



Temat 6 .

Cyberprzestępcstwo i jego aspekty prawne

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl>

BEZPIECZEŃSTWO
INFORMACJI



- Netykieta
- Cyfrowy ślad
- Cyberprzestępstwo
- Akty prawne

Zadanie

Treść

Prezentacja zadania podczas zajęć.

Około 9 osób podczas zajęć

(0-2 pkt)



Netykieta

Netykieta

nieformalny zbiór zasad uprzejmej i odpowiedzialnej komunikacji w Internecie.
Popularna szczególnie w latach 2000–2015, zwłaszcza w kontekście e-maili i forów

Zasada	Opis
Szanuj innych użytkowników	Nie obrażaj, nie poniżaj, nie stosuj mowy nienawiści – za ekranem siedzi drugi człowiek.
Pisz zwięźle i na temat	Unikaj rozwlekłych, chaotycznych lub nieczytelnych wypowiedzi. Dbaj o poprawność językową.
Nie nadużywaj wielkich liter	W internecie WIELKIE LITERY oznaczają krzyk – używaj ich z umiarem.
Unikaj spamu i łańcuszków	Nie wysyłaj niezamówionych reklam, wiadomości masowych ani nieistotnych treści.
Szanuj prywatność swoją i innych	Nie publikuj danych osobowych, zdjęć czy informacji bez zgody.
Cytuj źródła i nie kopiuj cudzych treści	Plagiat online jest tak samo poważny jak offline – podawaj autorów i linki.
Dostosuj styl wypowiedzi do sytuacji	Inaczej piszemy w mailu do wykładowcy, a inaczej na czacie z kolegami.
Nie trolluj i nie prowokuj	Nie wchodź celowo w spory ani nie wrzucaj kontrowersji „dla zabawy”.
Pomagaj mniej doświadczonym użytkownikom	W społecznościach internetowych bądź życzliwy wobec początkujących.
Pamiętaj, że nic nie ginie w sieci	Twoje wypowiedzi mogą zostać zapisane, udostępnione i zacytowane – myśl przed kliknięciem.

Cyfrowy ślad

Cyfrowy ślad (digital footprint)

wszystkie informacje, jakie użytkownik pozostawia w Internecie podczas korzystania z różnych usług online, zarówno świadomie (np. publikując posty, komentarze, logując się do serwisów), jak i nieświadomie (np. poprzez ciasteczka, metadane, historię przeglądania), które razem tworzą jego unikalny profil cyfrowej aktywności.

Rodzaj danych	Przykład / Opis
Zdjęcia i filmy	Publikacje w mediach społecznościowych, chmurach, galeriach online
Historia lokalizacji (GPS)	Ślady z aplikacji typu Google Maps, Uber, zdjęć z geolokalizacją
Rejestr kliknięć i czasu spędzonego	Dane analityczne gromadzone przez strony (np. Google Analytics)
Komentarze i aktywność społeczna	Lajki, wpisy, udział w grupach, komentarze na YouTube czy TikTok
Dane logowania i adresy IP	Informacje o urządzeniu, czasie i miejscu logowania
Dane zakupowe i transakcyjne	Historia zakupów online, zapisane dane płatnicze, koszyki, listy życzeń
Subskrypcje i newslettery	Zapisy do biuletynów, preferencje marketingowe, zgody na przetwarzanie danych
Wyszukiwania w Internecie	Historia zapytań w wyszukiwarkach, analiza intencji zakupowych i informacyjnych
Dane z aplikacji mobilnych	Informacje zbierane przez aplikacje (np. zdrowotne, pogodowe, transportowe)
Aktywność w chmurze	Zmiany, edycje, współdzielenie plików w usługach takich jak Google Drive, OneDrive
Zgłoszenia do usług online	Rejestracje w serwisach, udział w webinarach, wypełnianie formularzy
Rozpoznawanie twarzy / biometryka	Dane biometryczne zapisane w systemach zabezpieczeń i mediów społecznościowych

Cyfrowy ślad

Jak ograniczyć swój cyfrowy ślad?

Działanie	Opis / Cel
Przeglądanie w trybie incognito	Ogranicza zapisywanie historii przeglądania i ciasteczek
Używanie VPN	Ukrywa adres IP i lokalizację, szyfruje połączenie
Zarządzanie ustawieniami prywatności	Pozwala decydować, jakie dane zbiera dana aplikacja lub strona
Regularne czyszczenie ciasteczek	Usuwa zapisane dane śledzące i preferencje z przeglądarki
Rozważne publikowanie treści	Zmniejsza ryzyko ujawnienia prywatnych informacji i negatywnego echa online
Wylogowywanie się z kont po użyciu	Zmniejsza ryzyko przechwycenia sesji i nieautoryzowanego dostępu
Ograniczanie zgód na pliki cookies	Minimalizuje śledzenie przez zewnętrzne podmioty
Korzystanie z menedżera haseł	Chroni dane logowania i zmniejsza ryzyko używania tych samych haseł
Unikanie publicznych sieci Wi-Fi	Zmniejsza ryzyko przechwycenia danych przez osoby trzecie
Usuwanie nieużywanych kont online	Ogranicza ilość miejsc, gdzie przechowywane są nasze dane
Weryfikacja ustawień prywatności w social media	Zapobiega niepożądanemu udostępnianiu treści i danych osobom trzecim

Cyberprzestępcstwo

Cyberprzestępcstwo

Polskie prawodawstwo do dzisiaj nie stworzyło jednolitej definicji cyberprzestępczości.

Pojęcie przestępczości komputerowej nie jest jednoznacznie zdefiniowane nawet na gruncie Kodeksu karnego. Funkcjonuje natomiast wiele tworzonych doraźnie, w zależności od potrzeb, definicji opierających się na najprostszym założeniu, iż ogólnie są to przestępstwa popełniane za pomocą komputerów oraz Internetu.

Cyberprzestępczość – próba diagnozy zjawiska , Kwartalnik Policyjny

<https://kwartalnik.csp.edu.pl/kp/archiwum-1/2017/nr-42017/3730,Cyberprzestepczosc-proba-diagnozy-zjawiska.html>



**Cyberprzemoc jest często formą
cyberprzestępczości**

Międzynarodowe określenia CyberCrime



Źródło	Określenie cyberprzestępczości	Adres URL
Konwencja Rady Europy o cyberprzestępczości (Konwencja Budapeszteńska)	Konwencja określa cyberprzestępstwa jako działania przestępcze skierowane przeciwko poufności, integralności i dostępności systemów komputerowych, sieci oraz danych, a także nadużycia związane z takimi systemami, sieciami i danymi.	https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE	Dyrektywa określa cyberprzestępczość jako nielegalne działania wymierzone w systemy informatyczne, w tym nieuprawniony dostęp, ingerencję w systemy i dane oraz zakłócanie funkcjonowania systemów.	https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32013L0040
Organizacja Narodów Zjednoczonych (ONZ) UNODC	UNODC określa cyberprzestępczość jako przestępstwa, w których komputer jest narzędziem, celem lub miejscem przestępstwa, obejmujące szeroki zakres działań od oszustw internetowych po ataki na infrastrukturę krytyczną.	https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_2_10213.pdf
Europol	Europol określa cyberprzestępczość jako przestępstwa, które są popełniane przy użyciu technologii informatycznych lub są wymierzone w takie technologie, w tym ataki hakerskie, dystrybucję złośliwego oprogramowania i przestępstwa związane z ciemną stroną internetu (Darknet).	https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime
Interpol	Interpol określa cyberprzestępczość jako przestępstwa obejmujące ataki na systemy komputerowe, oszustwa internetowe, kradzież tożsamości oraz inne nielegalne działania prowadzone w cyberprzestrzeni.	https://www.interpol.int/Crimes/Cybercrime

Międzynarodowe określenia CyberCrime

Wspólne cechy

Nielegalne działanie

- wszystkie definicje wskazują na przestępcze wykorzystanie technologii.

Działania przeciwko poufności, integralności i dostępności

- te kluczowe aspekty cyberbezpieczeństwa.

Nieuprawniony dostęp do systemów i danych

- uzyskiwanie dostępu do systemów informatycznych bez zgody.

Ingerencja w systemy i dane

- manipulacja lub uszkodzenie danych i funkcji systemów.

Oszustwo informatyczne

- działania mające na celu wprowadzenie w błąd lub wyłudzenie korzyści majątkowych.

Atak na infrastrukturę krytyczną

- działania celujące w kluczowe dla funkcjonowania państwa lub organizacji systemy.

Działanie związane z „ciemną stroną” Internetu

- wykorzystanie anonimowości Internetu do prowadzenia nielegalnych aktywności.

Próba definicji

Cyberprzestępczość to każde działanie przestępcze wykonane z wykorzystaniem technologii informatycznych, które jest skierowane przeciwko poufności, integralności i dostępności systemów komputerowych, sieci lub danych.

Obejmuje szeroki zakres działań, w tym nieuprawniony dostęp, manipulacje systemami i danymi, zakłócanie funkcjonowania systemów, ataki na infrastrukturę krytyczną, dystrybucję złośliwego oprogramowania oraz działania związane z ciemną stroną internetu (Darknet).

Cyberprzestępczość rozumiana jest jako globalne zjawisko, gdzie komputer może być narzędziem, celem lub miejscem przestępstwa.

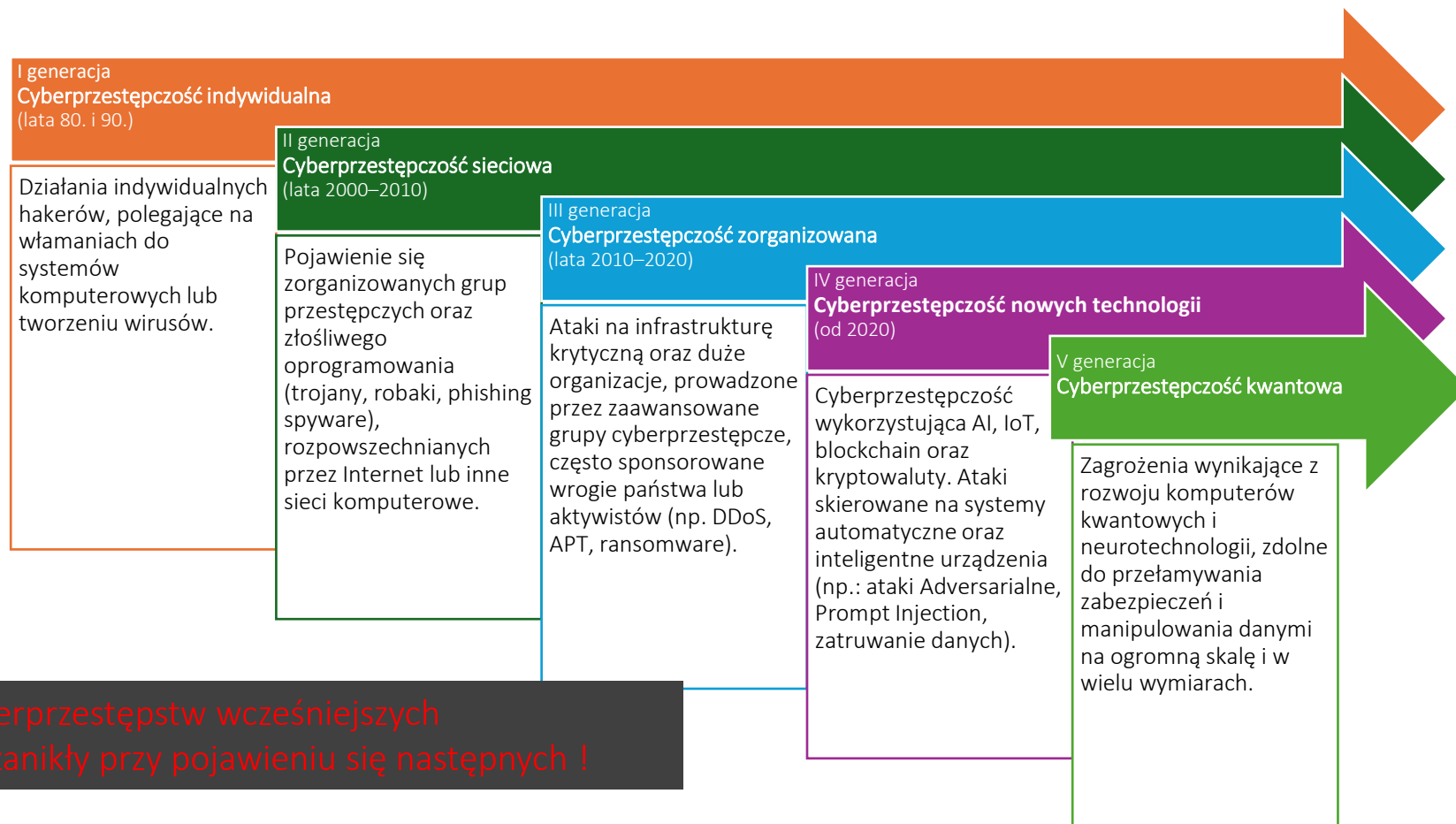
Dodatkowo, obejmuje wykorzystanie sztucznej inteligencji do tworzenia i propagowania oszustw, manipulowanie algorytmami, oraz inne działania mające na celu wykorzystanie lub zakłócenie systemów AI w sposób niezgodny z prawem.

Wersja skrócona



Cyberprzestępczość – działania przestępcze realizowane z użyciem systemów informatycznych, które naruszają poufność, integralność lub dostępność danych i systemów komputerowych, obejmujące nieuprawniony dostęp, manipulacje danymi, zakłócenia funkcjonalności systemów, ataki na infrastrukturę krytyczną, dystrybucję złośliwego oprogramowania, jak również oszustwa, manipulację algorytmami oraz szkodliwe wykorzystanie sztucznej inteligencji.

Formy popełniania cyberprzestępstw



Kto pierwszy?



Obrońca



Atakujący

To jak sobie poradzić ?



Kodeks Karny

W *Kodeksie Karnym* są zawarte przestępstwa które można utożsamiać z pojęciem cyberprzestępczości, między innymi:

Przestępstwa ściśle komputerowe

Działania bezpośrednio skierowane na systemy komputerowe, zgodne z przepisami rozdziału XXXIII Kodeksu Karnego.

Przestępstwa związane z treściami

Rozpowszechnianie nielegalnych treści, takich jak pornografia dziecięca (art. 202 KK) oraz propagowanie nienawiści (art. 256 KK).

Przestępstwa związane ze spowodowaniem zagrożenia powszechnego

Zakłócanie funkcjonowania systemów teleinformatycznych (art. 165 KK).

Przestępstwa związane z nękaniem (cyberstalkingiem) i kradzieżą tożsamości

Uporczywe nękanie innych osób lub kradzież tożsamości (art. 190a KK).



Dz.U.2024.0.17 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553>

Rozdział XXXIII KK

Przestępstwa przeciwko ochronie informacji



Ujawnienie i wykorzystanie informacji niejawnych

- **Art. 265 KK:** Ujawnienie lub wykorzystanie informacji niejawnych, zwłaszcza „tajnych” lub „ściśle tajnych”.
- **Art. 266 KK:** Ujawnienie informacji uzyskanej w związku z pełnioną funkcją, pracą lub działalnością publiczną, społeczną czy naukową.

Artykuły te dotyczą naruszeń związanych z informacjami niejawnymi, szczególnie tych, które mogą stanowić zagrożenie dla bezpieczeństwa państwa lub interesów instytucji publicznych.

Pracownik instytucji państwowej udostępnia tajne informacje dotyczące bezpieczeństwa narodowego zewnętrznym podmiotom.

Funkcjonariusz publiczny przekazuje dane zastrzeżone dotyczące negocjacji handlowych firmie konkurencyjnej.

Rozdział XXXIII KK

Przestępstwa przeciwko ochronie informacji



Bezprawne uzyskiwanie dostępu do informacji

- **Art. 267 KK:** Bezprawne uzyskanie dostępu do informacji poprzez przełamanie zabezpieczeń, podsłuchy, podłączenie do sieci telekomunikacyjnej.
- **Art. 269b KK:** Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie narzędzi przeznaczonych do popełniania przestępstw informatycznych.

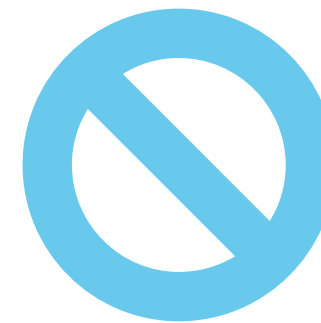
Artykuły te obejmują działania związane z uzyskaniem nieuprawnionego dostępu do informacji, jak również udostępnianie narzędzi umożliwiających popełnianie cyberprzestępstw.

Atak hakerski na system bankowy w celu pozyskania danych klientów, które następnie są wykorzystane w oszustwach finansowych.

Osoba udostępnia programy do łamania haseł na forach internetowych, które są wykorzystywane przez cyberprzestępców do włamań do systemów.

Rozdział XXXIII KK

Przestępstwa przeciwko ochronie informacji



Niszczenie, uszkodzanie i zmienianie danych informatycznych

- **Art. 268 KK:** Utrudnianie dostępu do informacji poprzez niszczenie, uszkodzanie lub zmienianie jej zapisu.
- **Art. 268a KK:** Niszczenie, usuwanie lub zmienianie danych informatycznych, co powoduje zakłócenia w systemach przetwarzania danych.
- **Art. 269 KK:** Niszczenie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju lub funkcjonowania administracji publicznej.

Artykuły te koncentrują się na przestępstwach związanych z niszczeniem lub modyfikowaniem danych informatycznych, które mogą zakłócać funkcjonowanie ważnych systemów.

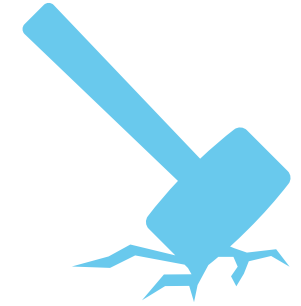
Haker usuwa kluczowe pliki z serwera przedsiębiorstwa, uniemożliwiając ich odtworzenie i powodując chaos operacyjny.

Cyberprzestępcy przeprowadzają atak ransomware, blokując dostęp do danych firmowych i żądając okupu za ich odblokowanie.

Cyberatak na infrastrukturę energetyczną kraju, prowadzący do zakłócenia dostaw prądu na dużym obszarze.

Rozdział XXXIII KK

Przestępstwa przeciwko ochronie informacji



Zakłócanie pracy systemów teleinformatycznych

- **Art. 269a KK:** Zakłócanie pracy systemów informatycznych lub teleinformatycznych poprzez usunięcie, zniszczenie, uszkodzenie danych lub utrudnienie dostępu do nich..

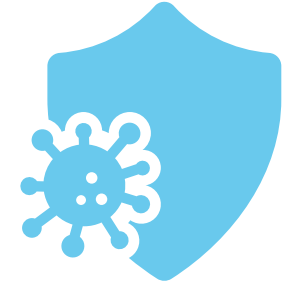
Ten artykuł dotyczy przestępstw związanych z celowym zakłócaniem pracy systemów teleinformatycznych, co może prowadzić do znacznych zakłóceń w dostępie do usług lub danych.

Atak DDoS na serwery banków, który blokuje dostęp klientów do ich kont i powoduje utratę reputacji banku.

Atak hakerski na dostawcę internetu powoduje przerwę w dostępie do sieci, uniemożliwiając korzystanie z bankowości online i pracy zdalnej.

Rozdział XXXIII KK

Przestępstwa przeciwko ochronie informacji



Działania w celu wykrycia błędów w systemach informatycznych

- **Art. 269c KK:** Wyjątek dla osób, które uzyskują dostęp do systemów w celu wykrycia luk w zabezpieczeniach i niezwłocznie informują o nich dysponenta systemu.

Ten artykuł stanowi wyjątek od odpowiedzialności karnej dla osób działających w dobrej wierze, w celu poprawy zabezpieczeń systemów informatycznych.

Badacz bezpieczeństwa odkrywa lukę w zabezpieczeniach systemu bankowego i informuje o tym bank, zamiast wykorzystać ją do popełnienia przestępstwa.

Programista odkrywa lukę w Serwisie WWW Jednostki Wojskowej i niezwłocznie informuje o niej odpowiednie służby, zamiast wykorzystać ją do modyfikacji strony

Przepisy dziedzinowe

Przepisy i regulacje dziedzinowe zawierają w sobie aspekty związane z działaniami utożsamianymi z cyberprzestępczością:

Prawa autorskie:

Chroni przed piractwem internetowym, nielegalnym udostępnianiem materiałów i oprogramowania.

Ochrona danych osobowych:

Zapewnia ochronę przed wyciekami danych, nielegalnym przetwarzaniem i phishingiem.

Usługi elektroniczne:

Reguluje zabezpieczenia transakcji e-commerce i ochronę danych użytkowników.

Płatności elektroniczne:

Przeciwdziała oszustwom w płatnościach online i zapewnia ochronę środków finansowych.

Prawo telekomunikacyjne:

Chroni sieci przed atakami i zapewnia poufność komunikacji.



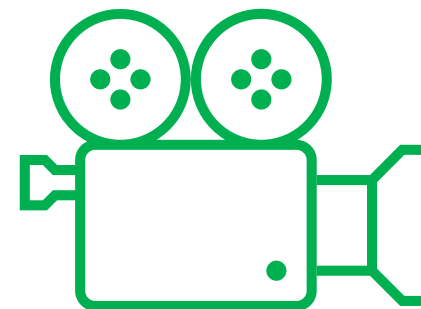
Prawa autorskie

Nieautoryzowane streamowanie filmów na platformie internetowej bez odpowiedniej licencji.

Instalacja oprogramowania biurowego na wielu komputerach przy posiadaniu licencji tylko na jedno urządzenie.

Ustawa z dnia 4 lutego 1994 r.
o prawie autorskim i prawach pokrewnych (art. 115-123)

- Naruszenie praw autorskich w usługach streamingowych: nieautoryzowane emitowanie treści chronionych przez prawo autorskie.
- Piractwo internetowe: udostępnianie i pobieranie treści chronionych prawem autorskim z sieci bez odpowiedniej licencji.
- Nielegalne rozpowszechnianie oprogramowania: dystrybucja kopii programów komputerowych bez zgody posiadacza praw autorskich.
- Reverse engineering: dekompilacja oprogramowania w celach niezgodnych z licencją.



Dz.U. 1994 nr 24 poz. 83

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19940240083>

Ochrona danych osobowych

Utworzenie i wykorzystanie fałszywych stron internetowych do phishingu, mających na celu wyłudzenie danych osobowych.

Niezabezpieczenie danych klientów przez firmę, co prowadzi do wycieku danych osobowych, takich jak adresy e-mail i numery telefonów.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 101-108)

- Wyciek danych osobowych: niezabezpieczenie danych klientów przed cyberatakami skutkujące ich ujawnieniem.
- Naruszenie zasad RODO: brak zgody na przetwarzanie danych lub nieprzestrzeganie praw osób, których dane dotyczą.
- Ataki phishingowe na dane osobowe: wyłudzenie informacji osobistych, takich jak numery PESEL przez fałszywe strony internetowe.
- Nielegalne profilowanie: wykorzystywanie danych osobowych do tworzenia profili użytkowników bez ich wiedzy i zgody.



Dz.U. 2018 poz. 1000

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000>

Usługi elektroniczne

Włamanie do platformy e-commerce i kradzież danych kart kredytowych użytkowników.

Wysyłanie niezamówionej korespondencji reklamowej do użytkowników bez ich zgody.

Ustawa z dnia 18 lipca 2002 r.
o świadczeniu usług drogą elektroniczną (art. 23-25)

- Niezabezpieczona transakcja e-commerce: brak odpowiednich środków ochrony danych w procesie sprzedaży online.
- Nieprzestrzeganie zasad informacyjnych: brak jasnych informacji o przetwarzaniu danych klientów w serwisach e-commerce.
- Ataki na systemy e-commerce: włamania do platform sprzedażowych i kradzież danych kart kredytowych użytkowników.
- Spam i niechciane komunikaty: wysyłanie niezamówionej korespondencji w celach marketingowych bez zgody odbiorcy.



Dz.U. 2002 nr 144 poz. 1204

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20021441204>

Płatności elektroniczne

Wykorzystanie podrobionych danych identyfikacyjnych w procesie autentykacji płatności online.

Oszustwo finansowe polegające na manipulowaniu transakcjami elektronicznymi w celu nieautoryzowanego przekierowania środków z konta klienta.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (art. 150-153d)

- Przeciwdziałanie oszustwom: obowiązek monitorowania transakcji w celu zapobiegania nadużyciom finansowym.
- Autentykacja płatności: mechanizmy weryfikacji tożsamości klienta przy transakcjach elektronicznych.
- Ochrona środków finansowych: regulacje dotyczące ochrony środków na rachunkach klientów w przypadku naruszenia bezpieczeństwa.
- Zgłaszanie incydentów: procedury raportowania podejrzanych działań do właściwych organów nadzorczych.



Dz.U. 2011 nr 199 poz. 1175

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111991175>

Prawo telekomunikacyjne

Podłuchiwanie rozmów telefonicznych bez zgody użytkowników i odpowiednich organów.

Przeprowadzenie ataku DDoS na serwery telekomunikacyjne, co prowadzi do zakłóceń w dostępie do sieci oraz usług komunikacyjnych.

Ustawa z dnia 16 lipca 2004 r.

Prawo telekomunikacyjne (art. 208-210)

- Bezpieczeństwo sieci telekomunikacyjnych: ochrona przed nieautoryzowanym dostępem i atakami typu DDoS na infrastrukturę krytyczną.
- Tajność komunikowania: zasady ochrony przekazywanych informacji, obowiązek zachowania poufności przez operatorów.
- Zarządzanie incydentami: procedury reagowania na naruszenia bezpieczeństwa i wycieki danych w sektorze telekomunikacyjnym.
- Wymogi dot. sprzętu i oprogramowania: przepisy regulujące bezpieczeństwo urządzeń i oprogramowania wykorzystywanych do transmisji danych.



Dz.U. 2004 nr 171 poz. 1800

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800>

Centralna organizacja

Zapewnia merytoryczne ramy funkcjonowania organów odpowiedzialnych za Cyberbezpieczeństwo na szczeblu krajowym i w kontekście międzynarodowym. W tym w szczególności w zakresie:

Tworzenia strategii ochrony cyberbezpieczeństwa:

Opracowują narodowe strategie, które określają zasady i cele w zakresie ochrony przed cyberzagrożeniami.

Wdrażania przepisów i regulacji dotyczących cyberprzestępczości:

Zapewniają, że wszelkie działania są zgodne z krajowymi i międzynarodowymi regulacjami prawnymi.

Współpracy międzynarodowa w zakresie zwalczania cyberzagrożeń:

Uczestniczą w wymianie informacji i wspólnych działaniach z organizacjami międzynarodowymi.

Nadzoru nad zgodnością działań z przepisami prawa:

Sprawdzają, czy organizacje i instytucje przestrzegają obowiązujących przepisów w zakresie cyberbezpieczeństwa.



Krajowy system cyberbezpieczeństwa

Ustawa z dnia 5 lipca 2018 r.
o krajowym systemie cyberbezpieczeństwa (art. 73-76)

- Określa podstawowe zasady funkcjonowania Krajowego Systemu Cyberbezpieczeństwa (KSC).
- Określa podmioty odpowiedzialne za cyberbezpieczeństwo, ich obowiązki oraz uprawnienia.
- Definiuje usługi kluczowe oraz infrastrukturę krytyczną, które podlegają szczególnej ochronie przed cyberatakami.



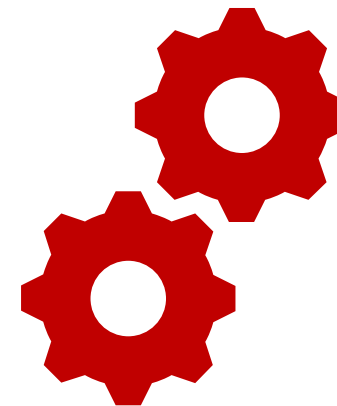
Dz.U. 2018 poz. 1560

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560>

Strategia cyberbezpieczeństwa RP

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r.
w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

- Wyznacza główne cele i kierunki rozwoju narodowego cyberbezpieczeństwa.
- Wzmacnianie odporność państwa na cyberataki.
- Rozwija kompetencje i współpracę międzynarodową.
- Implementacja strategii poprzez konkretne inicjatywy, projekty i regulacje.



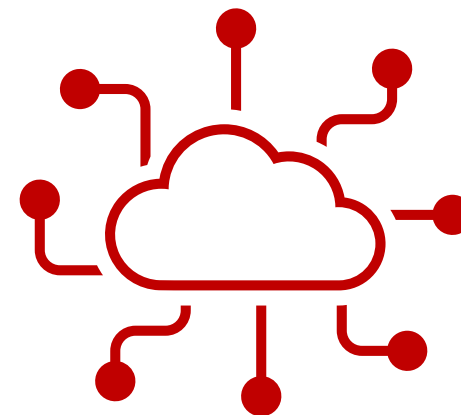
M.P. 2019 poz. 1037

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037>

Narodowe standardy cyberbezpieczeństwa

Zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych

- Wyznaczanie kierunków dla polityki bezpieczeństwa informacji w sektorze prywatnym i publicznym.
- Znaczenie standardów dla ochrony infrastruktury krytycznej i podniesienia poziomu świadomości cybernetycznej w organizacjach.
- Zalecenia i najlepsze praktyki dotyczące zarządzania ryzykiem cybernetycznym.



Narodowe Standardy Cyberbezpieczeństwa

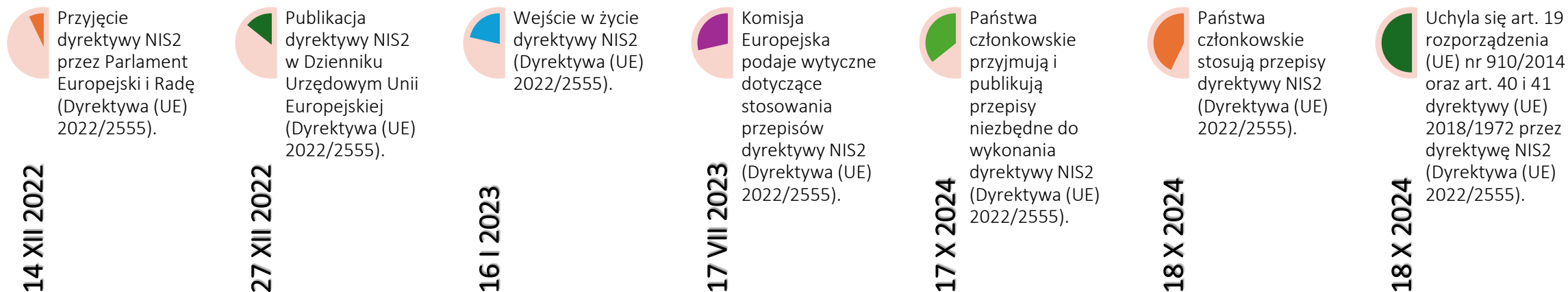
<https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber>

Dyrektywa NIS2

NIS 2 (Network and Information Security Directive 2) to zaktualizowana dyrektywa UE dotycząca poprawy cyberbezpieczeństwa w sektorach krytycznych, takich jak energetyka, transport, finanse i infrastruktura cyfrowa.

NIS 2 wprowadza surowsze wymogi dotyczące zgłaszania incydentów, rozszerza zakres podmiotów objętych regulacjami i wzmacnia współpracę między państwami członkowskimi w zakresie ochrony przed cyberzagrożeniami. Jej celem jest zwiększenie odporności na cyberataki w całej UE.

Oś czasu wdrożenia Dyrektywy NIS2



Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022

<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555>

Porównanie sektorów objętych NIS i NIS2



NIS + NIS2	NIS2
 Energetyka	 Żywność
 Zdrowie	 Przemysł produkcyjny
 Transport	 Poczta i kurierzy
 Bankowość	 Dostawcy publicznych sieci łączności elektronicznej
 Infrastruktura rynków finansowych	 Zarządzanie usługami ICT (między przedsiębiorstwami)
 Infrastruktura cyfrowa	 Oczyszczalnie ścieków
 Dostawcy usług cyfrowych	 Gospodarka odpadami
 Woda pitna	 Administracja publiczna
	 Przestrzeń kosmiczna
	 Badania i rozwój
	 Chemikalia

Rozporządzenie AI Acta

AI Act (Artificial Intelligence Act) to rozporządzenie Unii Europejskiej mające na celu uregulowanie stosowania sztucznej inteligencji.

Jego głównym celem jest zapewnienie, że systemy AI są bezpieczne, przejrzyste i zgodne z wartościami UE. Rozporządzenie wprowadza klasyfikację systemów AI według poziomu ryzyka oraz nakłada surowe wymogi na te o wysokim ryzyku, takie jak systemy wykorzystywane w zdrowiu czy sądownictwie. AI Act ma wspierać innowacje, jednocześnie chroniąc prawa obywateli.

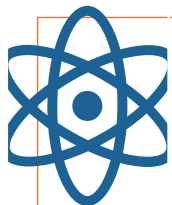
Oś czasu wdrożenia Dyrektywy AI Act



Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r.

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/pol>

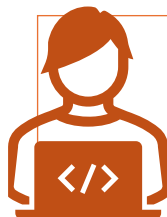
Kierunki rozwoju prawa



Komputery
kwantowe



Fake news



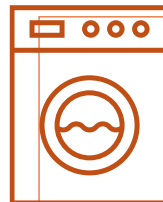
Wojny
algorytmów



Sztuczna
inteligencja



Bezpieczeństwo
dzieci online



Internet Rzeczy
(IoT)

Cyberobrona



Gdzie zgłaszać cyberprzestępstwa

Zagrożenie cyberbezpieczeństwa	Odpowiadające akty prawne	Gdzie zgłosić
Phishing	Kodeks Karny - Art. 269b KK	Policja, CSIRT
Ataki ransomware	Kodeks Karny - Art. 269b KK, Ustawa o usługach płatniczych	Policja, ABW, KNF
Malware	Kodeks Karny - Art. 269b KK	Policja, CSIRT
Ataki DDoS	Kodeks Karny - Art. 269a KK	Policja, CSIRT
Wycieki danych	Ustawa o ochronie danych osobowych	UODO, Policja, GIODO
Insider Threats	Ustawa o ochronie danych osobowych	UODO, Policja
Exploity zeroday	Ustawa o krajowym systemie cyberbezpieczeństwa	Policja, CSIRT
Ataki Man-in-the-Middle (MITM)	Kodeks Karny - Art. 269b KK	Policja, CSIRT
SQL Injection	Kodeks Karny - Art. 269b KK	Policja
Cross-Site Scripting (XSS)	Kodeks Karny - Art. 269b KK	Policja
Ataki na infrastrukturę krytyczną	Rozporządzenie Rady Ministrów w sprawie usług kluczowych	CSIRT, ABW
Spoofing	Kodeks Karny - Art. 269b KK	Policja
Inżynieria społeczna	Kodeks Karny - Art. 269b KK	Policja
Cryptojacking	Kodeks Karny - Art. 269b KK	Policja, CSIRT
Bezpieczeństwo Internetu Rzeczy (IoT)	Ustawa Prawo telekomunikacyjne	UKE, Policja, CSIRT
Ataki sieciowe	Kodeks Karny - Art. 269a KK	Policja, ABW, NASK, CSIRT
Kradzież konta lub przedmiotu w grze online	Kodeks Karny - Art. 268 KK, Ustawa o świadczeniu usług drogą elektroniczną	Policja

Cyberobrona

CSIRT (Computer Security Incident Response Team) **Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego**

to grupa ekspertów zajmujących się zarządzaniem i reagowaniem na incydynty związane z bezpieczeństwem informacji w organizacji.

Głównym celem CSIRT jest minimalizacja skutków incydentów bezpieczeństwa, przywrócenie normalnej operacyjności systemów oraz zapobieganie przyszłym zagrożeniom.

CSIRT GOV

Zespół prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego (ABW).

Administracja Publiczna

Infrastruktura Krytyczna

CSIRT NASK

Zespół działający w ramach NASK

Sektor Prywatny i Przedsiębiorstwa

Analizy i Badania

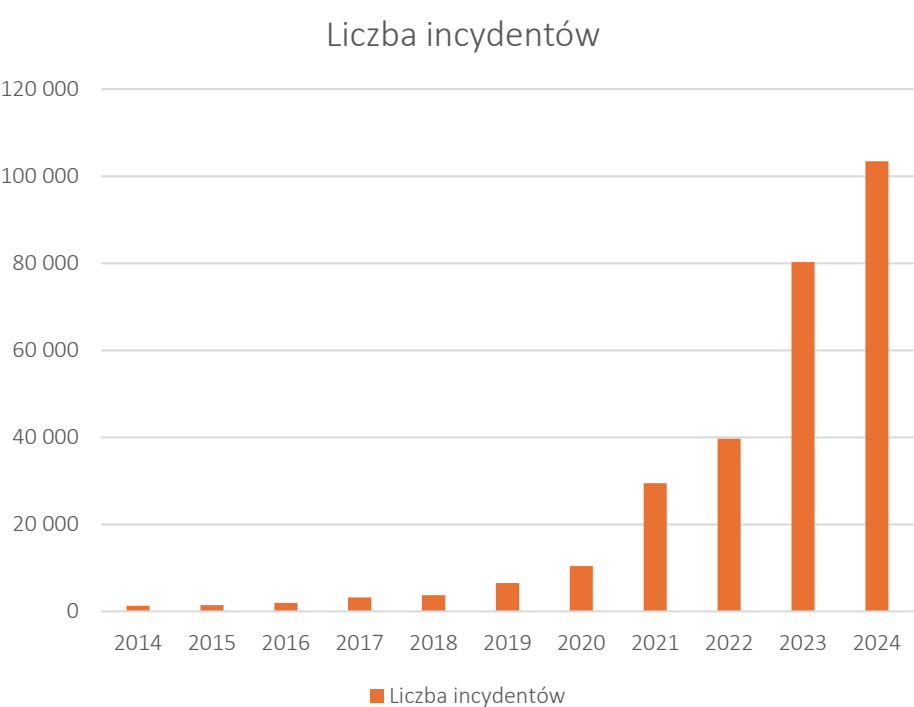
CSIRT MON

Zespół w ramach Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni

Siły Zbrojne RP

Organizacje pracujące na rzecz obronności

Incydenty bezpieczeństwa



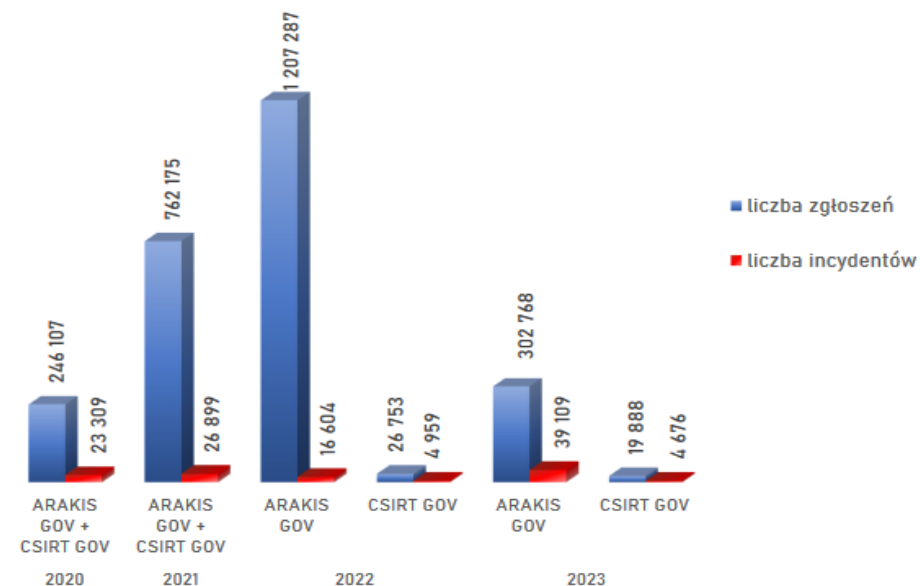
Raport roczny z działalności CERT POLSKA (CSIRT NASK)

https://cert.pl/uploads/docs/Raport_CP_2024.pdf

Liczba incydentów: **103 449** (2024)

~1 incydent na 282 użytkowników w roku

Liczba incydentów bezpieczeństwa



Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 (CSIRT GOV)

<https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf>

Liczba incydentów: **43 785** (2023)

Incydenty bezpieczeństwa

Rodzaje incydentów obsługiwanych przez CERT Polska w 2024 r.

Rodzaj	Liczba incydentów	Procent
Oszustwa komputerowe	97 995	94,70%
Szkodliwe oprogramowanie	1 891	1,80%
Podatne usługi	1 634	1,60%
Obrażliwe i nielegalne treści	775	0,70%
Włamania	447	0,40%
Dostępność zasobów	426	0,40%
Próby włamań	179	0,20%
Atak na bezpieczeństwo informacji	62	0,10%
Gromadzenie informacji	26	0,00%
Inne	14	0,00%

Raport roczny z działalności CERT POLSKA (CSIRT NASK)

https://cert.pl/uploads/docs/Raport_CP_2024.pdf

Incydenty obsługiwane przez CERT Polska w 2024 r.
w podziale na sektor gospodarki

Sektor	Liczba incydentów	Procent
Infrastruktura rynków finansowych	44 020	42,60%
Handel hurtowy i detaliczny	18 324	17,70%
Media	13 322	12,90%
Poczta i usługi kurierskie	5 216	5,00%
Energetyka	4 632	4,50%
Infrastruktura cyfrowa	4 055	3,90%
Osoby fizyczne	2 735	2,60%
Bankowość	2 544	2,50%
Administracja publiczna	2 337	2,30%
Hotele, restauracje, catering	1 108	1,10%
Produkcja	956	0,90%
Inne	837	0,80%
Usługi inne	737	0,70%
Oświata i wychowanie	733	0,70%
Ochrona zdrowia	604	0,60%
Transport	565	0,50%
Kultura i ochrona dziedzictwa narodowego	292	0,30%
Logistyka i dystrybucja	184	0,20%
Budownictwo i gospodarka nieruchomościami	68	0,10%
Wodociągi	59	0,10%
Rolnictwo	32	0,00%
Gospodarka odpadami	27	0,00%
Turystyka	19	0,00%
Izby gospodarcze i handlowe	15	0,00%
Działalność ubezpieczeniowa	14	0,00%
Kultura fizyczna	8	0,00%
Wyznania religijne i mniejszości narodowe	5	0,00%
Rybołówstwo	1	0,00%



<https://youtu.be/XPMAzcbfDOM?si=hwuC7VOWVNdQmZxK>

Zadanie

(0-2 pkt)

Treść

Zapoznaj się z poniższymi przykładami sytuacji codziennych dotyczących naruszeń cyberbezpieczeństwa. Dla każdego przypadku:

- Wskaż, który artykuł Kodeksu karnego może zostać naruszony.
- Uzasadnij swój wybór, odwołując się do treści przepisu.

Sytuacja

- 1 Student używa skryptu do włamania się do systemu ocen w systemie uczelnianym.
- 2 Osoba wysyła wielokrotnie natrętne wiadomości e-mail do byłej partnerki z różnych adresów.
- 3 Firma hostingowa traci dane klientów wskutek ataku ransomware – serwery nie miały kopii zapasowych ani zabezpieczeń.
- 4 Użytkownik zamieszcza na forum internetowym wezwania do nienawiści wobec danej narodowości.
- 5 Nieletni udostępnia w grupie znajomych zdjęcia pornograficzne innej osoby bez jej zgody.
- 6 Pracownik podszywa się pod kolegę z pracy, wysyłając fałszywe wiadomości w jego imieniu.

Termin przesłania sprawozdania,
wskazany w zadaniu w Moodle.

Blokowanie ludzi 30 lat temu:

