CYBERPRZESTĘPCZOŚĆ
ZAGROŻENIA WYNIKAJĄCE Z UŻYTKOWANIA INTERNETU

Autor:
dr hab. prof. UPH Norbert Malec

Warszawa 2021

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

Spis treści

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

1. Obszary zagrożeń

Przełom XX i XXI wieku to czas kolejnej rewolucji przemysłowej nazywanej transformacją cyfrową. Warto podkreślić, że ta transformacja najintensywniej zmieniła życie i organizację otaczającej nas rzeczywistości dając źródło nowym, dotąd nieznanym, zagrożeniom.

Postęp technologiczny sprawił, że żyjemy w erze wiedzy cyfrowo upowszechnianej i informacji, które są nieustannie przetwarzane. Jest to era zdominowana przez komputeryzację, automatyzację oraz optymalizację różnych procesów działalności człowieka. Z rozmysłem wprowadzane są nowe procesy, które z założenia mają być szybsze, bardziej efektywne i co najważniejsze coraz tańsze. Coraz częściej mówi się o koncepcji cyfrowego wiru (The Digital Vortex)[1]. Według której to technologia sama w sobie wpływa i kształtuje decyzje człowieka, a tym samym niejako wyznacza kierunek w jakim idziemy i napędza cały proces transformacji. Technologia jest obecna we wszystkich dziedzinach i obszarach otaczającej nas rzeczywistości od telekomunikacji i energetyki poprzez edukację, handel, przemysł, ochronę zdrowia aż do rozrywki i mediów. Powszechnie staje się korzystanie z rozwiązań takich jak bankowość elektroniczna, podpis elektroniczny czy portale społecznościowe i rozrywkowe, dzięki którym wirtualizacja i cyfryzacja na dobre wkraczają do codziennej aktywności człowieka. Wszystkie obszary aktywności są połączone i działają w wielu sieciach przepływu informacji, tym samym nie można lekceważyć cyberprzestrzeni oraz cyberbezpieczeństwa, które stają się największymi wyzwaniami dzisiejszej rzeczywistości.

Do niedawna środowiskiem aktywności i prowadzenia działań ludzkich była przestrzeń lądowa, morska, powietrzna i kosmiczna. Cyberprzestrzeń jest dziś wymieniana jako kolejna płaszczyzna i wymiar, w którym człowiek wykazuje aktywność (również militarną). Warto zaznaczyć, że w odróżnieniu od dotychczas znanych środowisk, jest w pełni stworzona i ukształtowana przez człowieka i nie jest ograniczona terytorialnie. Przyjmuje się również, że człowiek ma nad nią największą kontrolę. Wymieniając cechy cyberprzestrzeni najczęściej

[1] Koncepcja opracowana przez IMD Switzerland (Instytut badawczy w Szwajcarii). Koncepcja „The Digital Vortex" pojawia się od 2015 roku w raportach publikowanych przez IMD.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

przedstawiane są jej cztery zasadnicze elementy: anonimowość, aterytorialność, systematyczność i globalny zasięg.[2]

Najszerzej dostępnym źródłem wiedzy, przestrzenią najszybszej wymiany informacji oraz świadczenia niezliczonych usług jest dziś Internet, często mylnie utożsamiany z pojęciem cyberprzestrzeni. Historia Internetu sięga lat 60-tych XX wieku, kiedy to powstała akademicka sieć ARPANET będąca jego pierwowzorem. ARPANET, finansowany ze środków na rozwój wojska, miał być eksperymentalną próbą utworzenia sieci komputerowej, która miałaby działać bez wyraźnie wyodrębnionego punktu centralnego. Takie podejście miało zapewnić ciągłe działanie nawet w przypadku uszkodzenia jednego z komponentów sieci. Zastosowanie koncepcji sieci rozproszonej, czyli brak jednego, wyraźnego węzła, który zarządza całą siecią miał z założenia eliminować podatność i zagrożenie ataku przeciwnika na ten fragment sieci. Szczególnie ważne stawało się to w przypadku zamiaru korzystania z sieci do dowodzenia armią w czasie konfliktu. Eksperyment z biegiem lat rozrastał się, sieć powiększała się i obejmowała kolejne uczelnie oraz środowiska akademickie.

W latach 80-tych postanowiono ostatecznie rozdzielić część wojskową ARPANET od części akademickiej. Cywilna część sieci rozwijała się od tej pory bez wsparcia i nadzoru wojska tworząc współczesny Internet, czyli globalną sieć połączonych ze sobą urządzeń umożliwiająca komunikację w oparciu o protokół TCP/IP. Część wojskowa zapewne nadal funkcjonuje, jednak prace nad jej rozwojem zostały utajnione.

Warto wspomnieć, że często zamiennie z Internetem używane jest również określenie World Wide Web (WWW). Również i w tym przypadku, tak jak cyberprzestrzeń nie jest Internetem, tak WWW nie może być używana w tym znaczeniu. Web to zaledwie jedna z wielu usług świadczona w Internecie, podobnie jak poczta elektroniczna itp. Internet jest wykorzystywany jako warstwa nośna dla aplikacji. Usługa ta wykorzystuje protokół HTTP i stanowi zbiór powiązanych ze sobą dokumentów i różnorakich zasobów. Web jako usługa rozpoczął swoje działanie w 1990 roku i z założenia jest systemem informacyjnym tworzonym z myślą o zbieraniu, publikowaniu, udostępnianiu zasobów wiedzy i umożliwianiu współpracy oraz dzielenia się pomysłami na odległość.

[2] Marczyk M., Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, Przegląd Teleinformatyczny nr 1-2/2018, s. 60 i nast.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

Charakterystyczna dla Internetu jest jego złożoność i wielowarstwowość. Szacuje się że przeciętny użytkownik podczas codziennego korzystania z sieci widzi nie całe 5% zawartości całego Internetu. Dzieje się tak ponieważ najczęściej korzystamy z najszerzej dostępnej, zewnętrznej warstwy, czyli Internetu powierzchniowego. Oprócz tej warstwy możemy wyróżnić jeszcze dwie kolejne – Deep Web oraz Dark Web stanowiące około 96% pozostałych zasobów Internetu.

Struktura sieci www

World Wide Web

Sufrace Web	Yahoo Google Bing CNN.com	Dostępny Indeksowane dla wyszukiwarek Mała nielegalna działalność Stosunkowo mały rozmiar
Deep Web	Sieć ukryta Akademickie bazy danych Dokumenty rządowe	Dostępne za pomocą hasła, szyfrowania Nieindeksowane dla wyszukiwarek Niewielka nielegalna działalność Ogromny rozmiar, rosnący wykładniczo
Darknet/Dark Web	TOR Silk Road	Ograniczone do specjalnych przeglądarek Nieindeksowane dla wyszukiwarek Duża skala nielegalnej działalności Z natury niemierzalny

Surface Web, czyli sieć powierzchniowa, zwana również siecią widoczną, indeksowaną lub Lightnetem jest warstwą sieci WWW najłatwiej dostępną dla ogółu użytkowników. Do poruszania się w jej obrębie wykorzystywane są szeroko dostępne, standardowe wyszukiwarki internetowe, jak na przykład popularny Google.

Następną warstwę stanowi sieć ukryta o nazwie Deep Web. Głębokiej zawartości sieci nie można wyszukać ani uzyskać do niej bezpośredniego dostępu przy użyciu powszechnie znanych i używanych wyszukiwarek internetowych. Użytkownik musi wiedzieć czego szuka i najczęściej dysponować bezpośrednim linkiem prowadzącym do poszukiwanego zasobu czy strony. Deep Web obejmuje wiele szeroko używanych serwisów jak chociażby poczta internetowa, bankowość elektroniczna jak również płatne usługi, serwisy streamingowe (np. Netflix itp.).

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

Ostatnia, a zarazem najgłębsza i najciemniejsza warstwa Internetu to Dark Web zamiennie nazywany Darknetem. Ciemna sieć to strony na serwerach, do których zwykła wyszukiwarka nie ma dostępu. Aby użytkownik mógł korzystać z zasobów tej warstwy potrzebuje specjalnych uprawnień i narzędzi. Najbardziej znanym i najczęściej używanym narzędziem w Darknecie jest TOR (The Onion Router), który aby zapewnić użytkownikowi anonimowość kieruje ruch do stron poprzez warstwy szyfrowania. TOR wielokrotnie szyfruje dane użytkownika (głównie lokalizację) oraz kieruje ruch przez losowo wybrane serwery przesiadkowe które odszyfrowują tylko niewielki fragment zapytania. Zastosowany mechanizm to trasowanie warstwowe trzeciej generacji mające na celu zapobieganie analizie ruchu sieciowego i ukrywaniu użytkownika. Takie działanie zapewnia użytkownikowi pełną anonimowość i uniemożliwia jego namierzenie.

Darknet z założenia miał być niedostępny, ukryty i anonimowy. Taki zestaw cech jak można się domyślić przyciąga osoby, którym zależy, aby ich działania w sieci zostały nieujawnione. To właśnie ciemna strona sieci jest miejscem nielegalnej działalności. Przykładem działań jakie można spotkać w tej warstwie może być przestępczość komputerowa, udostępnianie plików (nielegalne oprogramowanie, pliki poufne, zakazane treści), sprzedaż towarów objętych ograniczeniami (substancje psychoaktywne i niedozwolone) czy też rozpowszechnianie nieprawdziwych informacji.

Wiele trudności sprawia jednoznaczne zdefiniowanie Internetu i prawidłowe posługiwanie się nomenklaturą związaną z siecią. Obecnie jedną z największych przeszkód stojących na drodze formalno-prawnego uregulowania kwestii bezpieczeństwa cyberprzestrzeni, zarówno na poziomie państwowym, jak i międzynarodowym, są trudności ze spójnym zdefiniowaniem terminów dotyczących tego zagadnienia. Problem stanowi nawet uzgodnienie definicji pojęcia samej cyberprzestrzeni[3]. W jednej ze swoich opublikowanych rekomendacji poświęconej narodowym strategiom cyberbezpieczeństwa również Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji (ENISA – European Network and Information Security Agency) podkreśla brak jednolitej nomenklatury. Zarówno na poziomie europejskim, jak i międzynarodowym wyraźnie brakuje zharmonizowanej definicji bezpieczeństwa cybernetycznego. Rozumienie cyberbezpieczeństwa i innych kluczowych

[3] Grzelak M., Liedel K., Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, Bezpieczeństwo Narodowe nr 22/2012, s. 129 i nast.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

terminów różni się znacznie w zależności od kraju. Wpływa to na różne podejścia do strategii bezpieczeństwa cybernetycznego w poszczególnych krajach. Brak wspólnego zrozumienia i podejścia między krajami może utrudniać współpracę międzynarodową, której potrzebę uznają wszystkie kraje.[4]

Dynamiczny rozwój technologii informatycznych sprawił, że ENISA wprowadza standaryzację dla pojęcia cyberprzestrzeni. Ze względu na kompleksowość i złożoność pojęcia zaproponowano kontekstową definicję: „Cyberbezpieczeństwo odnosi się do bezpieczeństwa cyberprzestrzeni, gdzie sama cyberprzestrzeń rozumiana jest jako zestaw powiązań i relacji między obiektami dostępnymi za pośrednictwem sieci telekomunikacyjnej, jak również do samych obiektów, gdy posiadają one interfejsy umożliwiające ich zdalną kontrolę, zdalny dostęp do danych lub ich udział w kontroli działań w cyberprzestrzeni." Cyberbezpieczeństwo będzie zatem stanowiło „zbiór narzędzi, zasad, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, podejść do zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk i technologii, które mogą być wykorzystane do ochrony środowiska cybernetycznego oraz zasobów organizacji. Zasoby organizacji obejmują podłączone urządzenia komputerowe, personel, infrastrukturę, aplikacje, usługi, systemy telekomunikacyjne oraz całość przekazywanych, a także przechowywanych, informacji w środowisku cybernetycznym. Cyberbezpieczeństwo stara się zapewnić osiągnięcie i utrzymanie pożądanego poziomu ochrony organizacji i jej zasobów przed zagrożeniami bezpieczeństwa w środowisku cybernetycznym"[5].

W polskim porządku prawnym funkcjonują pojęcia cyberprzestrzeni i jej bezpieczeństwa. W nowelizacji ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej w art. 2 czytamy, że cyberprzestrzeń jest rozumiana jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[6]. Zgodnie z ustawą o informatyzacji działalności

[4] ENISA, National Cyber Security Strategies, s. 9 i nast.
[5] ENISA, Definition of Cybersecurity. Gaps and overlaps in standardization, s. 30-31
[6] Dz. U. 2002 nr 156 poz. 1301- Ustawa o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

podmiotów realizujących zadania publiczne systemem teleinformatycznym jest to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, 1579, 1823, 1948, 1954 i 2003)”[7]. Urządzeniem końcowym zgodnie z Prawem Telekomunikacyjnym jest natomiast „urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci”[8].

Zgodnie z przytoczonymi definicjami możemy wywnioskować, że cyberprzestrzeń określa przestrzeń przetwarzania i wymiany informacji oraz powiązania między jej składowymi urządzeniami, systemami, a także ich relacje z użytkownikami. Przestrzeń ta jest tworzona przez zespół połączonych ze sobą urządzeń i systemów, które umożliwiają wysyłanie, przetwarzanie i przechowywanie danych za pomocą sieci telekomunikacyjnych.

Bezpieczeństwo cyberprzestrzeni w Polsce będzie się odnosiło do „procesu obejmującego zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego i bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych)”[9].

[7] Dz. U. z 2017 r. poz. 570 – Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne
[8] Dz. U. 2004 nr 171 poz. 1800 - Prawo Telekomunikacyjne
[9] https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, (11.12.2021)

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

2. Rodzaje zagrożeń w cyberprzestrzeni

Zagrożenia są nieodłącznym elementem przestrzeni cybernetycznej. Obecnie, gdy tak wiele procesów przebiega w sieci i zależy od podłączenia do Internetu, za pomocą cyberataków można osiągnąć praktycznie wszystko. Za zagrożeniami i atakami w sieci prawie zawsze stoi możliwość osiągnięcia korzyści finansowej, czy też chęć przeprowadzenia ataku ideologicznego, politycznego czy nawet militarnego. Cyberprzestrzeń pozostaje obszarem działania zarówno indywidualnych przestępców, jak i zorganizowanych grup przestępczych oraz środowisk ekstremistycznych i organizacji terrorystycznych.

Upowszechnienie dostępu do Internetu, w kontekście globalnego charakteru cyberprzestrzeni, przy jednocześnie stosunkowo dużej możliwości zachowania anonimowości i popełniania przestępstw na terenie jednego państwa z obszaru innego, sprzyja występowaniu różnego rodzaju zagrożeń dotyczących bezpieczeństwa systemów informatycznych. Zagrożenia te mają charakter elastyczny i bezpośrednio zależą od kierunków rozwoju nowoczesnych technologii. Istotnym jest również to, że zagrożeń tych nieustannie przybywa i pojawiają się nowe ich formy. ENISA wyróżniła osiem głównych kategorii właściwych dla różnych źródeł zagrożeń[10]. Ataki fizyczne obejmujące wszelkiego typu fizyczne zagrożenia mogące oddziaływać na urządzenia stanowią pierwszą kategorię. Do tej grupy będą należały akty wandalizmu, kradzieże (nośników, dokumentów, urządzeń), zniszczenia i uszkodzenia sprzętu powstałe w wyniku działań wojennych lub aktów terroryzmu, ale również szkody spowodowane przez nieautoryzowany dostęp do pomieszczeń, wyciek informacji czy nieuprawnione udostępnianie informacji.

Kolejna grupa to niezamierzone uszkodzenie bądź utrata informacji lub zasobów, czyli szkody powstałe w wyniku błędu ludzkiego. Będą to nieintencjonalne udostępnienia informacji poufnych przez pracowników, wyciek informacji w wyniku błędu użytkownika, niewłaściwe zachowanie osób z podniesionymi uprawnieniami (administratorów), nieintencjonalna ingerencja w zmianę konfiguracji systemów, straty powstałe na skutek działania osób trzecich, wywołane przez testy penetracyjne lub poprzez usunięcie i utratę danych, jak również nieprawidłowe użycie systemów lub urządzeń skutkujące utratą integralności danych.

[10] P. Trimintzios Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for EU, s. 72-78

Bezgraniczne Bezpieczeństwo

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

Trzecią kategorią wskazaną przez ENISA są katastrofy naturalne lub środowiskowe, a więc wszelkiego typu zdarzenia losowe związane z działaniem sił przyrody. W tej kategorii znajdą się klęski żywiołowe oraz katastrofy i anomalie pogodowe, których działanie będzie stanowiło zagrożenie utraty dostępności do danych lub infrastruktury. Przykładem są tu powodzie, trzęsienia ziemi, huragany, pożary, eksplozje, promieniowanie, duże zapylenie, jak również zagrożenia z przestrzeni kosmicznej związane z burzami elektromagnetycznymi.

Następna grupa zagrożeń ma swoje źródło w niepoprawnym działaniu, usterkach technicznych itp. Mówimy to o każdym niepoprawnym, wadliwym działaniu systemu lub sprzętu, które jest spowodowane awarią dowolnego komponentu urządzenia. Przykładem może być niepoprawne działanie np. systemu chłodzenia w serwerowni, które może doprowadzić do załamania używanej infrastruktury.

Piąta kategoria zagrożeń to awarie o dużym zasięgu dotyczące zwykle braku jakiegoś zasobu, przykładowo personelu w wyniku strajku, dostępu do Internetu, odcięcia prądu czy też brak wsparcia dla utrzymania przykładowego systemu.

Podsłuch, przejęcie informacji związane z przechwyceniem informacji, czy też ruchu sieciowego zostały wyodrębnione przez ENISA jako kolejny zestaw. Jest to grupa zagrożeń mających związek ze szpiegostwem gospodarczym i wywiadem. Prowadzenie rekonesansu sieci, manipulowanie ruchem sieciowym i zbieranie informacji rodzi zagrożenie identyfikacji i wykrycia słabych punktów bezpieczeństwa w jej obszarze. Do tej grupy należą również atak typu „*Man in the middle*" (atak wykorzystujący podsłuch i modyfikujący treść wiadomości przesyłanych między stronami).

Jedną z kategorii stanowią zagrożenia prawne wynikające z naruszenia zasad, przepisów i ustawodawstwa, naruszenia związane z nieprawidłowym wykorzystaniem i przetwarzaniem danych osobowych. Można do tej kategorii zaliczyć także wszelkie nieuprawnione korzystanie z zasobów chronionych prawem własności intelektualnej powodujące narażenie na kary finansowe, prawne czy tez utratę reputacji.

Ostatnią grupę zagrożeń wskazywanych przez ENISA stanowią nadużycia i złośliwe oprogramowanie. Jest to najszersza, a zarazem najbardziej znacząca kategoria. Znalazły w niej miejsce różne typy ataków technicznych oraz zagrożenia społeczne zagrażające bezpieczeństwu użytkowników przestrzeni cyfrowej. Tą kategorię możemy podzielić na:

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

1. Działania związane z kradzieżą tożsamości użytkowników:
   a) przechwytywanie danych używanych do logowania przez np. trojany.
2. Otrzymywanie i odbieranie niechcianej korespondencji z nieznanych źródeł za pomocą poczty elektronicznej (SPAM).
3. Ataki na systemy komputerowe lub usługi sieciowe mające na celu uniemożliwienie ich działania (DoS – Denial of Service i DDoS – Distrubuted Denial od Service):
   a) DDoS na warstwę sieci – wykorzystywanie protokołu komunikacji, zniekształcanie oraz fałszowanie pakietów, zalewanie dużą ilością pakietów i zapytań,
   b) DDoS na warstwę aplikacji – przykładowo Ping of Death[11] lub WinNuke[12],
   c) DDoS sieciowo-aplikacyjny.
4. Wykorzystywanie złośliwego kodu, oprogramowania w celu szkodliwego działania na sprzęt lub użytkownika:
   a) Zatruwanie wyszukiwarek jest metodą ataku, w ramach którego cyberprzestępcy tworzą złośliwe strony internetowe i tak modyfikują wyszukiwarki, aby prezentowały wyniki w pierwszej kolejności prowadząc użytkowników do nich. Witryny te zwykle są powiązane z najczęściej wyszukiwanymi i popularnymi frazami w danym momencie przez dużą grupę osób (np. wiadomości, ostatnie wydarzenia itp.). Szacuje się, że nawet jedna czwarta pierwszej strony wyników wyszukiwania popularnych fraz jest powiązana ze złośliwymi stronami internetowymi. Najskuteczniejszą ochroną przed tym zagrożeniem jest regularne instalowanie dostępnych aktualizacji dla wszystkich używanych przeglądarek.
   b) Wykorzystywanie zaufania użytkowników do mediów społecznościowych. Użytkownicy mają duże zaufanie do informacji publikowanych przez sieci

[11] Atak, w którym atakujący próbuje zniszczyć, zdestabilizować lub zawiesić docelowy komputer lub usługę poprzez wysyłanie zniekształconych lub ponadwymiarowych pakietów za pomocą prostej komendy ping.
[12] Atak polegający na wysłaniu do komputera ofiary zniekształconego pakietu TCP mającego wywołać zawieszenie atakowanego urządzenia. Komputer wyświetla komunikat błędu (blue screen of death), a tym samym uniemożliwia dalszą pracę urządzenia. Konieczne jest zresetowanie maszyny, a co za tym idzie utrata wszelkich niezapisanych danych.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

znajomych na portalach społecznościowych, ze względu na poczucie bezpieczeństwa wynikające z przekonania, że są wśród grona przyjaciół. Najczęściej nie weryfikują oni udostępnianych linków lub plików pod kątem potencjalnego zagrożenia dla bezpieczeństwa, co sprawia, że ten obszar jest chętnie wykorzystywany do przeprowadzania ataków.

c) Robaki i trojany czyli odpowiednio samoreplikujące się programy komputerowe nie potrzebujące pliku w roli nosiciela oraz programy podszywające się pod aplikacje, tak aby móc implementować dodatkowe, szkodliwe funkcje.
d) Rootkity pozwalające na niezauważane działanie w systemie poprzez ukrywanie szkodliwych plików lub procesów w systemie.
e) Oprogramowanie złośliwe dedykowane na telefony komórkowe.
f) Infekowanie znanych i popularnych aplikacji dostępnych dla telefonów komórkowych.
g) Podnoszenie i rozszerzanie uprawnień.
h) Ataki skierowane na aplikacje internetowe, wstrzykiwanie kodu.
i) Spyware i adware czyli oprogramowanie szpiegujące oraz fałszywe reklamy.
j) Wirusy komputerowe będące niewielkimi programami komputerowymi o zdolności powielania się, które atakują urządzenia bez wiedzy i zgody użytkowników. W przeciwieństwie do robaków, aby się przenosić między urządzeniami potrzebują nośnika, najczęściej w postaci pliku załączonego np. do poczty elektronicznej z nieznanego źródła.
k) Rougeware, scareware – fałszywe oprogramowanie podszywające się na przykład pod oprogramowanie bezpieczeństwa, a które faktycznie zastrasza użytkownika.
l) Ransomware będący szkodliwym oprogramowaniem, które po dostaniu się do urządzenia atakowanego blokuje dostęp do danych i zasobów. Aby przywrócić stan pierwotny i umożliwić użytkownikowi odczyt danych i dostęp do zasobów żąda okupu.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

m) Eksploity wykorzystujące błędy i podatności w oprogramowaniu pozwalające na uruchomienie obcego kodu i tym samym na przejęcie kontroli nad danym procesem.

5. Inżynieria społeczna wykorzystująca podstęp i manipulację w celu zmuszenia użytkownika do ujawnienia poufnych informacji, tak aby wykorzystać je do nieuczciwych celów:
   a) Phishing czyli oszustwo z wykorzystaniem poczty elektronicznej. Sprawca ataku tworzy i wysyła korespondencję wyglądającą na prawdziwą. Celem takiego e-maila jest próba zebrania danych osobowych lub finansowych od nabranego odbiorcy. Zazwyczaj podszywające się e-maile przychodzą z szeroko rozpoznawanych, popularnych i godnych zaufania adresów.
   b) Spear phishing – ukierunkowany na konkretną instytucję lub osobę phishing. Wiadomość e-mail, która została stworzona, aby zdobyć fałszywe zaufanie i tym samym zmusić ofiarę do ujawnienia niejawnych tajemnic biznesowych lub osobistych, które mogą zostać wykorzystane przez przeciwnika.
6. Wycieki informacji i nadużycia z nimi związane:
   a) wycieki mające wpływ na prywatność i aplikacje mobilne,
   b) wycieki mające wpływ na prywatność i aplikacje internetowe,
   c) wycieki mające wpływ na ruch sieciowy,
   d) wycieki wpływające na pracę chmury obliczeniowej.
7. Generowanie, a także wykorzystywanie niepoprawnych certyfikatów elektronicznych używanych w celu zwiększenia bezpieczeństwa oraz wiarygodności komunikacji lub sesji. Chodzi tu o certyfikaty SSL.
   a) Utrata integralności danych wrażliwych.
   b) Man in the middle, przechwytywanie sesji.
   c) Inżynieria społeczna – atakujący podpisują malware wyglądającym na ważny certyfikatem, zwykle pochodzącym od znanego oraz rozpoznawanego i cieszącego się zaufaniem dostawcy certyfikatów.
   d) Fałszywe certyfikaty SSL.

8. Manipulowanie sprzętem lub oprogramowaniem:
    a) anonimowe proxy czyli serwer anonimizujący, który ma na celu ukrywanie maszyny użytkownika oraz usunięcie innych informacji dzięki którym możliwe byłoby jego zidentyfikowanie,
    b) nadużywanie mocy obliczeniowej chmury w celu przeprowadzania ataków (cybercrime as a service – cyberprzestępczość),
    c) wykorzystywanie luk w zabezpieczeniach i podatności, szczególnie podatności typu 0-day,
    d) dostęp do stron internetowych poprzez łańcuchy serwerów proxy zapewniający brak możliwości śledzenia ruchu,
    e) dostęp i ingerencja w firmware urządzenia, czyli oprogramowanie sprzętowe zainstalowane na stałe na urządzeniu, a umożliwiające jego obsługę,
    f) niedozwolone i nieautoryzowane zmiany wprowadzane do oprogramowania,
    g) używanie niedozwolonych i niedopuszczonych do użytku urządzeń.
9. Manipulowanie informacją:
    a) takie manipulowanie informacją, aby możliwe było wyparcie się, a także zaprzeczenie działaniu,
    b) przejmowanie przestrzeni adresowej (prefiksy IP) określane również jako przechwytywanie tras lub przechwytywaniem adresów IP. Jest to nielegalne przejmowanie grup adresów IP przez niszczenie tabel routingu internetowego,
    c) manipulacje w obrębie tablic routingu,
    d) manipulacje dotyczące usługi DNS takie jak zatrucie, podszywanie się mające na celu przekierowanie ruchu sieciowego na konkretne strony,
    e) fałszowanie rekordów,
    f) przejęcie adresacji autonomicznej czyli zbioru połączonych prefiksów routingu adresacji,
    g) manipulacja i zmiany w obrębie systemu adresacji autonomicznej,
    h) nieautoryzowane zmiany w konfiguracji.
10. Używanie narzędzi audytorskich niezgodnie z ich przeznaczeniem.

Bezgraniczne Bezpieczeństwo

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

11. Niewłaściwe i niezgodne z przeznaczeniem wykorzystywanie informacji i systemów włącznie z aplikacjami mobilnymi.
12. Nieautoryzowane działania:
    a) nieautoryzowane korzystanie z administracji urządzeniami i systemami,
    b) nieautoryzowane korzystanie z oprogramowania,
    c) nieautoryzowany dostęp do systemów i sieci,
    d) włamanie do sieci,
    e) nieautoryzowane zmiany rekordów.
13. Nieautoryzowana instalacja oprogramowania:
    a) ataki internetowe jak złośliwy URL czy inne ataki oparte na przeglądarce.
14. Ujawnienie danych poufnych – wyciek danych.
15. Oszustwa oparte o rozsiewanie nieprawdziwych informacji, pogłosek lub nieprawdziwych oskarżeń:
    a) wywoływanie u ofiary określonego, z góry zaplanowanego zachowania i reakcji poprzez udostępnienie nieprawdziwej informacji.
16. Działania zdalne:
    a) zdalne wykonanie kodu,
    b) zdalne wykorzystanie narzędzi dostępowych,
    c) botnety wykorzystywane zdalnie np. do rozsyłania spamu.
17. Ataki ukierunkowane typu APT szczególnie trudne do wykrycia i z założenia działające długotrwale. Zwykle wybranym celem są media, duże korporacje i rządy, czyli podmioty posiadające znaczne zasoby danych, które są atrakcyjnym łupem dla atakujących.
    a) złośliwe oprogramowanie na urządzenia mobilne (telefony).
    b) spear phishing,
    c) instalacja wyrafinowanego i ukierunkowanego złośliwego oprogramowania,
    d) ataki typu Watering Hole będące strategią polegającą na obserwowaniu grupy do której należy ofiara. Określa się z jakich stron najczęściej dana grupa korzysta i zaraża się jedną z nich. Prowadzi to do zainfekowania co najmniej jednego członka grupy docelowej i pozwala w dalszej strategii na

Bezgraniczne Bezpieczeństwo

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

rozszerzenie grupy zainfekowanych. Potocznie takie działanie nazywane jest atakiem wodopoju.

18. Wadliwie zaprojektowane i działające procesy biznesowe.
19. Brute force czyli technika wykorzystywana do łamania haseł. Polega ona na przetestowaniu wszelkich istniejących kombinacji. Taki atak siłowy może trwać długo zanim przyniesie oczekiwane rezultaty. Powszechnie znanym rozwiązaniem będącym zabezpieczeniem przed tym atakiem jest automatyczne blokowanie konta użytkownika jeśli wpisuje on niepoprawne hasło logowania więcej niż określoną liczbę razy.
20. Nadużycie autoryzacji.

Zaproponowany przez Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji katalog zagrożeń jest obszerny i wraz z dynamicznym rozwojem technologii nie jest to katalog zamknięty i odzwierciedla złożoność i kompleksowość potencjalnych zagrożeń występujących w cyberprzestrzeni. Użytkownicy sieci mogą być narażeni na wiele typów działań mających wpływ na bezpieczeństwo korzystania z zasobów tej przestrzeni. Ze względu na niejednorodny charakter tych zagrożeń nie istnieje jeden, skuteczny sposób ochrony i konieczne jest stosowanie takiego zestawu mechanizmów, który najpełniej i najskuteczniej mógłby zabezpieczać użytkownika przed wieloma potencjalnymi możliwościami ataków.

Krajobraz cyberbezpieczeństwa ciągle się zmienia, ale oczywiste jest, że cyberzagrożenia stają się coraz poważniejsze i występują coraz częściej. Statystyki cyberbezpieczeństwa za rok 2021 przedstawiają się w następujący sposób:

- 85% naruszeń cyberbezpieczeństwa spowodowanych jest błędem ludzkim,
- 94% wszystkich złośliwych programów jest dostarczanych przez e-mail,
- ataki z wykorzystaniem wiadomości e-mail zdarzają się co 10 sekund,
- 71% wszystkich cyberataków jest motywowanych finansowo (po których następuje kradzież własności intelektualnej, a później szpiegostwo on-line),
- szacuje się, że roczny globalny koszt cyberprzestępczości wyniesie 10,5 biliona $ do 2025 r.[13].

[13] https://www.websiterating.com/pl/research/cybersecurity-statistics-facts/ (10.12.2021)

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

3. Regulacje prawne i najczęściej popełniane przestępstwa

Wraz z rozpowszechnianiem się komputerów i rosnącej ilości zagrożeń bezpieczeństwa oraz nadużyć przy wykorzystaniu komputerów lub infrastruktury teleinformatycznej pojawiła się potrzeba stworzenia jasnej definicji przestępstw komputerowych utożsamianych z cyberprzestępczością. W większości przypadków, poza atakami wymierzonymi w funkcjonowanie systemów teleinformatycznych, cyberprzestrzeń nie tworzy nowego rodzaju przestępstw, tylko dostarcza nowych narzędzi informatycznych lub metod do prowadzenia przestępczej działalności, a także stanowi nową przestrzeń, w której taka działalność jest prowadzona.

Szeroko ujęte zachowania kryminalne w cyberprzestrzeni – cyberprzestępstwo – można zdefiniować jako każde nielegalne działanie realizowane przy pomocy urządzeń działających w sieci, które jest wymierzone przeciw bezpieczeństwu samego systemu komputerowego lub przeciwko danym przetwarzanym za jego pomocą. Przestępstwem komputerowym będą zatem wszelkie włamania do systemu komputerowego, nieuprawnione pozyskiwanie informacji, sparaliżowanie pracy systemu (sabotaż) oraz piractwo komputerowe czy kradzież oprogramowania. Działania te zazwyczaj są przeprowadzane przy użyciu komputera lub sieci telekomunikacyjnej.

W polskim ustawodawstwie nie znajdziemy jednolitej definicji dla cyberprzestępstwa. W kodeksie karnym jest mowa o przestępstwach komputerowych. W rozdziale XVII odnoszącym się do przestępstw przeciwko Rzeczypospolitej Polskiej w art. 130 § 3 czytamy: *„Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2[14], gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8*."[15] Rozdział XX traktujący o przestępstwach przeciwko bezpieczeństwu powszechnemu przewiduje w art. 165 karę pozbawienia wolności od 6 miesięcy do lat 8 dla każdego „*kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach zakłócając, uniemożliwiając lub w inny*

[14] Mowa tu o informacjach których przekazanie może spowodować wyrządzenie szkody RP.
[15] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych"[16].

Kolejne przepisy odnoszące się do przestępstw komputerowych to rozdział XXXIII typizujący przestępstwa przeciwko ochronie informacji. W art. 267 § 1 stanowi: „*kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*"[17]. Taka sama kara jest przewidziana za bezprawne uzyskanie dostępu do systemu informatycznego oraz korzystanie z urządzeń lub oprogramowania podsłuchowego w celu uzyskania informacji do których użytkownik nie jest uprawniony. Natomiast art. 268 i 268a k.k. zakłada karę w wysokości do 5 lat pozbawienia wolności dla każdego kto „*nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią*"[18] oraz „*niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych*"[19].

Ponadto kodeks karny typizuje czyny zabronione związane z przestępstwami komputerowymi w art. 269, 269a i 269b k.k. Karze podlega kto: „*niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego (...) albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych*"[20], a także kto „*przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej*"[21]. Niedozwolone jest również wytwarzanie, udostępnianie i korzystanie z programów komputerowych które

[16] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.
[17] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.
[18] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.
[19] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.
[20] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.
[21] Kodeks karny Dz. U. 1997 nr 88 poz. 553 z późn. zm.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

umożliwiają popełnienie przestępstwa lub umożliwiają nieuprawniony dostęp do informacji (np. przekazywanie haseł czy kodów dostępu).

W przypadku przestępstw przeciwko mieniu wymienionych w rozdziale XXXV kodeksu karnego kary przewidziane są dla sprawców, którzy: „*bez zgody osoby uprawnionej uzyskują cudzy program komputerowy w celu osiągnięcia korzyści majątkowej*”[22], „*w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływają na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmieniają, usuwają albo wprowadzają nowy zapis danych informatycznych*”[23].

[22] Tamże, art. 278.
[23] Tamże, art. 287.

Bezgraniczne Bezpieczeństwo

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

4. Grupy potencjalnych ofiar, obszary zagrożeń

Biorąc pod uwagę regulacje prawne wśród przestępstw komputerowych możemy wyróżnić następujące obszary i typy cyberprzestępstw:

1. przestępstwa komputerowe przeciw Rzeczypospolitej Polskiej:
    a) szpiegostwo i wywiad komputerowy;
2. przestępstwa przeciwko bezpieczeństwu powszechnemu:
    a) sprowadzenie niebezpieczeństwa dla życia zdrowia lub mienia wielu osób,
    b) zakłócanie przetwarzania, gromadzenia, przesyłania informacji;
3. przestępstwa przeciw wiarygodności dokumentów:
    a) fałszerstwo komputerowe;
4. przestępstwa komputerowe przeciw ochronie informacji:
    a) nieuprawnione wejście do systemu, naruszenie zabezpieczeń, manipulacja w systemie,
    b) podsłuch komputerowy,
    c) bezprawne niszczenie informacji,
    d) sabotaż;
5. przestępstwa komputerowe przeciwko mieniu:
    a) nielegalne uzyskanie programu komputerowego,
    b) paserstwo,
    c) oszustwo komputerowe i telekomunikacyjne.

Przedstawiony katalog przestępstw nie jest katalogiem zamkniętym. Odwołując się do innych obowiązujących w Polsce przepisów należy pamiętać o pozostałych rodzajach przestępstw takich jak nielegalne kopiowanie i rozpowszechnianie prawem chronionego programu komputerowego, czy upowszechnianie treści pornograficznych, informacji pochwalających przemoc, rasizm, uporczywe nękanie, dyskredytowanie, czy też podszywanie się pod osoby trzecie – kradzież tożsamości. Wszystkie wymienione zachowania mogą nosić znamiona przestępstwa komputerowego jeśli są popełniane w cyberprzestrzeni.

Ważnym obszarem zagrożeń związanych bezpośrednio z Internetem jest cyberterroryzm. Rozwój technologiczny oraz rosnące znaczenie cyberprzestrzeni dostarczają terrorystom nie tylko nowych możliwości i technik dokonywania ataków, ale również tworzą nowy obszar dla ich działalności. Cyberterroryzm jest zatem połączeniem cyberprzestrzeni

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

i terroryzmu, czyli wykorzystywaniem zdobyczy technologicznych do przeprowadzania aktów terroru. Odnosi się on do bezprawnych gróźb i ataków na komputery, sieci i informacje w nich przechowywane, inicjowanych w celu zastraszania lub zmuszania rządu lub jego obywateli do realizacji określonych celów politycznych, ideologicznych, religijnych lub społecznych.

Terroryzm w cyberprzestrzeni polega na: „celowym zakłóceniu interaktywnego, zorganizowanego obiegu informacji w cyberprzestrzeni. Cyberterroryzm może mieć również na celu zdezorganizowanie, lub zdezorientowanie pracy wybranych obiektów, systemów czy służb, chociażby w celu zwiększenia skuteczności planowanych zamachów terrorystycznych innymi metodami."[24] Zazwyczaj głównym obiektem zainteresowania cyberterrorystów staje się infrastruktura krytyczna dla gospodarki oraz obronności atakowanego podmiotu i najczęściej w nią są wymierzone ataki. Dobrym przykładem typowego celu ataku może być system kontroli lotów, elektrownie, infrastruktura bankowa, a także systemy zapewniające dostarczanie wody czy systemy wykorzystywane w służbie zdrowia.

W cyberprzestrzeni możemy też spotkać się z tzw. haktywizmem i innymi formami aktywizmu internetowego. Haktywizm („hacktivism") jako termin powstał z potrzeby opisania zachowań będących połączeniem hakowania i aktywności politycznej. Haktywiści wykorzystują techniki komputerowe aby zwrócić uwagę społeczeństwa, jak również decydentów, na aktualne problemy. Ataki są przeprowadzane tak, aby promowały postulaty, programy polityczne, czy też adresowały potrzebę zmiany społecznej. Aktywność haktywistów jest najczęściej związana z wolnością słowa, prawami człowieka oraz swobodą przepływu i dostępu do informacji. Do najbardziej znanych przedstawicieli haktywistów możemy zaliczyć ruch Anonymous oraz WikiLeaks[25].

Początki ruchu Anonymous to 2003 rok i pojawienie się portalu umożliwiającego publikowanie kontrowersyjnych treści, które to były komentowane i oceniane przez użytkowników, którzy nie oznaczali swojej tożsamości pozostając anonimowymi („anonymous"). Początkowo angażowanie się w tematy polityczne nie było założeniem tego ruchu. Dopiero w 2008 roku Anonymous nabrał charakteru ruchu haktywistycznego, kiedy to uruchomił kampanię skierowaną przeciwko scjentologom[26]. W 2012 roku Anonymous

[24] https://www.omegasoft.pl/blog/jak-wyglada-cyberterroryzm/ (12.12.2021)
[25] https://pl.wikipedia.org/wiki/Haktywizm (12.12.2021)
[26] Projekt Chanology był odpowiedzią na publikowanie w sieci przez scjentologów nieprawdziwe treści oraz podejrzenie kontrolowania przez scjentologów publicznych wypowiedzi jej członków. Projekt ten wyznaczył

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

przeprowadziło ataki na korporacyjne i rządowe strony USA, Irlandii, Francji, Słowenii oraz Polski, które miały na celu zwrócić uwagę opinii publicznej na treść ACTA[27]. Dziś Anonymous jako ruch haktywistyczny jest zaliczany do grona najbardziej wpływowych organizacji na świecie. Z upływem lat stał się globalną, niescentralizowaną społecznością aktywistów, która sprzeciwia się ograniczaniu wolności obywatelskich, cenzurze, korupcji, wpływowi religii na życie oraz łamaniu praw zwierząt.

Równie ważnym przykładem haktywisty jest Julian Assange stojący za serwisem WikiLeaks. Witryna ta od wielu lat jest wykorzystywana do anonimowego publikowania często tajnych dokumentów rządowych lub korporacyjnych. Upublicznianie informacji ma zasygnalizować i zwrócić uwagę opinii publicznej na działania niezgodne z prawem. Za cel WikiLeaks stawia sobie zapewnienie wszystkim dostępu do informacji oraz zapewnienie bezpieczeństwa i uchronienie przed potencjalnymi represjami informatorów publikujących materiały.

Działania haktywistów mogą być zatem konstruktywną formą anarchistycznego nieposłuszeństwa obywatelskiego, politycznie umotywowanym hackerstwem albo gestem skierowanym przeciwko systemowi. Mogą wyrażać protest antykapitalistyczny, polityczny lub być głosem zwolenników otwartego oprogramowania. Haktywizm wzbudza wiele kontrowersji ponieważ niezwykle trudno jest określić granice między aktywnością polityczną i ruchem zaangażowanym społecznie a cyberprzestępstwem, które jest w tym działaniu narzędziem służącym do ekspresji postulatów. W tym aspekcie haktywizm nigdy nie będzie pozbawiony pierwiastka destrukcyjności i w efekcie będzie podawał w wątpliwości bezpieczeństwo Internetu jako platformy wymiany informacji.

Cyberbezpieczeństwo w sposób oczywisty jest problemem technicznym, ale także i politycznym. „Obejmuje zagadnienia technologii, badań, polityki i także spraw międzynarodowych, dyplomacji i wojska”[28]. Dlatego też strategie dotyczące cyberbezpieczeństwa powinny być wielowymiarowe. Dziś takie strategiczne podejście względem bezpieczeństwa przestrzeni cybernetycznej staje się w wielu państwach standardem.

---

pryncypia działania i wartości, na rzecz których Anonymous podejmował aktywność, czyli wolność wypowiedzi i prawo dostępu do informacji.

[27] Anti-Counterfeiting Trade Agreement – umowa handlowa walcząca z piractwem oraz chroniąca własność intelektualną budząca kontrowersje ze względu na możliwość blokowania treści, cenzurę oraz możliwość monitorowania użytkowników i udostępniania ich danych identyfikacyjnych.

[28] https://prywatnik.pl/2018/09/07/najwiekszy-cyberatak-w-historii-polski-bez-odpowiedzi-o-strategii-cyberbezpieczenstwa/ (06.12.2021)

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

5. Działania profilaktyczne i wsparcie

Najważniejsze polskie regulacje prawne dotyczące cyberbezpieczeństwa to:

- Polityka Ochrony Cyberprzestrzeni RP,
- Doktryna Cyberbezpieczeństwa RP,
- Założenia Strategii Cyberbezpieczeństwa RP,
- Dyrektywa NIS,
- Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022,
- Plan działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022,
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa,
- Rozporządzenie ws. wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych,
- Rozporządzenie ws. progów uznania incydentu za poważny,
- Strategia Cyberbezpieczeństwa RP na lata 2019-2024.

Pierwszym w Polsce strategicznym dokumentem dotyczącym cyberbezpieczeństwa była Polityka Ochrony Cyberprzestrzeni RP wydana w 2013 roku dzięki współpracy Ministerstwa Administracji i Cyfryzacji oraz Agencji Bezpieczeństwa Wewnętrznego. Strategicznym celem Polityki było „osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa. Osiągnięcie celu strategicznego jest realizowane poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami CRP[29]"[30]. W dokumencie wskazywano również cele szczegółowe odnoszące się do zwiększenia poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa, podniesienia zdolności zapobiegania i zwalczania cyberzagrożeń, a tym samym zmniejszenia skutków incydentów. Ponadto, określono kompetencje podmiotów oraz stworzenie spójnego systemu zarządzania bezpieczeństwem CRP, jak również trwałego systemu pozwalającego na koordynację i wymianę informacji pomiędzy podmiotami odpowiedzialnymi a użytkownikami. Podkreślono także wagę zwiększenia świadomości

[29] CRP – cyberprzestrzeń Rzeczypospolitej Polskiej.
[30] BBN, Polityka Ochrony Cyberprzestrzeni RP, 2013, s. 7 i nast.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

użytkowników dotyczącą dostępnych metod i środków zabezpieczeń stosowanych w cyberprzestrzeni. Polityka ustanowiła trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe zakładający koordynację (właściwy minister), reagowanie na incydenty (CERT.GOV.PL[31] oraz Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych dla zadań sfery militarnej) oraz realizację (administratorzy). Znajdujące się w niej zapisy obowiązywały wyłącznie administrację rządową z pominięciem niejawnych systemów teleinformatycznych.

Na początku 2015 roku Biuro Bezpieczeństwa Narodowego przygotowało Doktrynę Cyberbezpieczeństwa RP. Był to dokument koncepcyjny, bez mocy prawnej, którego celem było zapewnienie bezpiecznego funkcjonowania RP w cyberprzestrzeni poprzez skoordynowane w skali państwa działania. Doktryna postulowała wprowadzenie odpowiednich rozwiązań formalno-prawnych, utworzenie mechanizmów współpracy między sektorem publicznym i prywatnym, a także doradzała inwestowanie w narodowe rozwiązania oraz wykorzystanie potencjału obywateli na rzecz ochrony państwa w cyberprzestrzeni.

Politykę Ochrony Cyberprzestrzeni RP zastąpiły w 2017 roku Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022. Dokument miał charakter interdyscyplinarny i przekrojowy dzięki zaangażowaniu w jego tworzenie ekspertów z sektorów cyfryzacji, spraw wewnętrznych i administracji, obrony narodowej, Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa, a także Biura Bezpieczeństwa Narodowego. Celem tego dokumentu było zapewnienie wysokiego poziomu bezpieczeństwa zarówno w sektorze prywatnym jak i publicznym oraz wśród użytkowników cyberprzestrzeni. Krajowe Ramy były zabiorem ogólnych celów i wytycznych, które mają za cel zbudować odporność Polski na ataki i zagrożenia cybernetyczne. Poprzez wzmocnienie synergii działań wewnętrznych i międzynarodowych cyberprzestrzeń ma stać się bezpiecznym środowiskiem, w którym można realizować funkcje państwa oraz w pełni wykorzystywać jej potencjał gospodarczy jednocześnie szanując prawa i wolności obywateli. Cele które stawiają Ramy to „osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów

[31] CERT.GOV.PL – (ang. Computer Emergency Response Team) Rządowy Zespołu Reagowania na Incydenty Komputerowe działający w ramach ABW. Odpowiada on za koordynację procesu reagowania na incydenty komputerowe w cyberprzestrzeni. Jednym z jego podstawowych zadań jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

teleinformatycznych istotnych dla funkcjonowania państwa. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa cyberprzestrzeni. Zbudowanie silnej pozycji międzynarodowej RP obszarze cyberbezpieczeństwa."[32] W dokumencie tym położono duży nacisk na potrzebę rozbudowy i udoskonalenia struktury krajowego systemu cyberbezpieczeństwa, ochronę infrastruktury krytycznej, walkę z cyberprzestępczością i cyberterroryzmem oraz zbudowanie zdolności do działań militarnych w cyberprzestrzeni. Nawiązując do Krajowych Ram w 2018 roku przedstawiono dokument planistyczny jakim jest Plan działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022. Miał on formę wykazu przedsięwzięć, których realizacja miała umożliwić osiągnięcie celów założonych w uchwalonym dokumencie.

Parlament Europejski w lipcu 2016 roku przyjął Dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, skrótowo nazywaną Dyrektywą NIS (Network and Information Systems Directive). Jest to pierwszy dokument w dziedzinie cyberbezpieczeństwa obejmujący swoim zasięgiem całą Unię Europejską. Celem Dyrektywy jest wprowadzenie równego poziomu zabezpieczeń dla systemów w cyberprzestrzeni unijnej. Ma ona poprawić zdolności poszczególnych krajów członkowskich w obszarze cyberbezpieczeństwa oraz zoptymalizować współpracę międzynarodową i ujednolicić sposób zgłaszania incydentów bezpieczeństwa przez operatorów i dostawców usług kluczowych. Dyrektywa zobowiązuje również do utworzenia Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT[33]). Ponadto wskazuje na ENISA, która ma pełnić rolę kluczową we wdrażaniu Dyrektywy oraz koordynowaniu współpracy międzypaństwowej w ramach sieci CSIRT[34]. Dokument ten nakładał obowiązek dostosowania prawa krajowego i wdrożenia zaleceń w krajach członkowskich do połowy 2018 roku.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) z 2018 roku jest aktem prawnym, który ma implementować wytyczne Dyrektywy NIS w Polsce. Zarazem jest to

[32] Ministerstwo Cyfryzacji, Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022, s. 8 i nast.
[33] CSIRT – Computer Security Incident Response Team.
[34] Sieć CSIRT – Mechanizm powołany na podstawie art. 12 Dyrektywy NIS. W skład sieci wchodzą poszczególne CSIRTy krajowe oraz CERT-EU i Komisja Europejska. Polska jest reprezentowana przez CERT Polska działający w ramach NASK. Zadania sieci to wymiana informacji na temat incydentów, wsparcie w obsłudze incydentów transgranicznych, omawianie wniosków z ćwiczeń etc. Sieć ma umożliwić zbudowanie szybkiej i skutecznej współpracy między państwami członkowskimi.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

historycznie pierwszy w Polsce akt prawny w tym obszarze. Jej celem jest nie tylko wdrożenie NIS, ale również powołanie do życia sprawnie funkcjonującego systemu bezpieczeństwa teleinformatycznego o krajowym zasięgu.

Ustawa odnosi się do trzech typów podmiotów: operatorów usług kluczowych, dostawców usług cyfrowych, a także podmiotów publicznych. W rozumieniu ustawy operatorem usług kluczowych są „firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej, zależne od systemów informatycznych”[35]. Operatorzy mają zostać zidentyfikowani w obszarze energetycznym, transportowym, bankowym i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i infrastruktury cyfrowej. Dostawcą usług jest natomiast jednostka świadcząca usługę cyfrową, którą może być internetowa platforma handlowa, usługi przetwarzania w chmurze lub wyszukiwarka internetowa. Wobec tych podmiotów Ustawa o KSC wprowadza szereg obowiązków mających na celu ogólną poprawę kondycji bezpieczeństwa (jak wdrożenie systemu zarzadzania bezpieczeństwem, ryzykiem, audyt etc.) a jednym z nich jest konieczność raportowania incydentów bezpieczeństwa.

Podmioty są zobowiązane raportować incydenty do trzech wyznaczonych w Ustawie zespołów CSIRT na poziomie krajowym z jasno określonym podziałem kompetencji. CSIRT MON prowadzony przez Ministra Obrony Narodowej koordynuje incydenty zgłaszane przez podmioty mu podległe oraz przedsiębiorstwa o szczególnym znaczeniu dla gospodarki i obronności. CSIRT GOV działający w strukturach Agencji Bezpieczeństwa Wewnętrznego ma zajmować się incydentami spływającymi od administracji rządowej oraz operatorów infrastruktury krytycznej. Natomiast CSIRT NASK w strukturach Państwowego Instytutu Badawczego NASK koordynuje incydenty zgłaszane przez pozostałe podmioty, a także jest miejscem do którego mogą się zwracać zwykli użytkownicy cyberprzestrzeni. Wszelkie incydenty mające charakter terrorystyczny natomiast powinny być zgłaszane do CSIRT MON lub CSIRT GOV. Zadania wszystkich krajowych zespołów CSIRT to:

1. monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym,
2. szacowanie ryzyka w skali całego kraju,

[35] NASK, Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje. Cyberbezpieczeństwo w perspektywie policy, 2020, s. 5 i nast.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

3. przekazywanie informacji na temat incydentów i ryzyka do innych podmiotów krajowego systemu cyberbezpieczeństwa,
4. wydawanie komunikatów na temat zidentyfikowanych zagrożeń,
5. reagowanie na zgłaszane incydenty,
6. prowadzenie analizy zagrożeń i podatności,
7. opracowywanie narzędzi wykrywania oraz zwalczania zagrożeń.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa wprowadza również jasną klasyfikację dla poziomów incydentów. Poziom pierwszy obejmuje wszystkie zdarzenia które wpływają niekorzystnie na cyberbezpieczeństwo. Drugi poziom jest poświęcony incydentom poważnym i istotnym występującym odpowiednio u operatorów usług kluczowych i dostawców usług cyfrowych, a także incydentom w podmiocie publicznym. Na trzecim poziomie umiejscowiono incydenty krytyczne, czyli o dużej skali, najczęściej wiążące się z większym zagrożeniem niż te wcześniej wymienione. Zaprojektowano też mechanizm współpracy wszystkich krajowych CSIRT na okoliczność wystąpienia incydentów krytycznych. „Ustawa wprowadza formułę Zespołu ds. Incydentów Krytycznych, będącego organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą CSIRT poziomu krajowego oraz Rządowe Centrum Bezpieczeństwa jako sekretariat – taka formuła zapewnia współpracę z Rządowym Zespołem Zarządzania Kryzysowego (RZZK).”[36]

Ustawa przewiduje także powołanie zespołów cyberbezpieczeństwa wyspecjalizowanych w konkretnych sektorach. Zaletą takiego podejścia jest możliwość uwzględnienia specyfiki danego sektora, a tym samym dostosowania wsparcie do potrzeb operatorów usług kluczowych. Zespół oprócz przyjmowania i analizy incydentów, wspiera ich obsługę formułuje wnioski oraz współpracuje z właściwym CSRIT. Ma on również możliwość wymiany komunikacji o incydentach poważnych z pozostałymi krajami Unii Europejskiej.

Wprowadzono również regulacje nakładające obowiązek przygotowania i przyjęcia pięcioletniej Strategii Cyberbezpieczeństwa RP. Dodatkowo powołano Pełnomocnika i Kolegium ds. Cyberbezpieczeństwa których zadaniem ma być koordynacja strategiczno-polityczna systemu cyberbezpieczeństwa w skali ogólnopolskiej.

[36] NASK, Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje. Cyberbezpieczeństwo w perspektywie policy, 2020, s. 10

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

Ustawa o KSC wraz z rozporządzeniami Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz w sprawie progów uznania incydentu za poważny stanową dowód na zakończenie pełnego wdrożenia Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii w Polsce.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

Bezgraniczne Bezpieczeństwo

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

6. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

Dyrektywa NIS zobowiązywała kraje członkowskie również do sformułowania i wdrożenia krajowych strategii bezpieczeństwa sieci i informacji. Obecnie obowiązująca Strategia Cyberbezpieczeństwa RP na lata 2019-2024 jest dokumentem wypełniającym te zalecenia. Strategia zastąpiła obowiązujące dotychczas Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022. Strategia została przyjęta aby realizować główny cel określony jako „podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji”[37]. Strategia definiuje również pięć celów szczegółowych oraz określa dla nich konkretne działania[38]:

1. Rozwój krajowego systemu cyberbezpieczeństwa:
    a) wdrożenie i ewaluacja stosownych przepisów,
    b) rozbudowa systemu wymiany informacji odpornego na zagrożenia,
    c) zwiększenie bezpieczeństwa usług kluczowych, cyfrowych i infrastruktury krytycznej poprzez wdrożenie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Cyberprzestrzeni RP,
    d) opracowanie i implementacja metodyki szacowania ryzyka na poziomie krajowym,
    e) zwiększenie zdolności zwalczania przestępczości, szpiegostwa i terroryzmu w cyberprzestrzeni.
2. Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty:
    a) opracowanie, wdrożenie Narodowych Standardów Cyberbezpieczeństwa i promocja dobrych praktyk i zaleceń (ukończono prace nad Standardami Cyberbezpieczeństwa Chmur Obliczeniowych),
    b) bezpieczeństwo łańcucha dostaw,

[37] M.P 2019 poz. 1037 punkt 4.2
[38] M.P 2019 poz. 1037 punkt od 5 do 9.2

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

c) okresowe audyty bezpieczeństwa.

3. Zwiększanie potencjału narodowego w zakresie cyberbezpieczeństwa:
   a) rozbudowa zasobów przemysłowych i technologicznych,
   b) rozwój współpracy sektora prywatnego i publicznego,
   c) stymulowanie badań i rozwoju,
   d) budowa kompetencji prowadzenia działań militarnych w cyberprzestrzeni.
4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa:
   a) zwiększanie kompetencji pracowników podmiotów istotnych dla cyberbezpieczeństwa RP (administracja rządowa, jednostki samorządu terytorialnego),
   b) stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni dla obywateli,
   c) budowanie świadomości społecznej w zakresie bezpiecznego korzystania z zasobów cyberprzestrzeni (dedykowane programy edukacyjne, kampanie na rzecz zwiększania świadomości).
5. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa:
   a) aktywna współpraca na poziomie strategiczno-politycznym, operacyjnym i technicznym.

Strategia Cyberbezpieczeństwa RP na lata 2019-2024 jest przykładem kompleksowego podejścia do kwestii bezpieczeństwa w cyberprzestrzeni. Kształtuje ona również ogólny poziom bezpieczeństwa narodowego wskazując konkretne zalecenia konieczne do realizacji w celu zapewnienia odporności na cyberzagrożenia dla systemów informacyjnych, operatorów usług kluczowych i infrastruktury krytycznej oraz administracji publicznej i obywateli.

W skład polskiego ekosystemu cyberbezpieczeństwa, obok aktów prawnych precyzujących zagadnienia i organizujących wymiar przestrzeni cybernetycznej, wchodzą projekty o charakterze krajowym. Wszystkie mają za cel zwiększenie krajowego bezpieczeństwa w cyberprzestrzeni.

Jedną z takich inicjatyw jest Rządowy Klaster Cyberbezpieczeństwa. Program ten ma zapewnić efektywny i bezpieczny dostęp do zasobów sieciowych systemom wykorzystywanym

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

w administracji publicznej oraz ich użytkownikom. Jednocześnie klaster ma zadbać o bezpieczeństwo i ciągłość komunikacji pomiędzy instytucjami państwowymi (także w wypadku ataku na dużą skalę) poprzez zapewnienie bezpiecznej poczty elektronicznej, dostępu do baz danych itp.

Na mocy Ustawy o KSC utworzono Narodową Platformę Cyberbezpieczeństwa, czyli system teleinformatyczny o charakterze platformy mającej zarządzać bezpieczeństwem cyberprzestrzeni RP i stanowić źródło informacji oraz ostrzeżeń o zagrożeniach. Jest systemem koordynowanym przez Centrum Cyberbezpieczeństwa NASK-PIB a uczestniczą w nim Politechnika Warszawska, Instytut Łączności, a także Narodowe Centrum Badań Jądrowych.

Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy NASK-PIB jest odpowiedzialna za realizację strategicznych inicjatyw wspierających instytucje publiczne. Przykładami takich projektów są ACADEMICA mająca na celu zastąpienie tradycyjnej formy wypożyczania w bibliotekach publikacjami cyfrowymi, projekt Safer Internet budujący świadomość społeczną w obszarze bezpiecznego korzystania z nowoczesnych technik komunikacji, jak również projekt SISSDEN oferujący usługi powiadamiania ofiar o atakach. Największym i najszerzej rozpoznawalnym projektem jest ARAKIS-GOV. Jest to dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Jego głównym zadaniem jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych przy wykorzystaniu agregacji, analizy i korelacji danych z różnych źródeł. ARAKIS-GOV składaj się trzech modułów. Moduł Reflector (REF) jest odpowiedzialny za obserwację ruchu sieciowego występującego. Generuje sygnatury podejrzanego ruchu sieciowego, automatycznie przesyłając je z sond zainstalowanych u uczestników Projektu do Centrum Systemu. Kolejny to moduł Forwarder (FWD) odbierający oraz interpretujący dane przesyłane przez źródła dodatkowe (np. oprogramowanie firewall, oprogramowanie antywirusowe serwera pocztowego, oprogramowanie serwera WWW) oraz przesyłający je do Centrum Systemu. Trzeci z modułów to APTDetect Sensor (APTDetect) odpowiedzialny za monitoring produkcyjnego ruchu sieciowego generowanego przez Uczestnika oraz wykrywania niepożądanego ruchu w oparciu o analizę protokołów warstwy aplikacyjnej. Warto podkreślić, że przyłączenie się do ARAKIS-GOV jest bezpłatne, system nie monitoruje treści przekazywanych przez chronioną instytucję, obecnie jego sensory działają w większości

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

urzędów państwowych oraz jest projektem realizowanym we współpracy z Agencją Bezpieczeństwa Wewnętrznego.

Aby móc efektywniej wykrywać sprawców przestępstw komputerowych ramach struktury Komendy Głównej Policji w 2016 roku utworzone zostało Biuro do Walki z Cyberprzestępczością. Biuro prowadzi następujące działania: „nadzorowanie, koordynowanie i wspieranie ukierunkowanych na zwalczanie cyberprzestępczości działań prowadzonych przez komendy wojewódzkie (Stołeczną) Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałanie z Centralnym Biurem Śledczym Policji w tym zakresie; prowadzenie całodobowej służby mającej na celu koordynowanie działań Policji w zakresie zagrożeń przestępstwami w sieci Internet, ich zwalczania oraz współdziałania jednostek organizacyjnych Policji z krajowymi i zagranicznymi organami i podmiotami pozapolicyjnymi, prowadzenie konsultacji technicznych, inicjowanie i wspieranie badań oraz projektów, a także współpraca z podmiotami krajowymi i zagranicznymi zmierzająca do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z cyberprzestępczością”[39].

Polskie podmioty odpowiedzialne za realizację zadań mających na celu wzmocnienie cyberbezpieczeństwa aktywnie angażują się we współpracę międzynarodową. Świadczy to o transgranicznym i aterytorialnym wymiarze przestrzeni cybernetycznej, a tym samym o konieczności skoordynowania działań i wypracowania mechanizmów wczesnego ostrzegania o zagrożeniach pomiędzy poszczególnymi państwami.

Współpraca z Unią Europejską w zakresie poprawy stanu cyberbezpieczeństwa to jedno z podstawowych kompetencji Ministerstwa Cyfryzacji. Ministerstwo reprezentuje Polskę będąc członkiem wielu grup, które kooperując nadają ramy prawne i kształt unijnej cyberprzestrzeni. Realizując zalecenia Dyrektywy NIS Polska jako państwo członkowskie jest zobowiązana do działania w ramach sieci CSIRT oraz Grupy Współpracy (NIS Cooperation Group), która to tworzy niewiążące wytyczne, umożliwiające skuteczne i spójne wdrożenie dyrektywy w całej Unii Europejskiej.

W ramach Horyzontalnej Grupy Roboczej ds. Cyberbezpieczeństwa (Horizontal Working Party on Cyber Issues) Ministerstwo Cyfryzacji angażuje się w działania legislacyjne. Praca w ramach tej grupy ma na celu opracowanie jednolitego stanowiska państw UE będącego

[39] http://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html (12.12.2021)

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

odpowiedzią na wszelkie istotne zagadnienia jak na przykład wytyczenie wspólnej odpowiedzi na nielegalne działania w przestrzeni cybernetycznej.

Polska jest także jednym z założycieli Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO). „Współpraca w ramach ECSO przyczynia się do połączenia zbieżnych inicjatyw w dziedzinie cyberbezpieczeństwa z różnych krajów UE we wspólne przedsięwzięcia – ma to pozwolić na uzyskanie przewagi konkurencyjnej w stosunku do państw spoza UE. Ponadto w ramach strategii Jednolitego Rynku Cyfrowego Komisja pragnie wzmocnić współpracę transgraniczną między wszystkimi zainteresowanymi stronami i sektorami zajmującymi się cyberbezpieczeństwem, a także wspomóc rozwój innowacyjnych i bezpiecznych technologii, produktów i usług w całej UE."[40]

Wspólnie z państwami Grupy Wyszehradzkiej i Austrii w ramach Środkowoeuropejskiej Platformy Cyberbezpieczeństwa (CECSP) Polska dwukrotnie w roku omawia główne problemy polityczne i techniczne w cyberprzestrzeni.

Ponadto polskie reprezentacje wielokrotnie brały udział w międzynarodowych zawodach potwierdzających kompetencje ekspertów z dziedziny cyberbezpieczeństwa. Za przykład można podać ćwiczenia Cyber Europe organizowane przez ENISA oraz European Cyber Security Challenge. Polska bierze również udział w organizowanej od 2012 roku inicjatywie o nazwie Europejski Miesiąc Bezpieczeństwa Cybernetycznego mający promować cyberbezpieczeństwo oraz poprawiać świadomość o zagrożeniach występujących w Internecie.

Ministerstwo Obrony Narodowej również aktywnie przyczynia się również do zapewnienia cyberbezpieczeństwa Polski i jej obywateli powołując programu CYBER.MIL.PL. Dobrym przykładem realizacji założeń programu jest zacieśnianie współpracy z Sojuszem Północnoatlantyckim. W lipcu 2019 roku doszło do podpisania porozumienia dzięki któremu została nawiązana stała współpraca w obszarze cyberbezpieczeństwa. Umowa między NATO a Polską określa podstawy prawne do przeprowadzenia reakcji w przypadku cyberataku na nasz kraj. Zapowiada utworzenie „całodobowych punktów kontaktowych, które będą odpowiedzialne za prowadzenie bieżącej współpracy w kwestiach dotyczących zarówno polityki w dziedzinie cyberbezpieczeństwa, jak i technicznych aspektów zagrożeń występujących w cyberprzestrzeni"[41]. Porozumienie jest

[40] https://www.gov.pl/web/cyfryzacja/wspolpraca-miedzynarodowa1 (10.12.2021)
[41] https://www.gov.pl/web/obrona-narodowa/w-kierunku-bezpiecznej-cyberprzestrzeni (29.11.2021)

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima"* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO

także podstawą prawną do wykorzystania przez NATO Zespołów Szybkiego Reagowania (ang. Rapid Reaction Teams) w przypadku zidentyfikowania zagrożenia cybernetycznego. Dokument definiuje płaszczyznę współpracy, a także udzielania Polsce wsparcia. Zawarta umowa ma zapewnić Polsce możliwość współuczestniczenia w rozwijaniu systemów wczesnego ostrzegania o zagrożeniach w cyberprzestrzeni oraz doradztwo ekspertów NATO i współpracę z przemysłem zbrojeniowym w tym zakresie.

Warto tu również wspomnieć o udziale polskich zespołów w organizowanych od 2010 roku przez Sojusznicze Centrum Doskonalenia Obrony Cybernetycznej NATO (NATO Cooperative Cyber Defence Centre of Excellence) ćwiczeniach Locked Shields. Cieszą się one opinią największych, a zarazem najtrudniejszych technicznie międzynarodowych ćwiczeń obrony teleinformatycznej na świecie. „Głównym celem ćwiczeń było sprawdzenie w praktyce zdolności do prowadzenia kolektywnej obrony w cyberprzestrzeni, weryfikacja procedur, koordynacja działań w chwili wystąpienia cyberataku o charakterze globalnym, nawiązanie relacji i zacieśnienie współpracy między siłami zbrojnymi Sojuszu, instytucjami odpowiedzialnymi za infrastrukturę krytyczną oraz firmami i instytucjami z sektora prywatnego.”[42] Polski zespół, po raz pierwszy wspierany przez skład amerykański, w 2019 roku zajął szóste miejsce co jest ogromnym sukcesem[43].

[42] https://www.cyber.mil.pl/articles/aktualnosci-y/2019-04-15j-polscy-informatycy-w-gronie-najlepszych-na-locked-shields-2019/ (29.11.2021)

[43] W Locked Shields 2019 brały udział zespoły z 24 państw.

Projekt *Kampania edukacyjno-informacyjna „Ubi crimen, ibi victima”* jest współfinansowany przez Unię Europejską ze środków Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego.

UNIA EUROPEJSKA
FUNDUSZ BEZPIECZEŃSTWA WEWNĘTRZNEGO