.fbi.gov/investigate/cyber
•**Dyrektywy UE dotyczące cyberprzestępczości**
https://eur-lex.europa.eu
•Literatura:
•Golat R., *Prawo autorskie i prawa pokrewne*, Wydawnictwo C.H.Beck
•Kozłowski T., *Licencje Wolnego Oprogramowania*