MATERIAŁY DYDAKTYCZNE 116

Przyjęcie zawiadomienia o cyberprzestępstwie – wybrane zagadnienia

KATOWICE 2024

podkom. Barbara Baran
podkom. Natalia Karpuk
asp. Grzegorz Szokiel
Zakład Służby Kryminalnej

Przyjęcie zawiadomienia o cyberprzestępstwie – wybrane zagadnienia

Katowice 2024

Nadzór merytoryczny:
mł. insp. Violetta Grudzień

Redakcja, korekta, skład:
Paweł Mięsiak

© Szkoła Policji w Katowicach, Katowice 2024, pewne prawa zastrzeżone.

Niniejsza publikacja w całości stanowi materiał dydaktyczny Szkoły Policji w Katowicach. Publikacja dostępna jest na licencji:
Creative Commons – Uznanie autorstwa – Użycie niekomercyjne – Na tych samych warunkach (CC-BY-NC-SA) 4.0 Polska.

Postanowienia licencji są dostępne pod adresem:
https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pl

Spis treści

Wstęp

W dzisiejszym społeczeństwie, w którym każdy aspekt naszego życia jest coraz bardziej związany z technologią, bezpieczeństwo cybernetyczne staje się kluczowym wyzwaniem naszych czasów. Świat online nieustannie ewoluuje, oferując nieograniczone możliwości w zakresie komunikacji, pracy i rozwoju pod każdym względem, stawiając nas jednocześnie wobec nowych zagrożeń. Zrozumienie złożoności cyberprzestępczości staje się nieodzowne, aby skutecznie zauważyć moment ataku, ale i również przeciwdziałać atakom, które zagrażają naszej prywatności, finansom, a nawet bezpieczeństwu narodowemu.

Niniejsza publikacja to spojrzenie na cyberprzestępczość nie tylko, aby zgłębić jej mechanizmy i metody działania, ale także aby odkryć narzędzia i strategie konieczne do jej zwalczania.

Celem opracowania niniejszego skryptu jest przybliżenie funkcjonariuszom Policji zagadnienia przyjęcia zawiadomienia o popełnieniu cyberprzestępstwa, w szczególności tym, którzy nie posiadają jeszcze doświadczenia w tym zakresie. Mając na uwadze konieczność prawidłowego, merytorycznego wykonania pierwszej czynności procesowej jaką jest przyjęcie zawiadomienia o przestępstwie, mamy nadzieję, że publikacja przyczyni się do pogłębienia wiedzy dotyczącej wskazanej problematyki.

Rozdział 1.
Kontekst cyberprzestępczości

Cyberprzestępczość obejmuje szereg sytuacji związanych ze zjawiskami kryminalnymi w środowisku cyfrowym, w którym technologie informatyczne pełnią kluczową rolę. Główne cechy charakteryzujące cyberprzestępczość, które należy wymienić to:

Globalny charakter: cyberprzestępczość nie zna granic narodowych. Atakujący mogą działać z dowolnego miejsca na świecie, co sprawia, że dochodzi do globalnych zagrożeń dla bezpieczeństwa.

Szybki rozwój technologii: dynamiczny rozwój technologii informatycznych sprawia, że cyberprzestępcy mogą wykorzystywać najnowsze narzędzia i technologie, a także szybko adaptować się do środowiska online.

Internet jako platforma działania: Internet stanowi główną platformę dla działań cyberprzestępczych. Atakujący wykorzystują różnorodne usługi internetowe do przeprowadzania cyberataków, kradzieży danych czy manipulacji informacjami.

Cyberprzestępczość zorganizowana: cyberprzestępcy często działają w zorganizowanych grupach przestępczych o złożonych strukturach, które posługują się specjalistyczną wiedzą z zakresu cyberprzestępczości.

Handel danymi i informacjami: dane osobowe, finansowe oraz korporacyjne są cennym towarem na czarnym rynku. Kradzież i sprzedaż danych są powszechne wśród cyberprzestępców.

Zastosowanie technologii kryptograficznych: cyberprzestępcy często wykorzystują technologie kryptograficzne, zarówno do zabezpieczania swoich działań, jak i do szyfrowania danych wymaganych w przypadku ataków ransomware.

Aspekty ekonomiczne: cyberprzestępczość generuje ogromne straty ekonomiczne. Firmy i jednostki są narażone na utratę danych, finansowe konsekwencje ataków, a także koszty związane z ochroną przed cyberzagrożeniami.

Rola państwa i instytucji międzynarodowych: rządy i organizacje międzynarodowe podejmują wysiłki w celu opracowania regulacji oraz współpracy na arenie międzynarodowej w celu zwalczania cyberprzestępczości.

Przestępczość hybrydowa: cyberprzestępczość często łączy się z innymi formami przestępczości, tworząc tzw. przestępczość hybrydową. Przykładem są m.in. ataki hakerskie, które mogą być wykorzystywane do wsparcia działań terrorystycznych czy szpiegowskich.

Wyzwania dla bezpieczeństwa narodowego: cyberprzestępczość stanowi poważne wyzwanie dla bezpieczeństwa narodowego, w tym dla instytucji rządowych, przedsiębiorstw krytycznej infrastruktury, a także dla sektora obronnego.

Zagrożenia dla jednostek: indywidualni użytkownicy są narażeni na różne formy cyberzagrożeń, takie jak kradzież tożsamości, ataki phishingowe czy szkodliwe oprogramowanie.

Ochrona danych osobowych: w kontekście rosnącej liczby regulacji dotyczących ochrony danych osobowych cyberprzestępcy często celują w bazy danych, co podkreśla znaczenie odpowiednich środków ochronnych.

Zrozumienie powyższego kontekstu jest kluczowe dla skutecznej walki z cyberprzestępczością i opracowania odpowiednich strategii bezpieczeństwa. Wymaga to ciągłego dostosowywania się do zmieniającego się krajobrazu cyberbezpieczeństwa.

Rozdział 2.
Definicja cyberprzestępczości

Kiedy staniemy przed koniecznością określenia znamion przestępstwa związanego z technologią informatyczną, z pewnością każdy bez większych problemów będzie mógł samodzielnie określić, czym dla niego jest zjawisko cyberprzestępstwa. Jednakże w sytuacji, kiedy definicja ta musi być fundamentem jednobrzmiącego określenia, aby nie budzić wątpliwości co do interpretacji w środowisku prawniczym, zaczyna pojawiać się problem, bowiem na ostateczne jej brzmienie będzie miało wpływ środowisko cyfrowe oraz technologie internetowe, które rozwijają się bardzo szybko.

Nowe technologie i narzędzia pojawiają się znacznie szybciej niż regulacje prawne. To sprawia, że niektóre działania, które mogą być uznawane za cyberprzestępczość, nie zostały jeszcze formalnie zakwalifikowane jako przestępstwa, a tym samym stanowi to trudność w doprecyzowaniu definicji. Powyższy problem jest dość powszechnie zauważalny, bowiem polskie prawodawstwo do dzisiaj nie stworzyło jednolitej definicji cyberprzestępczości na gruncie Kodeksu karnego. Funkcjonuje natomiast wiele doraźnych. W znaczeniu najprostszym są to przestępstwa popełniane za pomocą komputerów oraz Internetu. Innym źródłem definicji, z którego można korzystać, mogą być międzynarodowe podmioty, takie jak Organizacja Narodów Zjednoczonych, Unia Europejska czy Interpol. Jednakże i te definicje opracowane zostały na własne potrzeby wymienionych instytucji.

Bez względu na to jaką definicję cyberprzestępczości przyjmiemy, zawsze będą to czyny zabronione skierowane przeciwko systemom informatycznym, w których komputer jest celem samym w sobie oraz czyny dokonane z użyciem komputera, w których stanowi on jedynie narzędzie[1].

Definicja Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

Jedna z najstarszych prób podjęcia rozwiązania problemu zdefiniowania cyberprzestępstwa znajduje się w dziś już nieobowiązującym akcie prawnym – uchwale nr 111/2013 Rady Ministrów z dnia 25 czerwca 2013 r. Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Na mocy tego dokumentu cyberprzestępstwo stanowi czyn zabroniony popełniony w obszarze cyberprzestrzeni, czyli przestrzeni

[1] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik policyjny nr 4/2017 https://kwartalnik.csp.edu.pl/kp/archiwum-1/2017/nr-42017/3730,Cyberprzestepczosc-proba-diagnozy-zjawiska.html). 2017 r. dostęp 21.04.2024 r.

przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

Definicja cyberprzestępczości według Interpolu

Definicja sformułowana przez Interpol jest bardzo praktyczna i określa cyberprzestępczość w dwóch ujęciach – tzw. wertykalnym oraz horyzontalnym. Ujęcie wertykalne dotyczy przestępstw specyficznych dla cyberprzestrzeni, czyli takich, które tylko tam mogą być dokonane, np. hacking czy sabotaż komputerowy. Z kolei ujęcie horyzontalne zakłada popełnianie przestępstw za pomocą technik komputerowych (np. oszustwa komputerowe, fałszowanie pieniędzy, pranie brudnych pieniędzy itp.)[3].

W kontekście działań Unii Europejskiej

Komisja Wspólnot Europejskich używa pojęcia „cybercrime" (cyberprzestępczość), definiując je jako czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom. Cyberprzestępstwa są podzielone na trzy kategorie obejmujące tradycyjne formy przestępstw z użyciem elektronicznych sieci informatycznych, publikację nielegalnych treści w mediach elektronicznych oraz przestępstwa specyficzne dla sieci łączności elektronicznej, takie jak ataki na systemy informatyczne i sabotaż komputerowy. Konwencja Rady Europy o cyberprzestępczości wprowadza podział cyberprzestępstw na kategorie obejmujące przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów, przestępstwa komputerowe, przestępstwa ze względu na charakter zawartych informacji oraz przestępstwa związane z naruszeniem praw autorskich i pokrewnych[4].

[2] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

[3] M. Stefanowicz, dz.cyt.

[4] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.

Rozdział 3.
Typy cyberprzestępstw i charakterystyka działań przestępczych w środowisku cyfrowym

Cyberprzestępczość obejmuje szereg różnorodnych form przestępstw, takich jak ataki hakerskie, kradzież danych, oszustwa internetowe, ataki ransomware, hakerstwo społecznościowe i wiele innych. Cyberprzestępczość nie zna granic narodowych. Atakujący mogą działać z dowolnego miejsca na świecie, co sprawia, że dochodzi do globalnych zagrożeń dla bezpieczeństwa. Motywy cyberprzestępców mogą być różnorodne, obejmując korzyści finansowe, szpiegostwo przemysłowe, działania terrorystyczne, zemstę, sabotowanie konkurencji czy po prostu chęć sprawdzenia swoich umiejętności.

Zjawisko obejmuje różnorodne formy, ponieważ wykorzystuje technologie informatyczne i sieciowe do popełniania działań przestępczych. W raporcie ENISA – Agencji Unii Europejskiej ds. Cyberbezpieczeństwa przedstawiono kilka głównych typów cyberprzestępstw i są to przede wszystkim:

Ataki hakerskie:

Ataki DDoS (*denial of service*): próba przeciążenia systemu lub sieci, aby uniemożliwić dostęp do usług.

Ataki *brute force*: próba złamania zabezpieczeń systemu poprzez wielokrotne próby odgadnięcia hasła.

Ataki *zero-day*: wykorzystanie luk w zabezpieczeniach systemów, które nie są jeszcze znane dostawcy usług czy producentowi oprogramowania.

Phishing i spoofing:

Phishing: oszustwa polegające na podszywaniu się pod zaufane źródło w celu zdobycia poufnych informacji, takich jak hasła czy dane finansowe.

Spoofing: fałszowanie informacji, aby sprawiać wrażenie, że komunikaty czy wiadomości pochodzą od wiarygodnego źródła.

Kradzież tożsamości:

Pharming: przekierowywanie użytkowników na fałszywe strony internetowe w celu pozyskania poufnych informacji.

Skimming: kradzież danych z kart kredytowych lub debetowych, najczęściej przy wykorzystaniu terminalach płatniczych.

Malware (złośliwe oprogramowanie):

Wirusy: programy, które rozprzestrzeniają się i infekują pliki na komputerze.

Trojany: oprogramowanie, które podszywa się pod legalne aplikacje, aby ukryć złośliwe funkcje.

Ransomware: programy szantażujące, które blokują dostęp do danych lub systemu, żądając okupu za ich odblokowanie.

Oszustwa finansowe:

Oszustwa kart kredytowych: nielegalne uzyskiwanie danych kart kredytowych i ich wykorzystywanie do nieautoryzowanych transakcji.

Wyłudzenia finansowe online: różnego rodzaju oszustwa polegające na uzyskiwaniu nielegalnych korzyści finansowych, na przykład przez fałszywe aukcje online czy inwestycje.

Włamania do systemów:

Włamania do systemów komputerowych: nielegalne uzyskiwanie dostępu do systemów komputerowych w celu kradzieży danych czy szkodzenia infrastrukturze.

Ataki na aplikacje webowe: włamania i ataki na aplikacje internetowe w celu uzyskania dostępu do danych lub naruszenia bezpieczeństwa.

Hakerstwo społecznościowe:

Inżynieria społeczna: manipulowanie ludźmi w celu uzyskania poufnych informacji, często poprzez wykorzystanie psychologii i socjotechniki.

Ataki BEC (*business email compromise*): oszustwa, w których atakujący podszywają się pod pracownika firmy w celu wyłudzenia środków finansowych.

Przemoc online i cyberprzemoc:

Nękanie i przemoc online: wykorzystywanie Internetu do nękania, szkalowania czy szantażowania innych osób.

Sextortion: szantażowanie ofiar za pomocą materiałów seksualnych uzyskanych drogą elektroniczną.

Włamania do sieci IoT (*Internet of things*): ataki na urządzenia podłączone do Internetu, takie jak kamery, urządzenia domowe czy urządzenia medyczne.

Handel ciemnymi rynkami: sprzedaż i kupno nielegalnych towarów, usług czy danych na tzw. ciemnych rynkach w sieci (Darknet)[5].

Zrozumienie różnych typów cyberprzestępstw jest kluczowe dla skutecznej ochrony przed nimi oraz ścigania sprawców. Przedsiębiorstwa, instytucje, a także indywidualni użytkownicy muszą być świadomi potencjalnych zagrożeń i stosować odpowiednie środki bezpieczeństwa[6].

Charakterystyka działań przestępczych w środowisku cyfrowym obejmuje realizacje różnych form przy użyciu technologii cyfrowych, Internetu, sieci komputerowych i innych elementów środowiska online i dotyczy przede wszystkim, nielegalnego uzyskania dostępu do systemów komputerowych, infekowania systemów komputerowych w celu kradzieży danych lub wyrządzenia szkód, oszustw polegających na zdobywaniu poufnych informacji poprzez podszywanie się pod zaufane źródła czego przykładem są przestępstwa określane jako phishing i spoofing.

Opis cyberprzestępczości musi być elastyczny, ponieważ pojawiają się nowe zagrożenia wraz z postępem technologii. Ciągłe dostosowywanie się organów ścigania, prawodawstwa i systemów bezpieczeństwa jest kluczowe w zwalczaniu tego rodzaju przestępczości.

[5] *6 rodzajów cyberprzestępstw, przed którymi możesz uchronić swoją firmę,* https://cyberware.pl/6-rodzajow-cyberprzestepstw-przed-ktorymi-mozesz-uchronic-swoja-firme, dostęp 21.04.2024 r.

[6] *Darknet: ciemna strona Internetu*, https://www.komputerswiat.pl/artykuly/redakcyjne/czym-jest-ciemna-strona-internetu-i-jak-sie-do-niej-dostac/qxt9m3y, dostęp 21.04.2024 r.

Rozdział 4.
Rola zgłaszania przestępstw w zwalczaniu cyberprzestępczości

Skuteczne i szybkie zgłaszanie incydentów przestępczych ma istotny wpływ na skuteczność zwalczania cyberprzestępczości. Do głównych punktów dotyczących roli zgłaszania przestępstw w tej dziedzinie należy zaliczyć:

Szybkie reagowanie: zgłaszanie incydentów cyberprzestępczych umożliwia szybkie reagowanie na zagrożenia. Im szybciej organy ścigania lub odpowiednie instytucje otrzymają informacje o ataku, tym większa szansa na zatrzymanie sprawcy i ograniczenie szkód. Najlepszym przykładem ukazującym znaczenie szybkiego przekazania informacji o przestępstwie będzie sytuacja, która będzie dotyczyła nieuprawnionego dostępu do rachunku bankowego przez sprawcę, a następnie dokonanie przez niego transakcji finansowych, które na pewnym etapie można zatrzymać poprzez blokadę środków na rachunku beneficjenta (art. 106a. Pr. bankowe – Podejrzenie wykorzystywania działalności banku dla celów przestępczych)[7].

Ochrona ofiar: składanie zgłoszeń jest kluczowe dla ochrony ofiar cyberprzestępstw. Dzięki zgłoszeniom możliwe jest udzielenie pomocy ofiarom, zwłaszcza jeśli są one indywidualnymi użytkownikami, firmami czy instytucjami[8].

Zbieranie danych dowodowych: organom ścigania potrzebne są informacje na temat rodzaju ataku, użytych narzędzi i technik, aby zbierać odpowiednie dowody. Zgłaszanie przestępstw dostarcza istotnych danych, które mogą być używane w procesie śledczym.

Współpraca międzynarodowa: zgłaszanie cyberprzestępstw jest kluczowe dla współpracy międzynarodowej. Ponieważ ataki często przenikają granice państw, skuteczna współpraca między różnymi krajami i agencjami jest niezbędna do ścigania sprawców.

---

[7] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe.

[8] Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych w tym kradzieży tożsamości. Informacja o wynikach kontroli. Nr ewid. 125/2022/P/21/042/KPB Warszawa: NIK.

Podnoszenie kwalifikacji: dzięki zgłoszeniom możliwe jest śledzenie najnowszych trendów w cyberprzestępczości, co pozwala na regularne szkolenie personelu odpowiedzialnego za bezpieczeństwo informacji.

Rozdział 5.
Proces przyjęcia zawiadomienia o cyberprzestępstwie

Pojęcie procesu samo w sobie jest wieloznaczne. Możemy nim określać bowiem pewne powiązane ze sobą działania, jakiś ciąg zdarzeń posiadający własny cel, zakres i przedmiot, jak też kolejne etapy określonego działania. W kontekście przyjęcia zawiadomienia o przestępstwie związanym z cyberprzestrzenią przedstawienie procesu przyjęcia zawiadomienia będzie mieściło się w tym samym zakresie definicyjnym. Rozmawiając o przyjęciu zawiadomienia o tak specyficznym przestępstwie jakim jest cyberprzestępstwo należy temat potraktować specjalistycznie, lecz wspierając się możliwościami jakie oferuje polskie prawo.

5.1. Kto ma obowiązek złożenia zawiadomienia o przestępstwie

Polska procedura karna nakłada obowiązek zawiadomienia organów ścigania o popełnieniu przestępstwa ściganego z urzędu. W tym celu w Kodeksie postępowania karnego został wprowadzony zapis dotyczący społecznego obowiązku zawiadomienia o przestępstwie określony w art. 304 § 1 k.p.k. Zgodnie z jego treścią, każdy kto dowiedział się o popełnieniu przestępstwa ściganego z urzędu ma społeczny obowiązek zawiadomić o tym fakcie prokuratora lub Policję. Oznacza to, że nie tylko pokrzywdzony lub bezpośredni świadek przestępstwa, ale każda osoba dysponująca informacjami na temat popełnienia przestępstwa powinna zawiadomić o tym organy ścigania. Przepis ten nie przewiduje kary za niedopełnienie wspomnianego obowiązku, odwołuje się natomiast do pożądanych postaw społecznych, dzięki którym popełnione przestępstwo nie pozostaje anonimowe, a jego sprawca nie może liczyć na bezkarność.

Ponadto w art. 304 § 2 k.p.k. ustawodawca przewidział prawny obowiązek zawiadomienia organów ścigania o popełnieniu przestępstwa. Jak wynika z przytoczonego przypisu instytucje państwowe i samorządowe, które w związku ze swą działalnością dowiedziały się o popełnianiu przestępstwa ściganego z urzędu są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa. W kontekście cyberprzestępczości powyższa sytuacja może mieć miejsce między innymi w przypadku popełnienia przestępstw takich

jak: uszkodzenie danych informatycznych (art. 269 § 1 k.k.) lub zakłócenie systemu komputerowego (art. 269a k.k.).

Należy pamiętać również o treści art. 240 k.k., który przewiduje karalne niezawiadomienie o przestępstwie. W wymienionym przepisie określony został katalog przestępstw, co do których każda osoba mająca wiarygodną wiadomość o karalnym przygotowaniu, usiłowaniu lub dokonaniu wymienionych czynów zabronionych jest zobowiązana zawiadomić niezwłocznie organ powołany do ścigania przestępstw. Oprócz wymienionych enumeratywnie przestępstw sytuacja ta dotyczy również przestępstw o charakterze terrorystycznym, które mogą zwierać znamiona cyberprzestępstw. Jako przykład warto przytoczyć wymieniony powyżej art. 269 § 1 k.k.

Jednak zgodnie z art. 240 § 2 k.k. nie popełnia przestępstwa określonego w art. 240 § 1 k.k., kto zaniechał zawiadomienia, mając dostateczną podstawę do przypuszczenia, że wymieniony w § 1 organ wie o przygotowywanym, usiłowanym lub dokonanym czynie zabronionym; nie popełnia przestępstwa również ten, kto zapobiegł popełnieniu przygotowywanego lub usiłowanego czynu zabronionego określonego w § 1. Ponadto jak wynika z treści art. 240 § 2a k.k. nie podlega karze pokrzywdzony czynem wymienionym w § 1, który zaniechał zawiadomienia o tym czynie. Jeżeli jednak sprawca zaniechał zawiadomienia organu ścigania z obawy przed odpowiedzialnością karną grożącą jemu samemu lub osobom mu najbliższym, popełnia on wprawdzie przestępstwo, ale zgodnie z Kodeksem karnym nie podlega karze (art. 240 § 3 k.k.)[9].

5.2. Złożenie zawiadomienia

Do złożenia zawiadomienia o przestępstwie uprawniona jest każda osoba, która posiada informację o jego popełnieniu lub podejrzeniu jego popełnienia, bez względu na wiek, płeć, rasę, narodowość itp. Ustne zawiadomienie o przestępstwie powinno być przyjęte od każdej osoby, która w tym celu przybyła do jednostki organizacyjnej Policji, również wtedy, gdy inna jednostka Policji lub inny organ ścigania jest właściwy miejscowo lub rzeczowo do prowadzenia postępowania przygotowawczego. Zawiadomienie o przestępstwie obliguje organy ścigania do podjęcia odpowiednich czynności, wynikających z sytuacji.

Osoba powyżej 17. roku życia składająca zawiadomienie o przestępstwie, pouczana jest m.in. o odpowiedzialności karnej za: zawiadomienie Policji o niepopełnionym przestępstwie (art. 238 k.k.), fałszywe oskarżenie (art. 234 k.k.) oraz za składanie fałszywych zeznań (art. 233 k.k.). Natomiast jeżeli o przestępstwie zawiadamia osoba

[9] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 10.

małoletnia, która nie ukończyła jeszcze 17 lat, należy tę osobę najpierw zapoznać z treścią art. 233 k.k., art. 234 k.k. i art. 238 k.k., z uprzedzeniem nie o odpowiedzialności karnej za naruszenie tych przepisów, lecz o konsekwencjach prawnych ich naruszenia, przewidzianych w ustawie z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich[10].

Podczas przyjmowania zawiadomienia o przestępstwie od pokrzywdzonego może być obecna osoba przez niego wskazana, jeżeli nie uniemożliwia to przeprowadzenia czynności albo nie utrudnia jej w istotny sposób, co wynika z treści art. 299a k.p.k. Osobą tą w szczególności może być osoba najbliższa, przedstawiciel instytucji lub organizacji społecznej wspierającej ofiary przestępstw.

Protokół przyjęcia ustnego zawiadomienia o przestępstwie od osoby niewładającej językiem polskim sporządza się zawsze z udziałem tłumacza, a od osoby głuchej, niemej lub głuchoniemej – z udziałem tłumacza języka migowego (daktylologa). Należy jednak zaznaczyć, że zgodnie z art. 204 § 1 pkt 1 k.p.k. można bez udziału daktylokloga przyjąć od osoby głuchej lub niemej zawiadomienie o przestępstwie w formie pisemnej, a także przesłuchać taką osobę wyłącznie na piśmie.

Jeżeli nie można sporządzić protokołu przyjęcia zawiadomienia o przestępstwie wobec niemożności dostatecznie komunikatywnego porozumienia się z zawiadamiającym z powodu jego specyficznego stanu psychofizycznego albo nieznajomości języka polskiego, przy jednoczesnej niemożności natychmiastowego sprowadzenia tłumacza – policjant sporządza jedynie notatkę urzędową wskazującą taki powód i zawierającą opis informacji na temat zgłaszanego przestępstwa, jakie udało się uzyskać[11]. Na podstawie danych zawartych w notatce urzędowej Policja podejmuje odpowiednie czynności. W powyższym przypadku protokół można spisać w odpowiednim do okoliczności terminie późniejszym, na który należy wezwać osobę zawiadamiającą o przestępstwie, jeżeli potrzeba jego sporządzenia nadal występuje.

W razie otrzymania zawiadomienia o przestępstwie ściganym na wniosek, należy uzyskać taki wniosek od podmiotu uprawnionego do jego złożenia. W przypadku, gdy pokrzywdzony nie jest osobą fizyczną, wniosek należy uzyskać od organu uprawnionego do działania w jego imieniu. W myśl art. 51 k.p.k., w przypadkach określonych w tym przepisie, do złożenia wniosku o ściganie jest uprawniony przedstawiciel ustawowy lub osoba, pod której stałą pieczą pokrzywdzony pozostaje, a w myśl art. 52 k.p.k. w przypadku śmierci pokrzywdzonego do złożenia wniosku są uprawnione osoby najbliższe lub osoby pozostające na jego utrzymaniu, a w wypadku ich braku

[10] Ustawa z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich.

[11] Wytyczne nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów, § 4.

lub nieujawnienia – prokurator, który działa z urzędu. Wniosek o ściganie może być złożony ustnie do protokołu lub na piśmie, przy czym Kodeks postępowania karnego nie wymaga żadnej szczególnej formy tego pisma. Nie jest wystarczające samo zawiadomienie o przestępstwie złożone przez pokrzywdzonego, jeżeli nie zawiera wyraźnego żądania ścigania sprawcy. W takim przypadku należy uzyskać wyraźne oświadczenie pokrzywdzonego, czy składa wniosek o ściganie, które może być zamieszczone w protokole przesłuchania pokrzywdzonego w charakterze świadka albo w odrębnym protokole przyjęcia wniosku o ściganie. Wniosek o ściganie można przyjąć także od osoby, która nie ukończyła 18 lat, jeśli osoba ta nabyła pełną zdolność do czynności prawnych przez zawarcie małżeństwa, chociażby nawet małżeństwo zostało unieważnione. Jeżeli pokrzywdzona osoba dorosła nie jest ubezwłasnowolniona chociażby częściowo, ale z okoliczności faktycznych wynika, że nie składa wniosku o ściganie dlatego, że z uwagi na zaburzenia psychiczne może nie rozumieć swojej sytuacji prawnej, Policja powinna wystąpić do sądu opiekuńczego o ustanowienie kuratora w tym zakresie. Należy również wystąpić do sądu opiekuńczego z wnioskiem o wydanie zarządzenia zastępującego wniosek o ściganie, jeśli przedstawiciel ustawowy lub opiekun małoletniego pokrzywdzonego nie chce złożyć wniosku o ściganie i przez to narusza jego dobro albo jest sprawcą danego przestępstwa[12].

5.3. Przyjęcie zawiadomienia o cyberprzestępstwie – zbiór dobrych praktyk

Większość najpospolitszych cyberprzestępstw poprzedza zastosowanie przez sprawcę socjotechniki, czyli innymi słowy wdrożenia pewnych zabiegów mających na celu osłabić czujność lub spowodować uczucie strachu w ofierze. Ta najczęściej stworzona na potrzeby chwili sytuacja, mówiąc w dużym skrócie i najogólniej, ma w krótkim czasie sprawić, aby ofiara przestępstwa uruchomiła dołączony do wiadomości link lub spowodowała, że poświęcimy czas na rozmowę, podczas której przekażemy dane, o które poprosi nas sprawca.

Z uwagi na powyższe, na podstawie analiz spraw karnych prowadzonych przez Prokuratury Rejonowe w Polsce w Departamencie do spraw Przestępczości Gospodarczej Prokuratury Krajowej sporządzono szereg dokumentów opisujących różne scenariusze i sposoby cyberataków. Na potrzeby niniejszej publikacji wybrano i opisano wybrane problemy, które powinny dostarczyć niezbędnej wiedzy i zbudować obraz problemu, ale i katalog możliwości jego prawidłowego, merytorycznego rozwiązania.

[12] Tamże, § 5.

Atak DDos

Ataki typu DDoS (ang. *distributed denial of service*, w wolnym tłumaczeniu: rozproszona odmowa usługi) są jednymi z najczęściej występujących ataków hakerskich, które kierowane są na systemy komputerowe lub usługi sieciowe i mają za zadanie zajęcie wszystkich dostępnych i wolnych zasobów w celu uniemożliwienia funkcjonowania całej usługi w sieci Internet (np. strony internetowej i poczty znajdującej się na hostingu).

Na czym polega atak DDoS

Celem ataków sprawców są zarówno strony internetowe podmiotów publicznych, jak i prywatnych, platformy przetargowe i aukcyjne, portale edukacyjne, usługi hostingowe. Ataki powodują utrudnienia w prowadzeniu edukacji zdalnej, korzystaniu z elektronicznych usług publicznych czy prowadzeniu działalności gospodarczej przy wykorzystaniu sieci i systemów informatycznych. Ataki DoS i DDoS polegają na zablokowaniu dostępu do systemu przez zajęcie jego zasobów, przy czym w ataku DDoS do przeciążenia atakowanego systemu dochodzi poprzez wygenerowanie wielu poleceń przy wykorzystaniu wielu urządzeń (np. zainfekowanych złośliwym oprogramowaniem komputerów), którymi zarządza sprawca.

Przeprowadzenie przez sprawców ataku wymaga stworzenia lub wykorzystania zbudowanej przez inne osoby infrastruktury (tzw. botnetu), składającej się z przejętych urządzeń (tzw. botów, czyli m.in. komputerów, kamer internetowych, routerów itp.), które jednocześnie zaatakują system. Urządzenia te zazwyczaj są zainfekowane złośliwym oprogramowaniem powodującym, że wykonują na polecenie atakującego określone czynności. Należy zwrócić uwagę, że sprawcy mogą wykorzystać (odpłatnie lub nieodpłatnie) infrastrukturę stworzoną przez osoby trzecie.

Ustalając odpowiedzialność karną za atak odmowy usługi należy mieć na uwadze również:

a) odpowiedzialność karną za zainfekowanie szkodliwym oprogramowaniem urządzeń, które zostaną wykorzystane jako część botnetu do przeprowadzenia ataku (art. 267 § 1-3 k.k.);
b) odpowiedzialność karną za wytworzenie czy udostępnienie oprogramowania przystosowanego do infekowania urządzeń (art. 269b § 1 k.k.);
c) odpowiedzialność karną za przestępstwo prania pieniędzy – z uwagi na to, że atakom odmowy usługi towarzyszy zazwyczaj żądanie okupu za zaprzestanie ataku, a jako dane do płatności podawane są rachunki bankowe „słupów", portfele kryptowalut lub są wykorzystywane inne anonimowe metody płatności (art. 299 § 1 k.k.).

W sprawach z zakresu ataków odmowy usługi celowe jest podjęcie następujących czynności:

1. Przyjęcie zawiadomienia o podejrzeniu popełnienia przestępstwa oraz przesłuchanie zawiadamiającego, a także pokrzywdzonego (osobę reprezentującą pokrzywdzonego), jeśli nie jest zawiadamiającym w celu ustalenia:
   - w jaki sposób rozpoznano atak i jak wyglądał jego przebieg, kiedy się rozpoczął i zakończył atak, w jaki sposób pokrzywdzony ustalił ten przedział czasowy, w jakim okresie i jakie komunikaty o niedostępności odnotowali użytkownicy zaatakowanej strony/platformy/usługi/aplikacji;
   - skutków ataku: np. jak długo strona była niedostępna, jaka była wartość zaistniałej szkody; jeśli czyn ma zostać zakwalifikowany z art. 269 § 1 k.k. konieczne jest ustalenie czy brak dostępności dotyczył danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego i jakie były lub mogły być skutki braku dostępności;
   - celowości ataku (motywu działania sprawcy);
   - czy atak był powiązany z żądaniem okupu;
   - czy istnieje możliwość działań na zlecenie (np. konkurencji);
   - czy można korelować atak z istotnymi wydarzeniami (np. udostępnieniem nowego produktu lub usługi, ostatnim dniem terminu np. rozliczenia podatkowego, debiutem giełdowym, opublikowaniem budzącego zainteresowanie artykułu na stronie objętej atakiem);
   - komu i jaką korzyść przyniosłoby zablokowanie usługi;
   - czy był to atak jednorazowy czy powtarzający się (jeśli infrastruktura pokrzywdzonego była atakowana wcześniej, celowe jest ustalenie, czy składał w tym zakresie zawiadomienie o podejrzeniu popełnienia przestępstwa, która powszechna jednostka organizacyjna prokuratury i pod jaką sygnaturą prowadziła postępowanie i jakie były poczynione ustalenia; jeśli pokrzywdzony nie może wskazać sygnatury sprawy, do ustalenia wcześniejszych postępowań należy wykorzystać bazy danych Policji lub prokuratury);
   - jeśli atak odmowy usługi występował wcześniej, czy i jakie działania wdrożono w celu zapobieżenia atakom odmowy usługi, czy sprawcy ataku komunikowali się z pokrzywdzonym, a jeśli tak to w jaki sposób (jakich kanałów komunikacji używali sprawcy – istotnym jest ustalenie adresów poczty elektronicznej, telefonów, komunikatorów internetowych itp.);

- danych personalnych oraz kontaktowych osób mających wiedzę na temat ataku lub zaatakowanej strony/platformy/usługi/aplikacji oraz infrastruktury teleinformatycznej zaatakowanego (np.: informatyka, administratora infrastruktury sieciowej, administratora bezpieczeństwa informacji, wykonawcy zaatakowanej strony/platformy/usługi/aplikacji, zewnętrznego podmiotu, który świadczy usługi na rzecz pokrzywdzonego, podmiotu, który prowadził testy obciążeniowe) w celu przesłuchania ich w charakterze świadka na okoliczność sprawy;
- czy do odmowy usługi doszło w związku z jakimś szczególnym zdarzeniem związanym ze zwiększeniem obciążenia systemu (np. w sklepie internetowym: promocja/wyprzedaż, dla podmiotów publicznych: uruchomienie aukcji elektronicznej, ostatni dzień wykonania jakiegoś obowiązku – złożenia PIT, przesłania deklaracji 800+, podłączenie systemu do innych systemów [np. ePUAP], uruchomienie dodatkowych usług).

2. W zależności od przyjętej kwalifikacji czynu objętego postępowaniem – przyjęcie wniosku o ściganie od uprawnionej osoby, o ile jest wymagany. Wniosek niezbędny będzie w sprawach kwalifikowanych z art. 267 § 1-3 k.k., 268a § 1 k.k.
3. W zależności od stanu faktycznego rozważenie zażądania również od pokrzywdzonego lub podmiotu przez niego wskazanego, będącego dysponentem danych (logów) obrazujących ruch sieciowy odnoszący się do normalnego obciążenia dla zdarzenia odpowiadającego charakterystyką zdarzeniu, w toku którego zawiadamiający twierdzi, że doszło do ataku (np. dla podmiotów publicznych: prowadzonych wcześniej aukcji elektronicznych, ostatniego dnia wykonania jakiegoś obowiązku – złożenia PIT, przesłania deklaracji 800+ itp.).

Dopiero po uprawdopodobnieniu ataku na podstawie zgromadzonego materiału dowodowego, przesłuchaniu kluczowych świadków i zgromadzeniu logów (ewentualnie również schematów sieci, testów obciążeniowych i innych materiałów dotyczących atakowanej usługi i przebiegu ataku) celowe jest powołanie biegłego z zakresu informatyki w celu m.in.:

- sporządzenia analizy natężenia ruchu sieciowego na osi czasu,
- wyselekcjonowania i zidentyfikowania adresów IP występujących w logach,
- określenia, w których przedziałach czasowych odnotowano największe natężenie ruchu sieciowego,
- określenia, w jakich przedziałach czasowych i przy jakim natężeniu ruchu sieciowego nastąpił brak dostępności usługi,
- stwierdzenia, czy dany ruch sieciowy wskazuje na atak odmowy usługi,
- stwierdzenia, jakie adresy IP są atakującymi,

- stwierdzenia, jaki jest czas i częstotliwość ataku, w przypadku występowania wcześniejszych ataków stwierdzenia, czy istnieje korelacja adresów IP aktualnego ataku z wcześniejszymi.

Po potwierdzeniu przez biegłego z zakresu informatyki, że ruch sieciowy świadczy o ataku odmowy usługi niezbędne jest zażądanie od podmiotów będących dostawcami usług internetowych wydania danych retencyjnych dotyczących abonentów, którym przydzielono adresy IP zidentyfikowane przez biegłego jako adresy IP atakujące (generujące podwyższony ruch). Kolejność czynności należy dostosować do czasu, jaki pozostał na przechowywanie danych retencyjnych (w Polsce retencja danych telekomunikacyjnych wynosi 12 miesięcy) i czasu, w jakim ma zostać wydana przez biegłego opinia. Dokonanie ustaleń abonentów, którym przydzielono adresy IP generujące podwyższony ruch sieciowy pozwoli biegłemu na przygotowanie kompleksowej opinii – biegły w opinii zobrazuje nie tylko adresy IP, z których był wygenerowany największy ruch, ale również podmioty generujące podwyższony ruch sieciowy, którym przydzielono wiele adresów IP[13].

Fałszywe sklepy internetowe

Czyn polegający na oferowaniu towarów w fikcyjnym sklepie internetowym kwalifikowany jest z art. 286 § 1 k.k. Cechą podstawową fikcyjnego sklepu internetowego jest to, że prowadzący sklep nigdy nie posiadają oferowanego towaru, nie planują go sprzedać, nie dostarczają towarów zakupionych przez klientów, ewentualne pozytywne komentarze dotyczące sklepu są wykreowane przez osoby go prowadzące. W sprawach z zakresu fałszywych sklepów internetowych celowe jest podjęcie następujących czynności:

1. Przyjęcie zawiadomienia o podejrzeniu popełnienia przestępstwa oraz przesłuchanie zawiadamiającego, a także pokrzywdzonego (osoby reprezentującej pokrzywdzonego), jeśli nie jest zawiadamiającym w celu ustalenia:
   - Jakiego sklepu dotyczy zawiadomienie. Należy ustalić pełną nazwę oraz adres strony internetowej, pod którą dany sklep był prowadzony. Jeśli pokrzywdzony nie pamięta danych sklepu jest prawdopodobne, że dane sklepu znajdują się w wiadomościach e-mail, jakie dostał po dokonaniu zamówienia. Adres strony internetowej fikcyjnego sklepu powinien być bezwzględnie wskazany w opisie

[13] Prokuratura Krajowa, Departament do spraw Przestępczości Gospodarczej (2021), nr 1001-7.025.1.2021, 20 sierpnia 2021 r.

sprawy lub czynu lub zarzutu w systemie PROK-SYS[14], co ułatwi łączenie postępowań prowadzonych o ten sam czyn.

- Kiedy i w jaki sposób pokrzywdzony znalazł ofertę tego sklepu.
- Jeżeli nastąpiło to w wyniku prowadzonej kampanii reklamowej, należy ustalić, gdzie i w jaki sposób fikcyjny sklep był reklamowany.
- Jakie produkty znajdowały się w ofercie sklepu.
- Czy na stronie sklepu podane były dane podmiotu prowadzącego sklep, jego adres, numer rachunku bankowego do dokonywania wpłat za towary, numery telefonów, adres poczty elektronicznej, regulamin, polityka zwrotu towaru, polityka prywatności i jakie dane były tam podane.
- Co przekonało zawiadamiającego/pokrzywdzonego do dokonania zakupów w danym sklepie. W szczególności należy ustalić, czy zapoznał się z regulaminem, polityką zwrotu towaru, czy dokumenty te były napisane poprawną polszczyzną czy ewentualne błędy językowe wskazywały, że mogą być to dokumenty tłumaczone maszynowo.
- Czy zawiadamiający/pokrzywdzony zapoznawał się z komentarzami innych kupujących. Na jakiej stronie internetowej czytał pozytywne komentarze dotyczące danego sklepu internetowego.
- Czy i w jaki sposób nastąpił kontakt z przedstawicielami sklepu internetowego.
- Czy na stronie sklepu dostępny był formularz kontaktowy, live chat lub kontakt przez komunikator internetowy. Czy pokrzywdzony korzystał z formularza kontaktowego znajdującego się na stronie sklepu internetowego.
- Jakie dane podał zawiadamiający/pokrzywdzony.
- Czego dotyczyła komunikacja prowadzona przez live chat lub komunikator internetowy.
- W jaki sposób uzyskał informację, na jaki rachunek bankowy wpłacić ma środki za zakupiony towar.
- W jaki sposób dokonał zapłaty za oferowane produkty/usługi.
- Czy i jakie dokumenty pokrzywdzony uzyskał po dokonaniu transakcji wiadomości e-mail, wiadomości SMS, dokumenty w formacie .pdf.
- Jeśli były przesyłane wiadomości SMS – jaki był numeru telefonu nadawców lub tzw. nadpis. Jeśli pokrzywdzony dostał wiadomość SMS – konieczne jest

[14] W. Krasnopolska, *Przygotowanie i wdrożenie metodyki z zakresu pozyskiwania i przetwarzania informacji oraz komunikacji przy realizacji zadań prokuratury z wykorzystaniem systemu informatycznego PROK-SYS*, Prokuratura Krajowa 2 stycznia 2023, https://www.gov.pl/web/prokuratura-krajowa/przygotowanie-i-wdrozenie-metodyki-z-zakresu-pozyskiwania-i-przetwarzania-informacji-oraz-komunikacji-przy-realizacji-zadan-prokuratury-z-wykorzystaniem-systemu-informatycznego-prok-sys, dostęp 28.04.2024 r.

procesowe utrwalenie treści i postaci wiadomości SMS (np. w drodze oględzin, załączenia do protokołu przesłuchania wydruku zdjęcia wiadomości SMS).
- Czy pokrzywdzony kontaktował się z bankiem.
- Czy bank podjął działania dotyczące zablokowania transakcji lub zwrotu środków.

2. Uzyskanie zapisu komunikacji prowadzonej z osobami prowadzącymi fałszywy sklep internetowy. Jeśli pokrzywdzony w związku ze złożonym zamówieniem otrzymał wiadomości e-mail (z potwierdzeniem zamówienia lub instrukcją jak ma zapłacić za zamówiony towar) niezbędne jest procesowe zabezpieczenie treści wiadomości wraz z nagłówkiem internetowym (źródłem wiadomości). Pozyskanie oraz analiza nagłówków wiadomości e-mail (źródła wiadomości) jest kluczowe dla ustalenia, z jakiego adresu poczty elektronicznej wiadomość została wysłana, na jaki adres poczty elektronicznej wysłana zostanie odpowiedź na wiadomość oraz kiedy wiadomość została nadana.
3. Uzyskanie potwierdzeń transakcji z rachunku bankowego pokrzywdzonego, – wskazujących na jaki rachunek bankowy przekazał on środki za zamawiany towar. Jeśli sklep powiązany był z fałszywym panelem logowania do bankowości elektronicznej należy pozyskać również wydruki/wyciągi z bankowości elektronicznej, dokumentujące nieuprawnione/kwestionowane transakcje (przelewy). Jeśli pokrzywdzony dokonał samodzielnych wydruków danych ze strony sklepu internetowego należy je włączyć w poczet materiału dowodowego sprawy (w szczególności celowe jest uzyskanie: wydruków regulaminu sklepu, polityki zwrotów towarów, polityki prywatności, danych kontaktowych lub innych danych i dokumentów).
4. Uzyskanie informacji o rachunkach bankowych, na które wpływały środki pieniężne osób pokrzywdzonych działaniem fikcyjnego sklepu internetowego (tj. rachunków służących do przestępstwa prania pieniędzy). Należy jednocześnie pamiętać o tym, że różni pokrzywdzeni mogli wpłacać środki na różne rachunki bankowe. Zasadniczo w fikcyjnym sklepie do przyjmowania pieniędzy wykorzystywane są rachunki bankowe zakładane na tzw. słupy, np. osoby bezdomne, uzależnione.
5. W zakresie rachunków bankowych wykorzystywanych w fikcyjnym sklepie należy pozyskać następujące dane:
   - dane osobowe i kontaktowe osób upoważnionych do dokonywania dyspozycji, dane pełnomocników,
   - kiedy, gdzie i jak zostały założone ustalone rachunki bankowe, czy do rachunków bankowych zostały wydane karty – jeśli tak to dla jakich osób i na jaki adres zostały wysłane karty wraz z danymi do ich aktywacji,

- oryginały umów o prowadzenie rachunku bankowego oraz inne dokumenty powiązane z umowami,
- historię transakcji z rachunków bankowych w wyznaczonym przez wnioskodawcę okresie, uwzględniającej również próby dokonania przelewów (w tym historię użycia kart wydanych do rachunku) w postaci elektronicznej, informacje o złożonych wnioskach o kredyty lub pożyczki, logowaniach do platformy ePUAP lub innych usług publicznych za pośrednictwem bankowości elektronicznej,
- informacje o numerze telefonu służącego do komunikacji z bankiem (w tym o numerze, na który były wysyłane SMS z hasłami autoryzacyjnymi) dysponenta rachunku oraz wszelkich zmianach w tym zakresie.

Zgodnie z art. 105 ust. 1 pkt 2 lit b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, bank ma obowiązek udzielenia informacji stanowiących tajemnicę bankową na żądanie sądu lub prokuratora w związku z toczącym się postępowaniem o przestępstwo m.in. z art. 299 k.k. Mając na uwadze powyższe, uwzględnienie już na etapie wszczęcia śledztwa czynu z art. 299 § 1 k.k., polegającego na przestępstwie prania pieniędzy, pozwala zdynamizować postępowanie i skrócić czas pozyskania danych objętych tajemnicą bankową. Szybkość pozyskiwania i analizy danych dotyczących transferów pieniężnych ma kluczowe znaczenie, a w szczególności pozwala na ustalenie miejsc, w których doszło do wypłat środków i zabezpieczenie nagrań z monitoringu.

Jeśli środki transferowane były na giełdy kryptowalut, należy zwrócić się do podmiotu prowadzącego giełdę w celu uzyskania danych dotyczących danego użytkownika – w tym danych osobowych, adresów e-mail, adresów IP logowań, numeru rachunku bankowego, na który dokonywano wypłat, informacji dotyczących weryfikacji tożsamości użytkownika (w tym np. nagrań z wideoweryfikacji). Po pozyskaniu danych z banku prowadzącego rachunki bankowe, na które wpłynęły lub miały wpłynąć środki pokrzywdzonego, należy dokonać analizy historii transakcji oraz danych podmiotu, na rzecz którego ten rachunek jest prowadzony (np. w drodze OSINT ang. open-source intelligence, czyli działania polegające na zdobywaniu i gromadzeniu informacji z otwartych, ogólnodostępnych źródeł) w celu ustalenia, czy jest to rachunek tzw. słupa służący do popełnienia przestępstwa prania pieniędzy.

Po ustaleniu adresu strony internetowej, za pośrednictwem której sklep internetowy prowadzi działalność, należy dokonać procesowego utrwalenia zawartości strony internetowej fałszywego sklepu internetowego poprzez dokonanie oględzin. Czynność procesowa może być przeprowadzona przy udziale biegłego z zakresu informatyki śledczej. Z przeprowadzonych oględzin należy sporządzić protokół, do którego jako załącznik należy dołączyć nośnik (płytę CD/DVD/pendrive), na którym zostanie zapisany obraz/kopia strony internetowej wraz z wszystkimi podstronami

obejmująca wszystkie jej funkcjonalności, dokumentująca w szczególności: strukturę strony, ofertę, zdjęcia i opisy produktów, regulaminy znajdujące się na stronie, jak też znajdujące się na stronie pliki tekstowe, dźwiękowe oraz video. Po ustaleniu adresu strony internetowej fałszywego sklepu (nazwy domenowej) należy dokonać jej sprawdzenia za pośrednictwem baz WHOIS, np. centralops.net, w zakresie domeny .pl na stronie dns.pl, zaś w zakresie domeny.eu na stronie eurid.eu w celu ustalenia danych powiązanych z rejestracją danej nazwy domenowej – daty rejestracji, abonenta i jego adresu e-mail czy pośrednika w rejestracji domeny. Po dokonaniu powyższych sprawdzeń należy zażądać danych abonenta domeny (czyli rejestrującego) od podmiotu prowadzącego rejestr (dla domeny.pl jest to NASK), rejestratora domeny (pośrednika w rejestracji nazwy domenowej) i hostingodawcy. Jeśli adresem strony internetowej (np. podanym przez pokrzywdzonego) jest link skrócony przy pomocy serwisów skracających adresy URL (takich jak np. tiny.pl, cutt.ly, bit.ly), należy ustalić właściwy adres strony internetowej (nazwę domenową), która została skrócona (sprawdzenia można dokonać na stronie serwisu służącego do skracania adresów URL). Konieczne jest również pozyskanie danych od podmiotu świadczącego usługi telekomunikacyjne w zakresie numerów MSISDN podanych przy zakładaniu rachunków bankowych służących do prania pieniędzy, numerów MSISDN służących do obsługi rachunku, na które wysyłane były kody do weryfikacji transakcji, numerów MSISDN podanych na stronie fałszywego sklepu lub numerów MSISDN, z których kontaktowano się z pokrzywdzonymi. Należy uzyskać od podmiotu świadczącego usługi telekomunikacyjne dane dotyczące wykazu połączeń tak ustalonego numeru MSISDN zawierającego wszystkie dane wskazane w art. 180c ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne w tym w szczególności lokalizację stacji przekaźnikowych BTS wraz ze współrzędnymi geograficznymi, azymutem i kątem anteny oraz zasięgiem wiązki, numery IMEI urządzeń z którymi współpracował wskazany numer abonencki w okresie, w którym doszło do zdarzenia objętego postępowaniem.

Pozyskanie od podmiotów świadczących usługi telekomunikacyjne informacji o abonentach, którym przydzielono adresy IP, z których logowano się do rachunków bankowych, tzw. słupów, służących sprawcom do przyjęcia środków pochodzących od pokrzywdzonych, kont na giełdach kryptowalut, paneli logowań do kont hostingowych, kont poczty elektronicznej oraz z których rejestrowano nazwy domenowe itp. (z uwzględnieniem wszystkich danych wskazanych w art. 180c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, w zakresie jak w pkt 11)[15].

[15] Prokuratura Krajowa, Departament do spraw Przestępczości Gospodarczej (2021), nr. 1001-7.024.6.202, 20 grudnia 2021 r.

Spoofing

W 2021 roku wśród spraw analizowanych i koordynowanych w Wydziale do Spraw Cyberprzestępczości Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej coraz częstsze były postępowania, w których sprawcy podszywali się pod numer telefonu innej osoby lub podmiotu. Tego typu działanie to tzw. spoofing, który polega na podszywaniu się pod inny element systemu teleinformatycznego. Wyróżnić można kilka rodzajów spoofingu, np. spoofing adresów e-mail. W tym zakresie wobec funkcjonariuszy przyjmujących zawiadomienia o popełnieniu przestępstwa, kierowane były zalecenia dotyczące pozyskiwania i procesowego zabezpieczania nagłówków internetowych wiadomości elektronicznych.

Spoofing telefoniczny polega na wykonywaniu połączeń telefonicznych z wykorzystaniem nieprawdziwego identyfikatora inicjującego połączenie (tzw. callerID). Korzystający z usług umożliwiających podszywanie się pod numer MSISDN, przy wykorzystaniu infrastruktury operatorów naruszających integralność sieci, może wprowadzić dowolny numer telefonu, który ma się wyświetlić na ekranie odbierającego połączenie. Przy tworzeniu sieci telefonicznych nie uwzględniono ryzyka związanego z podszywaniem się pod numer inicjujący połączenie, zaś sama komunikacja i przekazywanie wiązek połączeń pomiędzy operatorami opiera się na zaufaniu. Jeśli zatem inicjujący połączenie podszywa się pod inny numer MSISDN, operatorzy sieci telekomunikacyjnej nie weryfikują tej informacji, a centrale ufają komunikatom wysyłanym przez inne centrale. Usługi umożliwiające podszywanie się pod identyfikator inicjującego połączenie są łatwo dostępne w Internecie oraz tanie, zatem sprawca nie musi posiadać szczególnej wiedzy z zakresu funkcjonowania sieci telekomunikacyjnej.

Spoofing telefoniczny w 2021 roku najczęściej obserwowany był w scenariuszach oszustw, w których sprawcy podszywali się pod pracownika infolinii banku. Numerem telefonu wyświetlającym się u pokrzywdzonego był numer infolinii bankowej. Pokrzywdzeni najczęściej byli informowani o wykryciu próby rzekomego włamania na rachunek bankowy i proszeni o zainstalowanie aplikacji zdalnego pulpitu, dającej sprawcom dostęp do urządzenia pokrzywdzonego. W innym podobnym scenariuszu sprawcy podszywają się pod numer telefonu jednostki Policji (w tym m.in. pod numery telefonów wydziałów do walki z cyberprzestępczością komend wojewódzkich Policji), informując pokrzywdzonego o rzekomym włamaniu na jego rachunek bankowy i konieczności dokonania przelewu środków finansowych na inny rachunek bankowy.

Sprawcy podszywając się pod numery telefonów infolinii bankowych lub jednostek Policji chcą podnieść wiarygodność scenariusza socjotechnicznego i tym samym

zwiększyć skuteczność ataku, którego celem jest pozyskanie środków zgromadzonych na rachunku bankowym pokrzywdzonego.

Spoofing wykorzystywany jest również w sprawach dotyczących kierowania gróźb karalnych oraz informowania o podłożeniu ładunków wybuchowych. Znaczną ilość tego typu zdarzeń odnotowano na przełomie 2021 i 2022 roku. Sprawcy podszywali się pod numery telefonów osób publicznych, redaktorów serwisów zajmujących się cyberbezpieczeństwem, pracowników Naukowej i Akademickiej Sieci Komputerowej (NASK-PIB). Najczęściej odtwarzane były wówczas komunikaty, odczytywane przez narzędzia przekształcające tekst na mowę syntetyczną (np. syntezator mowy Ivona).

Z uwagi na sposób działania sprawców należy mieć na uwadze, że część z opisanych powyżej ataków miała na celu przede wszystkim wyrządzenie szkody osobie, której dane zostały wykorzystane – zarówno poprzez ośmieszenie jej lub obniżenie wiarygodności, jak również skierowanie wobec takich osób czynności organów ścigania. Osoby te, w zależności od poczynionych ustaleń, powinny zostać zatem uznawane za pokrzywdzonych czynem z art. 190 a § 2 k.k., nie zaś za sprawców czynów z art. 190 § 1 k.k. lub art. 224a k.k., co stwierdzono w niektórych sprawach.

Dla ustalenia, czy inicjującym połączenie była osoba lub podmiot, którego numer MSISDN wyświetlił się na urządzeniu osoby, do której dzwoniono, bezwzględnie konieczne jest pozyskanie danych bilingowych zarówno dla numeru, na który dzwoniono, jak również dla numeru, z którego połączenie miało zostać zainicjowane. Należy uzyskać od podmiotu świadczącego usługi telekomunikacyjne dane dotyczące wykazów połączeń tak ustalonych numerów MSISDN, zawierające wszystkie dane wskazane w art. 180c ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, w tym w szczególności lokalizację stacji przekaźnikowych BTS, numery IMEI urządzeń z którymi współpracował wskazany numer abonencki w okresie, w którym doszło do zdarzenia objętego postępowaniem.

Tak pozyskane dane bilingowe należy następnie zestawić i ustalić, czy nie ma pomiędzy nimi rozbieżności. Porównać należy zarówno połączenia przychodzące i wychodzące dla obydwu numerów czas, w którym doszło do połączenia (*time stamp*) oraz czas trwania połączenia. Celem tej czynności jest weryfikacja czy połączenie, którego dotyczy postępowanie, zostało ujęte w bilingach obu numerów MSISDN i czy dane bilingowe dotyczące tego połączenia są identyczne na obu bilingach (co do czasu rozpoczęcia i zakończenia połączenia). Jeśli na bilingu numeru MSISDN, który miał być wywołującym połączenie, brak jest połączenia z numerem MSISDN odbiorcy połączenia – oznacza to, że doszło do spoofingu. Na spoofing mogą wskazywać również rozbieżności w czasie, w jakim miało dojść do nawiązania połączenia, zakończenia

połączenia lub czasie trwania połączenia, brak wskazanego w bilingu numeru wywołującego numer IMEI urządzenia lub danych dotyczących BTS[16].

Oszustwa z wykorzystaniem oprogramowania typu „zdalny pulpit"

Oszustwa z wykorzystaniem tak zwanego „zdalnego pulpitu", to oszustwa w których jeden z etapów polega na uzyskaniu dostępu do komputera innego użytkownika w sposób umożliwiający wgląd do zasobów systemowych, ale również możliwość zdalnego korzystania z tych zasobów. Oszustwa te popełniane są za pośrednictwem aplikacji AnyDesk, Team Viewer czy Quick Support.

Mechanizm przestępstwa polega przede wszystkim na odebraniu wiadomości mailowej lub podjęcia kontaktu telefonicznego za pośrednictwem komunikatora, np. aplikacji WhatsApp, z propozycją skorzystania z oferty handlowej dotyczącej sprzedaży kryptowalut bądź z informacją, w której sprawca wykorzystuje element niepewności, dotyczący sytuacji zabezpieczeń rachunku ofiary mówiąc wprost, że zgromadzone środki pieniężne na rachunku bankowym ofiary są zagrożone atakiem przez oszusta, złodzieja.

Bardzo często sprawca dokładnie nawet nie precyzuje o jaki atak chodzi. Sytuacja pospieszania, wyimaginowanego zagrożenia, konieczności natychmiastowego podjęcia kroków i zapewnienie ze strony atakującego o jego najlepszych intencjach, przedstawienia siebie jako wybawcę z sytuacji ma na celu skłonić ofiarę do zainstalowania legalnego i ogólnie dostępnego oprogramowania służącego do zdalnej obsługi komputera. Sprawca w pierwszej kolejności uzyskuje dostęp do systemu komputera, a następnie do konta bankowego ofiary.

Oprogramowanie takie umożliwia dostęp do komputera za pomocą zdalnego pulpitu bez opóźnienia, nawet w przypadku słabego połączenia internetowego.

Możliwe do wykonania czynności:

- pobranie od zgłaszającego oświadczenia o zwolnieniu banku z tajemnicy bankowej;
- uzyskanie wszelkich danych dotyczących transakcji bankowych, w szczególności należy uzyskać adresy logowań IP wraz z portami. Ponadto należy uzyskać treść kodów autoryzacyjnych wysyłanych na telefon pokrzywdzonego wraz z informacją, na jaki numer telefonu zostały przesłane i czy zostały wykorzystane (czy sprawca zmienił numer telefonu do autoryzacji dwuetapowej);
- dokonanie ustaleń w zakresie operatora/operatorów numerów telefonów podawanych przez pokrzywdzonego i wystąpienie do prokuratury nadzorującej postępowanie o wydanie stosownych postanowień o żądaniu udzielenia informacji

[16] Prokuratura Krajowa, Departament do spraw Przestępczości Gospodarczej (2022), nr. 1001-7.024.2.202, 10 stycznia 2022 r.

w celu uzyskania danych abonenta, jak również lokalizacji stacji BTS oraz historii połączeń;
- dokonanie analizy danych przekazanych przez operatorów telefonii komórkowej w celu ustalenia sprawcy i zabezpieczenia materiału dowodowego;
- dołączenie wiadomości mailowych, które otrzymywał pokrzywdzony wraz z rozwinięciem nagłówka;
- analiza nagłówków wiadomości pod kątem wyodrębnienia właściwych adresów IP, a następnie zwrócenie się do prokuratury w wydanie stosownych postanowień o zwolnieniu operatorów w celu ustalenia danych użytkownika końcowego przypisanego adresu IP;
- dokonanie analizy danych uzyskanych z banku, w szczególności w zakresie końcowych beneficjentów wykonanych transakcji;
- w przypadku ustalenia, iż podmioty, na których rzecz zostały zaksięgowane środki, mają siedziby za granicą należy rozważyć wystosowanie wniosku do prokuratury o wdrożenie międzynarodowej pomocy prawnej;
- rozważenie możliwości powołania biegłego w celu wyodrębnienia danych w postacie adresów IP logowań do programów typu „zdalny pulpit", sprawdzenie w KSIP rachunków bankowych odbiorców, w celu ustalenia podobnych postępowań lub postępowań zbiorczych[17].

[17] *Metodyka postępowania organów ścigania województwa śląskiego w zakresie zwalczania cyberprzestępczości, w tym przestępstw popełnianych na szkodę banków,* praca zbiorowa, Wydział do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Katowicach.

Rozdział 6.
Ramy prawne i instytucje odpowiedzialne za przekazanie informacji o ujawnieniu cyberprzestępstwa

Ramy prawne to zbiór przepisów i regulacji, które określają ogólne zasady i granice działania w danej dziedzinie lub obszarze. Obejmują one przepisy ustawowe, rozporządzenia, akty prawne oraz inne dokumenty prawne, które stanowią podstawę dla funkcjonowania instytucji, organizacji lub systemów. Przyjęcie zawiadomienia na płaszczyźnie cyberprzestępstwa może niejednokrotnie rodzić pewne problemy z uwagi na fakt, że jest to temat dość zawiły ze względu poruszanie się często w dość abstrakcyjnej przestrzeni oraz nieostrych uregulowaniach prawnych, które nie zawsze nadążają za zjawiskiem.

6.1. Krajowe ramy prawne

W Polsce krajowe ramy prawne dotyczące przyjęcia zawiadomień o cyberprzestępstwach obejmują kilka kluczowych aspektów. Poniżej przedstawiono ogólne informacje w tym zakresie.

Osoby pokrzywdzone cyberprzestępstwem lub świadkowie cyberprzestępstwa mogą zgłaszać je organom ścigania, takim jak Policja czy Prokuratura. Zgłoszenia te mogą być składane osobiście, telefonicznie lub elektronicznie[18]. Kodeks karny oraz Kodeks postępowania karnego zawierają przepisy dotyczące różnych form przestępstw, w tym tych związanych z naruszeniem systemów informatycznych czy bezpieczeństwa danych oraz zasady, które powinny być spełnione, aby zawiadomienie o popełnieniu przestępstwa złożone było w sposób zgodny z procedurami określonymi w obowiązujących przepisach prawa.

Z uwagi na to należy mieć na uwadze fakt, że złożenie zawiadomienia o przestępstwie w formie elektronicznej wymaga uzupełnienia mogących się pojawić braków formalnych, bowiem zawiadomienie o podejrzeniu popełnienia przestępstwa jest pismem procesowym, a forma tego dokumentu została określona w art. 119 Kodeksu postępowania karnego[19].

Kolejnym ważnym aspektem jest również to, aby być świadomym przepisów dotyczących ochrony danych osobowych. W kontekście naruszeń bezpieczeństwa związanych

[18] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego.
[19] Tamże.

z danymi osobowymi, sytuacje reguluje ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, która określa obowiązki informacyjne, zarządzanie ryzykiem oraz zasady zgłaszania incydentów związanych z danymi osobowymi[20].

Ustawa o cyberbezpieczeństwie

W Polsce problem cyberprzestępczości uregulowany został w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która wchodzi w zakres działań zmierzających do zabezpieczenia infrastruktury krytycznej. Jednakże, z punktu widzenia przeciwdziałania cyberprzestępczości, ważne jest również monitorowanie przepisów dotyczących bezpieczeństwa systemów informatycznych[21].

Centrum Bezpieczeństwa Cyberprzestrzeni (CSIRT-CERT Polska)

CSIRT-CERT Polska, działające przy NASK (Naukowa i Akademicka Sieć Komputerowa), odgrywa kluczową rolę w reagowaniu na cyberincydenty. Organizacja ta jest zaangażowana w analizę i reagowanie na zgłaszane przestępstwa cybernetyczne[22].

6.2. Międzynarodowe umowy i współpraca

Instytucje odpowiedzialne za przyjęcie zawiadomienia o cyberprzestępstwach na szczeblu międzynarodowym podejmują działania, które obwarowane są wieloma różnymi umowami międzynarodowymi. Ich funkcjonowanie ma celu koordynację i współpracę państw w zwalczaniu przestępczości komputerowej. Poniżej przedstawiono przykłady międzynarodowych uregulowań prawnych w tym zakresie.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie z dnia 23 listopada 2001 r (Budapesztańska Konwencja): jest to pierwsza międzynarodowa konwencja ukierunkowana na zwalczanie cyberprzestępczości. Zawiera postanowienia dotyczące nielegalnego dostępu do systemów informatycznych, fałszerstwa komputerowego, naruszenia danych oraz innych rodzajów przestępstw związanych z technologią informatyczną[23].

Protokół o zapobieganiu, zwalczaniu oraz karaniu za handel ludźmi, w szczególności kobietami i dziećmi, uzupełniający Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęty przez

[20] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
[21] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
[22] Tamże.
[23] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.

Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r. (Protokół z Palermo): choć bardziej znany ze zwalczania przestępczości zorganizowanej, protokół ten obejmuje także postanowienia dotyczące cyberprzestępczości[24].

Organizacje Międzynarodowe

Interpol: Międzynarodowa Organizacja Policji Kryminalnej (Interpol) jest kluczowym graczem w międzynarodowym ściganiu przestępstw komputerowych. Interpol ułatwia wymianę informacji, koordynuje wspólne operacje i służy jako platforma do współpracy międzynarodowej w dziedzinie cyberprzestępczości[25].

Europol: Agencja Europolu działająca na szczeblu Unii Europejskiej skupia się na zwalczaniu przestępczości zorganizowanej, w tym cyberprzestępczości. Europol ułatwia współpracę między państwami członkowskimi w tym obszarze[26].

FBI's Cyber Division (Dywizja ds. Cyberprzestępczości): w Stanach Zjednoczonych Federalne Biuro Śledcze (FBI) pełni kluczową rolę w zwalczaniu przestępczości komputerowej i cyberprzestępczości na szczeblu krajowym i międzynarodowym[27].

6.3. Instytucje odpowiedzialne za przekazanie informacji o zaistnieniu zdarzenia cyberprzestępstwa organom ścigania

W Polsce istnieje kilka instytucji, które pełnią istotną rolę w zakresie bezpieczeństwa cyberprzestrzeni. Poniżej przedstawiono kilka z nich:

Centrum Bezpieczeństwa Cyberprzestrzeni (CSIRT-CERT Polska)

Jest to jednostka działająca przy NASK (Naukowa i Akademicka Sieć Komputerowa). CSIRT-CERT Polska zajmuje się reagowaniem na incydenty cybernetyczne, świadczeniem usług doradczych w zakresie bezpieczeństwa oraz prowadzeniem działań profilaktycznych i edukacyjnych[28].

---

[24] Protokół o zapobieganiu, zwalczaniu oraz karaniu za handel ludźmi, w szczególności kobietami i dziećmi, uzupełniający Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęty przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r.

[25] *Interpol – Międzynarodowa Organizacja Policji*, https://antykorupcja.gov.pl/ak/import/instytucje-zaangazowane/3681,Interpol-Miedzynarodowa-Organizacja-Policji.html, dostęp 21.04.2024 r.

[26] *Europol*, https://www.europol.europa.eu/about-europol:pl, dostęp 21.04.2024r.

[27] Edukacyjny portal o antykorupcji prowadzony przez Centralne Biuro Antykorupcyjne., dostęp 21.04.2024 r.

[28] NASK (2024) Naukowa i akademicka sieć komputerowa, Kim jesteśmy, https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html, dostęp 21.04.2024 r.

CERT Polska (Computer Emergency Response Team Polska)

CERT Polska to jednostka działająca w Instytucie Chemii Bioorganicznej PAN. Oferuje wsparcie w zakresie reagowania na incydenty cybernetyczne, udziela porad i informacji dotyczących bezpieczeństwa IT.

Generalny Inspektor Ochrony Danych Osobowych (GIODO)

GIODO, obecnie Urząd Ochrony Danych Osobowych (UODO), pełni rolę nadzoru i ochrony prywatności w obszarze przetwarzania danych osobowych. W kontekście cyberbezpieczeństwa, UODO współpracuje z innymi instytucjami w zakresie ochrony danych.

Agencja Bezpieczeństwa Wewnętrznego (ABW)

ABW jako jedna z agencji odpowiedzialnych za bezpieczeństwo wewnętrzne kraju prowadzi działania związane z kontrwywiadem i bezpieczeństwem informacyjnym, w tym w obszarze cyberbezpieczeństwa.

Warto podkreślić, że w Polsce dynamicznie postępuje rozwój struktur, które zajmują się bezpieczeństwem cyberprzestrzeni, a współpraca międzyinstytucjonalna staje się coraz bardziej istotna w reagowaniu na współczesne zagrożenia cybernetyczne. Aktualne informacje dotyczące tych instytucji można uzyskać z oficjalnych źródeł i stron internetowych odpowiednich organów.

Bibliografia

- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 2024 r. poz. 17 t.j. z późn. zm).
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U.2024.0.37 t.j. z późn. zm.).
- Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. 2023 r. poz. 2488 t.j. z późn. zm.) .
- Ustawa z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz.U. 2022 r. poz. 1700 z późn.zm.).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 r. poz. 1781 t.j.).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 r. poz. 913 t.j. z późn. zm.) .
- Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 poz. 728 t.j.).
- *Metodyka postępowania organów ścigania województwa śląskiego w zakresie zwalczania cyberprzestępczości, w tym przestępstw popełnianych na szkodę banków*, praca zbiorowa, Wydział do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Katowicach, Katowice 2021.
- Protokół o zapobieganiu, zwalczaniu oraz karaniu za handel ludźmi, w szczególności kobietami i dziećmi, uzupełniający Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęty przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r. (Dz.U. 2005 r. nr 18 poz. 160 t.j.).
- Prokuratura Krajowa, Departament do spraw Przestępczości Gospodarczej (2021), nr 1001-7.024.6.202, 20 grudnia 2021 r.
- Prokuratura Krajowa, Departament do spraw Przestępczości Gospodarczej (2022), nr 1001-7.024.2.202, 10 stycznia 2022 r.
- Wytyczne nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów (Dz.Urz.KGP z 2017 r. poz. 59 z późn. zm.).
- NIK. (2022). Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych w tym kradzieży tożsamości. Informacja o wynikach kontroli. Nr ewid. 125/2022/P/21/042/KPB Warszawa.

Strony internetowe

- *6 rodzajów cyberprzestępstw, przed którymi możesz uchronić swoją firmę*, https://cyberware.pl/6-rodzajow-cyberprzestepstw-przed-ktorymi-mozesz-uchronic-swoja-firme, dostęp 28.04.2024 r.
- *Darknet: ciemna strona Internetu*, https://www.komputerswiat.pl/artykuly/redakcyjne/czym-jest-ciemna-strona-internetu-i-jak-sie-do-niej-dostac/qxt9m3y, dostęp 21.04.2024 r.
- *Europol*, https://www.europol.europa.eu/about-europol:pl, dostęp 21.04.2024 r.
- *Interpol – Międzynarodowa Organizacja Policji*, https://antykorupcja.gov.pl/ak/import/instytucje-zaangazowane/3681,Interpol-Miedzynarodowa-Organizacja-Policji.html, dostęp 21.04.2024 r.
- Krasnopolska W., *Przygotowanie i wdrożenie metodyki z zakresu pozyskiwania i przetwarzania informacji oraz komunikacji przy realizacji zadań prokuratury z wykorzystaniem systemu informatycznego PROK-SYS*, Prokuratura Krajowa 2 stycznia 2023 r. https://www.gov.pl/web/prokuratura-krajowa/przygotowanie-i-wdrozenie-metodyki-z-zakresu-pozyskiwania-i-przetwarzania-informacji-oraz-komunikacji-przy-realizacji-zadan-prokuratury-z-wykorzystaniem-systemu-informatycznego-prok-sys, dostęp 28.04.2024 r.
- *NASK – Naukowa i akademicka sieć komputerowa. Kim jesteśmy*, https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html, dostęp 21.04.2024 r.
- Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik policyjny nr 4/2017 https://kwartalnik.csp.edu.pl/kp/archiwum-1/2017/nr-42017/3730,-Cyberprzestepczosc-proba-diagnozy-zjawiska.html), dostęp 21.04.2024 r.

Zakład Służby Kryminalnej

podkom. Barbara Baran
podkom. Natalia Karpuk
asp. Grzegorz Szokiel

Szkoła Policji w Katowicach
ul. gen. Jankego 276
40-684 Katowice-Piotrowice
www.katowice.szkolapolicji.gov.pl