# CYBERBEZPIECZEŃSTWO

– podstawowe informacje dla osób korzystających z usług podmiotu kluczowego lub podmiotu ważnego w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

# Spis treści

**Czym jest cyberbezpieczeństwo ?** ..... 3

**Rodzaje zagrożeń cyberbezpieczeństwa** ..... 4

**Czym jest CSIRT ?** ..... 7

**Czym jest incydent ?** ..... 9

**Zgłaszanie incydentu cyberbezpieczeństwa** ..... 10

**W jaki sposób powiadomić Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu ochrony danych ?** ..... 12

**Jak bezpiecznie korzystać z internetu i nie stać się ofiarą cyberprzestępcy ?** ..... 13

**Rozszerz swoją wiedzę – dodatkowe źródła informacji o zagrożeniach bezpieczeństwa użytkowników sieci internetowej** ..... 15

## Czym jest cyberbezpieczeństwo ?

Cyberbezpieczeństwo (ang. *cybersecurity*) stanowi zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Z pojęciem cyberbezpieczeństwa związana jest między innymi ochrona przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych. Cyberprzestrzeń rozumiana jest natomiast jako przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[1].

Cyberbezpieczeństwo odnosi się do szerokiego zakresu różnych działań przestępczych, w których jako podstawowe narzędzie lub jako główny cel wykorzystywane są komputery i systemy informacyjne. Może ona obejmować przestępstwa tradycyjne takie jak oszustwo, fałszerstwo, czy też kradzież, bądź może dotyczyć również przestępstw powiązanych z zakazaną prawem treścią jak nawoływanie do nienawiści. Najczęstsze jednak skojarzeniee z incydentami mającymi miejsce w świecie wirtualnym stanowią przestępstwa charakterystyczne wyłącznie dla komputerów i systemów informacyjnych jak ataki na systemy informatyczne, ataki odmowy usług, przejmowanie mocy obliczeniowej lub tworzenia i dystrybucja złośliwego oprogramowania[2].

Polski ustawodawca, w celu wdrożenia do krajowego obrotu prawnego Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2) (Dz.U.UE.L. 2022.333.80 ) – dokonał uchwalenia **Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa** – dalej zwaną ustawą o krajowym systemie cyberbezpieczeństwa.

Ustawa o krajowym systemie cyberbezpieczeństwa definiuje cyberbezpieczeństwo jako działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami.

[1] *MiniSterstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego (2013), Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa*

[2] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, K.* Czaplicki (red.), Warszawa, Wolters Kluwer 2019 r., s. 17

## Rodzaje zagrożeń cyberbezpieczeństwa

Celem cyberprzestępców jest kradzież danych użytkowników. Kradzież odbywać się może podczas niewielkich, dyskretnych ataków na pojedyncze ofiary lub podczas masowych operacji cyberprzestępczych na dużą skalę z wykorzystaniem stron internetowych www. i włamań do baz danych. Metody mogą być różne, ale cel pozostaje ten sam. W większości przypadków napastnicy próbują w pierwszej kolejności dostarczyć na komputer ofiary rodzaj szkodliwego oprogramowania, jako że jest to najkrótsza droga pomiędzy nimi a danymi użytkownika. Zamiary cyberprzestępcy ukierunkowane mogą być również na dokonanie strat finansowych w atakowanej instytucji lub utraty reputacji konkurencji, która zostaje sparaliżowana przez niedostępność usług, bądź w celu uzyskania okupu.

**Phishing** – Jest to metoda oszustwa, oznaczająca w tradycyjnym rozumieniu tego słowa podszywania się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron internetowych www.) pod inną osobę, instytucję lub znane marki, w celu wyłudzenia określonych informacji takich jak numery oraz hasła PIN kart płatniczych, hasła logowania do urzędów czy też płatności internetowej banków lub szczegółów karty kredytowej w celu wyłudzenia danych. Jest to rodzaj ataku oparty na tzw. inżynierii społecznej.

**Atak DDoS** (ang. *Distributed Denial of Service*) – Atak z tzw. rodziny DoS, atak na system komputerowy lub usługę sieciową w celu uniemożliwienia świadczenia tejusługi (odmowy jej realizacji) polegający na zablokowaniu działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów. Ataki te nie uszkadzają danych, gdyż ich celem jest utrudnienie lub uniemożliwienie dostępu do nich, co może skutkować równie kosztownymi stratami co utrata danych. Ataki te są stanowią jeden z najprostszych sposobów paraliżowania infrastruktury sieciowej oraz aplikacji, jednakże wymagają użycia równocześnie kilku tysięcy urządzeń. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania, i które na dany sygnał zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Do przeprowadzenia ataku DDoS używa się niezliczonego oprogramowania takiego jak LOIC (Low Orbit Ion Cannon), HOIC (High Orbit Ion Cannon), R-U-Dead-Yet (R.U.D.Y.), Mirai.

**Atak z wewnątrz** (ang. *The Inside Attack*) – Cyberatak nie zawsze musi pochodzić z internetu. Niektóre z najbardziej uciążliwych i groźnych naruszeń bezpieczeństwa mają miejsce wewnątrz podmiotu lub instytucji. Przykłady takich zdarzeń występują najczęściej w sytuacjach, gdy pracownik jest zwalniany lub sam odchodzi z pracy z własnych powodów. W celu uniknięcia zagrożenia, w każdym tego typu przypadku należy upewnić się, że powiązane z pracownikiem konta dostępu do sieci teleinformatycznej lub obsługiwanych przez niego zostały usunięte, a do wszystkich usług do których miał dostęp zmieniono hasła.

**Złośliwe oprogramowanie** *(Malware)* **-** To określenie opisuje całą gamę szkodliwych programów i aplikacji, które po uzyskaniu dostępu do sieci podmiotu lub instytucji może poczynić wiele szkód. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych, takich jak ransomware czyli programów żądających okupu za dostęp do danych.

**Atak Key Logger** (ang. *Key Logger Attack*) **–** Cyberprzestępcy używają programów, które mogą zapisywać naciśnięcie każdego klawisza na klawiaturze. Dzięki temu mogą poznać login i hasło użytkownika zainfekowanego komputera. Wystarczy raz zalogować się do danej usługi żeby dostarczyć przestępcom pełne dane.
Cyberprzestępcy przeprowadzają również ataki na usługi, które zawierają podatności oraz ataki na usługi źle skonfigurowane. Przykłady takich ataków stanowią:

**Atak SSL** (ang. *Secure Socket Layer*) – Protokół SSL/TLS ma za zadanie zapewnić integralność i poufność danych w komunikacji sieciowej, oparty jest na architekturze klient – serwer. Najczęściej kojarzony jest z protokołem HTTP (HTTPS), ale jest wykorzystywany także do zabezpieczania wielu innych protokołów, m. in. POP, IMAP, LDAP. Dzięki zastosowaniu protokołu szyfrującego wrażliwe dane przesyłane przez internet są zrozumiałe tylko przez uprawnionego odbiorcę. Jest to o tyle istotne, że informacje wędrują między wieloma urządzeniami, zanim trafią do adresata. Atak SSL jest próbą złamania, bądź też obejścia zabezpieczeń opartych na transmisji szyfrowanego strumienia danych.

**POODLE -** znane podatności protokołu SSL/TLS są nadal powszechnym zjawiskiem wśród użytkowników polskiego internetu. Zdecydowanie najczęściej występującą jest POODLE - przykłady podatności w kodzie, która umożliwia atak doprowadzający do ujawnienia zaszyfrowanych informacji. Mimo powszechnego występowania, POODLE nie jest podatnością najwyższego ryzyka, ponieważ nie umożliwia kradzieży kluczy

kryptograficznych, ani bezpośrednio przejęcia kontroli nad serwerem, a także wymaga aktywnego przechwycenia sesji TCP (atak typu man-in-the-middle).

**Man in the middle** – atak kryptologiczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy. Przykładem takiego ataku jest podsunięcie nadawcy własnego klucza przy transmisji chronionej szyfrem asymetrycznym. Wektor tego ataku wymaga umieszczenia atakującego lub pewnych złośliwych narzędzi pomiędzy ofiarą a docelowym zasobem, takim jak strona internetowa instytucji (urzędu lub banku) lub program służący do obsługi interesanta. Ataki te mogą być bardzo skuteczne i dość trudne do wykrycia, zwłaszcza dla użytkowników, którzy nie są świadomi niebezpieczeństw, jakie takie ataki stwarzają. Dla przykładu atak ten może to obejmować osobę tworzącą fałszywe rachunki lub faktury i umieszczającą je w skrzynce pocztowej ofiary, a następnie przechwytującą przelewy bankowe w momencie, gdy ofiara próbuje uregulować sfabrykowaną płatność.

**CWMP -** to usługa oparta na specyfikacji TR-069, implementowana najczęściej w domowych routerach DSL. Umożliwia zdalne zarządzanie urządzeniem przez operatorów, np. aktualizację firmware. Niepoprawna implementacja tej usługi pozwala na przejęcie całkowitej kontroli nad urządzeniem przez atakującego. Podatność tę wykorzystuje m.in. Mirai, infekując kolejne urządzenia.

**Malvertising** – pozwala przestępcom na dotarcie do użytkowników przeglądających zaufane strony internetowe poprzez nośniki jakimi są udostępniane na stronach internetowych reklamy, a następnie na instalowanie bez wiedzy i zgody użytkownika złośliwego oprogramowania na urządzeniach użytkownika.

## Czym jest CSIRT ?

Dyrektywa NIS, a następnie Dyrektywa NIS2 nałożyła na państwa członkowskie obowiązek wyznaczenia zespołu lub zespołów CSIRT - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego. W Polsce ustawa o krajowym systemie cyberbezpieczeństwa wyznacza trzy zespoły CSIRT na poziomie krajowym oraz CSIRT sektorowy, którym jest Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora. Ich zadaniem jest gromadzenie i wymiana informacji o incydentach bezpieczeństwa oraz współpraca operacyjna pomiędzy zespołami CSIRT w zakresie wykrywania, powstrzymywania i ograniczania skutków incydentów. Każdy CSIRT ma jasno określony zakres podmiotów, którym zapewniają wsparcie[3].

Dla większości podmiotów kluczowych lub podmiotów ważnych realizujących zadanie zależne od systemu informacyjnego ustawodawca powołał właściwy zespół reagowania na incydenty bezpieczeństwa komputerowego – CSIRT NASK. Jest to podmiot funkcjonujący w strukturach Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, nadzorowanego przez ministra właściwego do spraw informatyzacji. Do jego zadań należy m.in. zapewnienie spójnego i kompletnego systemu zarządzania ryzykiem na poziomie krajowym, realizacja zadań na rzecz przeciwdziałania cyberzagrożeniom o charakterze ponadsektorowym i transgranicznym, a także zapewnienie koordynacji obsługi zgłoszonych incydentów m.in. przez podmiot kluczowy lub podmiot ważny. **Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne** – interesanci podmiotu kluczowego lub podmiotu ważnego. CSIRT NASK stanowi kontynuacje działalności CERT POLSKA, który powstał w 1996 r. i był pierwszym w Polsce zespołem reagowania na incydenty.

Jak wskazują raporty roczne z działalności CERT Polska. CERT rejestruje łącznie średnio ok. 30 tys. i więcej zdarzeń, które można zakwalifikować jako incydenty cyberbezpieczeństwa, a liczba ta jest stale rosnąca. Tym samym odnotowuje się stały wzrost obsłużonych incydentów, w tym zdarzając się lata, w których wzrost ten przekracza 100 %. w porównaniu do roku ubiegłego. Najczęstszym typem incydentów był **phishing** – stanowiący aż ok 80 proc. wszystkich obsłużonych incydentów. (czym jest phishing – wyjaśniamy na str. 4).

[3] *ibidem*

**Dlatego użytkownicy i interesanci podmiotów medycznych i ochrony zdrowia powinni szczególnie zwracać uwagę na tę formę oszustwa.**

Jest to bardzo znaczący wzrost w porównaniu do poprzednich lat. Sektory gospodarki, których najczęściej dotyczyły incydenty to: media, handel hurtowy i detaliczny oraz poczta i usługi kurierskie. **Pomimo, że są to dziedziny dalekie od świadczeń opieki zdrowotnej, to pozyskane w ten sposób dane mogą posłużyć przestępcom do podszycia się pod skradzioną tożsamość i zrealizować płatne usługi lub uzyskać informacje o stanie zdrowia również w zakresie usług i informacji posiadanych przez podmioty medyczne i ochrony zdrowia.**

Najczęściej obserwowanym przez CERT schematem kampanii phishingowej było wyłudzenie danych logowania do portalu Facebook. Metoda ta bazuje na podszywaniu się pod właściciela konta Facebook i wysyłaniu wiadomości prywatnych do osób, które są dodane do listy znajomych na danym koncie, z prośbą o przelew przy użyciu systemu płatności mobilnych BLIK. Drugim popularnym atakiem phishingowym jest podszywanie się pod operatora szybkich płatności PayU oraz DotPay. Przestępcy w sposób masowy wysyłali do przypadkowych osób wiadomości e-mail lub SMS zawierające informacje o koniecznej opłacie np. dopłacie do paczki, zapłacie za egzekucję komorniczą itd. Podczas podawania danych uwierzytelniających (login, hasło) na fałszywej stronie serwisu płatności atakujący przechwytywali je i pozyskiwali możliwość zalogowania się do bankowości elektronicznej ofiary.

Znaczącą jest także lista incydentów dotyczących ataku **ransomware, polegających na kradzieży danych, zablokowaniu do nich dostępu i żądaniu okupu za dostęp do zaszyfrowanych danych.** Największą aktywność została odnotowana w podmiotach infrastruktury cyfrowej i wśród osób fizycznych oraz w administracji publicznej.

**Nie oznacza to jednak, że taki atak nie może przytrafi się osobie fizycznej. Może bowiem nastąpić zablokowanie dostępu do danych posiadanych przez podmiot medyczny, które akurat osobie zaatakowanej mogą być w danym momencie bardzo potrzebne (np. wyniki badań). W związku z tym bardzo istotnym jest by przestrzegać podstawowych zasad ochrony i bezpiecznego korzystania z internetu** **(zobacz str. 14).**

CSIRT NASK w ramach Ustawy o krajowym systemie cyberbezpieczeństwa w poprzednich latach obsługuje średnio kilkadziesiąt incydentów, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie powoduje lub może spowodować poważne obniżenie jakości lub

przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej; Zarejestrowane incydenty najczęściej dotyczą sektora bankowego, sektora energii, sektora ochrony zdrowia i coraz częściej sektora urzędowych usług publicznych.

**Warto zwrócić uwagę**, że CERT prowadzi **„Listę ostrzeżeń przed niebezpiecznymi stronami"**. Nieodpłatnie udostępnia się w niej spis domen (stron internetowych), który jest i powinien być wykorzystywany nie tylko przez operatorów telekomunikacyjnych, administratorów, ale także przez **użytkowników indywidualnych takich jak interesanci podmiotów medycznych** do poprawy bezpieczeństwa w sieci poprzez blokowanie znanych domen używanych do wyłudzeń danych oraz kradzieży środków finansowych[4].

## Czym jest incydent ?

Podmiot kluczowy lub podmiot ważny, o którym mowa w ustawie o krajowym systemie cyberbezpieczeństwa, realizuje zadanie zależne od systemu informacyjnego jest zobowiązany do obsługi incydentu w zakresie cyberbezpieczeństwa.

Incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.

Ustawodawca w przepisach ustawy o krajowym systemie cyberbezpieczeństwa zdefiniował kilka rodzajów incydentów związanych z cyberbezpieczeństwem. Najważniejszymi z punktu widzenia interesanta podmiotu kluczowego lub podmiotu ważnego są:

1) **incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej;**

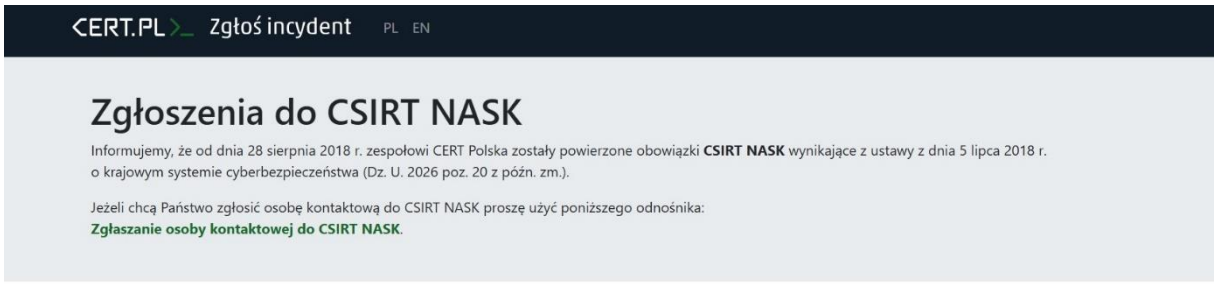
[4] *Dokumenty CERT Polska*

2) **incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;**

## Zgłaszanie incydentu cyberbezpieczeństwa

Zgłoszenia incydentu dokonują podmioty objęte przepisami ustawy o krajowym systemie cyberbezpieczeństwa, jednakże takie zgłoszenie może dokonać również każda osoba fizyczna np. będąca użytkownikiem przeznaczonego dla jej użytku systemu informatycznego udostępnionego przez podmiot medyczny i ochrony zdrowia.

Zgłoszenie incydentu cyberbezpieczeństwa, którego ofiarą padł podmiot będący administratorem systemów informatycznych przeznaczonych dla celów publicznych, może nastąpić poprzez przygotowany przez CSIRT NASK specjalnie do tego celu portal **www.incydent.cert.pl,** który umożliwia zgłaszanie incydentów zgodnie z Ustawą o krajowym systemie cyberbezpieczeństwa.



Po wejściu w portal internetowy, na samym początku należy dokonać wyboru, z perspektywy jakiego podmiotu planujemy dokonać zgłoszenia incydentu. Przyciski **„Osoba fizyczna/inne**

**podmioty”, „Podmiot kluczowy”, oraz „Podmiot ważny”** prowadzą do specjalnie przygotowanych formularzy, które umożliwiają zgłoszenie odpowiednio: incydentu poważnego, incydentu istotnego oraz incydentu w podmiocie publicznym.

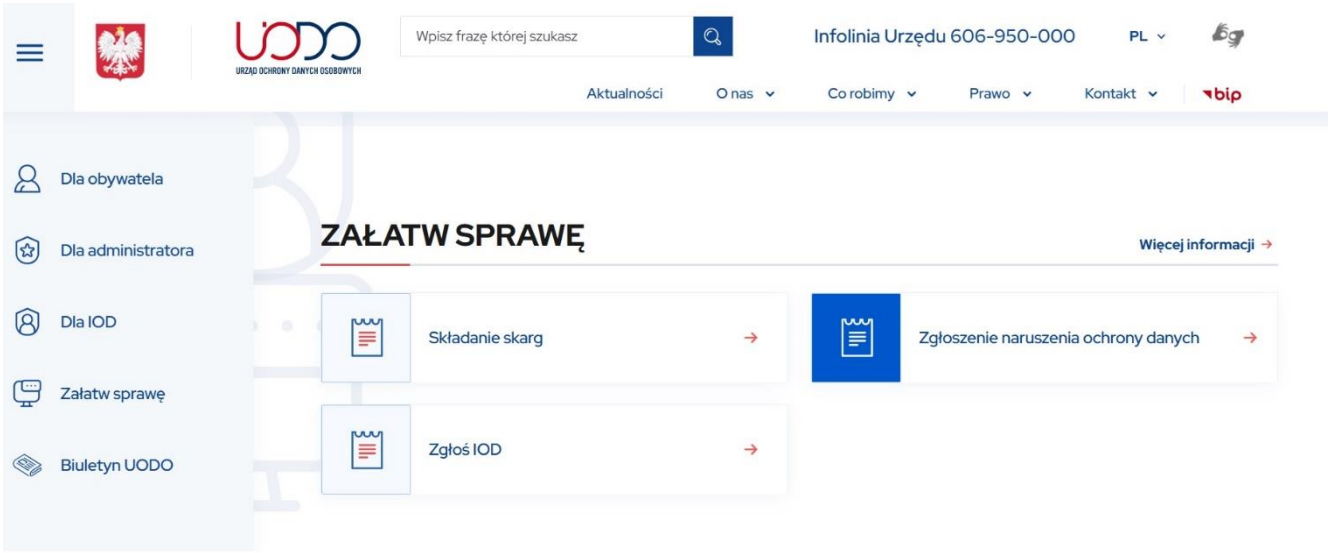
Rolę formularza dla dokonania zgłoszeń przez interesantów podmiotów kluczowych lub podmiotów ważnych pełni zakładka **„Osoba fizyczna / inne podmioty”**. W tym miejscu możliwe jest wybranie jednego z jedenastu najpopularniejszych rodzajów incydentów albo zaznaczenie **„Inne”** – co przedstawia fotografia poniżej.

Adekwatnie do wybranej opcji, prezentowany formularz zawiera dodatkowe wskazówki dla zgłaszającego.

## W jaki sposób powiadomić Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu ochrony danych ?

Zagrożenia nakierowane na przełamanie zabezpieczeń cyberbezpieczeństwa mogą godzić także w ochronę danych osobowych obywateli przechowywanych na serwerach podmiotu będący administratorem systemów informatycznych przeznaczonych dla celów publicznych. W przypadku naruszenia ochrony takich danych, podmiot oprócz zgłoszenia incydentu do CSIRT NASK, zobowiązany jest w terminie 72 godzin po stwierdzeniu naruszenia zgłosić je organowi nadzorczemu. Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

Zgłoszenia naruszenie ochrony danych osobowych administrator danych może dokonać poprzez stronę internetową Urzędu Ochrony Danych Osobowych (Urzędu) https://uodo.gov.pl/, wchodząc w podlink „Zgłoszenie naruszenia ochrony danych", znajdujący się u dołu strony internetowej.




Ważne jest, aby osoba, której dane dotyczą w pierwszej kolejności zwróciła się do administratora danych o usunięcie uchybień prawa. Po przeprowadzeniu postępowania w sprawie Prezes Urzędu Ochrony Danych Osobowych może nakazać spełnienie jej żądania.

Formularze znajdujące się na stronach internetowych przygotowane są dla zgłoszenia naruszeń ochrony danych z perspektywy administratora danych osobowych.

Urząd przewidział również formularza do wypełnienia przez osobę fizyczną, która doznała naruszenia ochrony jej danych osobowych, również dostępny w sekcji „Załatw sprawę",

w zakładce „Więcej informacji". Złożenie przez osobę fizyczną skargi na naruszenie ochrony danych może nastąpić także w każdej innej formie – najlepiej na piśmie – skierowanym pod adres siedziby Urzędu, bądź za pomocą ePUAP lub e-doręczeń.

**Adres:**
**Urząd Ochrony Danych Osobowych**
**ul. Stanisława Moniuszki 1A, 00-014 Warszawa**
**e-mail: kancelaria@uodo.gov.pl**

**Zgodnie z przepisami RODO – art. 57 ust. 1 pkt f) – Urząd rozpatruje skargi wniesione przez osobę, której dane dotyczą, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym.**

Jeżeli naruszenie dotyczy danych osób w różnych krajach Unii Europejskiej, Prezes UODO może, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy. W celu dokonania ustalenia wiodącego organu nadzorczego każdorazowo należy odnieść się do dokumentu **„Wytycznych dotyczących ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244 rew. 01)"**, przygotowanych przez Grupę Roboczą art. 29 Dyrektywy 95/46/WE, która jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności[5].

## Jak bezpiecznie korzystać z internetu i nie stać się ofiarą cyberprzestępcy ?

Internet jako ogólnoświatowy system połączeń między komputerami, niesie za sobą wiele zagrożeń, z których nie zawsze jako korzystający zdajemy sobie sprawę. Jak przy wykonywaniu każdej czynności, tak samo korzystając z internetu należy zachować ostrożność, by jak najbardziej ograniczyć prawdopodobieństwo zastania ofiarą cyberprzestępcy. Bezpieczeństwa w sieci internetowej nie można zdecydowanie ograniczyć jedynie do ochrony technologicznej. Cyberprzestępcy podejmują się najróżniejszych sposobów w tym zwykłej

[5] *Ibidem*

socjotechniki w celu nakłonienia użytkownika internetu do wykonania czynności, które ujawnią informacje o hasłach i stosowanych przez niego zabezpieczeniach, wykorzystują zainfekowane załączniki, fałszywe strony www i wiadomości e-mail, łudząco podobne do prawdziwych.

**Jak więc jak zminimalizować ryzyko stania się ofiarą cyberprzestępcy?**

1) korzystając z e-usług lub portali internetowych twórz długie i skomplikowane hasła dostępu – co najmniej ośmioznakowe zawierające małe, wielkie litery, znaki specjalne lub cyfry, a także poprzez zestawienie pięciu wyrazów niepowiązanych ze sobą i nieoddzielonych spacją;
2) dokonuj cyklicznych zmian haseł przynajmniej średnio co 60 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej;
3) przesyłając za pośrednictwem poczty e-mail pliki zawierające twoje dane osobowe przesyłaj je innym użytkownikom sieci w sposób zabezpieczony hasłem, natomiast samo hasło przekaż innym środkiem przekazu np. wiadomością sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata;
4) logując się na strony internetowe zwracaj uwagę na poziom bezpieczeństwa danej strony – symbolami znaczącymi o bezpieczeństwie są m.in. „zielona kłódka" informująca, że strona jest bowiem wyposażona w sprawdzony i ważny certyfikat lub element „https", oznaczający, że strona jest szyfrowana. Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel;
5) w przypadku spostrzeżenia czerwonej kłódki ze znakiem krzyżyka zachowaj szczególną ostrożność i powstrzymaj się od wprowadzania żadnych danych, gdyż istnieje możliwość, iż ktoś podszywa się pod daną witrynę, aby przechwycić cenne informacje;unikaj umieszczania w tzw. chmurze plików czy informacji zawierających wrażliwe danych na twój temat;
6) unikaj logowania się na swoje konta internetowe przy pomocy publicznego wifi lub na publicznych komputerach;
7) uważaj na strony internetowe, które wymagają instalacji oprogramowania – w takim przypadku najlepiej uprzednio przeskanuj wszystkie programy pobierane z internetu za pomocą aktualnego oprogramowania zabezpieczającego;
8) unikaj korzystania ze stron internetowych, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla użytkownika);
9) unikaj otwierania nieznanych linków i załączników w wiadomościach e-mail;

10) zwracaj uwagę i upewnij się czy osoba, z którą nawiązujesz kontakt jest tym, za kogo się podaje;
11) zwracaj uwagę na wiadomości z prośbą o podanie szczegółów konta, gdyż instytucje finansowe oraz urzędu bardzo rzadko proszą o podanie takich szczegółów drogą elektroniczną;
12) zainstaluj oprogramowanie antywirusowe i utrzymuj je w aktualności;
13) korzystaj z najnowszych wersji przeglądarek internetowych posiadających zainstalowane aktualizacje;
14) zwróć uwagę, by system operacyjny posiadał włączoną funkcję automatycznych aktualizacji i instalować wszelkie aktualizacje zaraz po ich udostępnieniu przez firmę dostarczającą oprogramowanie.

## Rozszerz swoją wiedzę – dodatkowe źródła informacji o zagrożeniach bezpieczeństwa użytkowników sieci internetowej

Mając na uwadze szerokie spektrum zagadnienia bezpieczeństwa użytkowników sieci internetowej, warto również na bieżąco pozostawać w kontakcie z aktualnymi informacjami o zagrożeniach. W tym celu przedstawiamy Państwu zaufane źródła informacji dostępne pod poniżej wskazanymi adresami internetowymi:

- zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch/
- publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/
- poradniki na witrynie internetowej Serwis Rzeczypospolitej Polskiej https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni. mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: https://www.stopthinkconnect.org/

**DZIĘKUJEMY ZA UWAGĘ.**