ZWALCZANIE CYBERPRZESTĘPCZOŚCI

przez polską Policję

nadkom. Mariusz Tomczak

radca Wydziału Wywiadu Kryminalnego
Centralne Biuro Zwalczania Cyberprzestępczości

Cyberprzestępczość, w jej różnych formach, stanowi od wielu już lat rosnące zagrożenie dla bezpieczeństwa globalnego. By uświadomić sobie skalę tego fenomenu, wystarczy tylko przytoczyć dane statystyczne komórki Internet Crime Complaint Center Federalnego Biura Śledczego Stanów Zjednoczonych (FBI), które wskazują, że liczba zgłoszeń w tym obszarze osiągnęła wartość 800 944 w 2022 r., w porównaniu do 351 937 takich zdarzeń w 2018 r. Cechą charakterystyczną tego zjawiska, obok niespotykanej dynamiki wzrostu, jest szerokie spektrum zagrożeń (np. cyberataki, rozpowszechnianie on-line treści pornograficznych z udziałem dzieci, oszustwa online i wiele innych), a także bardzo często niezwykle złożona konstrukcja przestępstw.

Tworzenie struktur zwalczania cyberprzestępczości w Polsce i w Europie

W Polsce, w ujęciu historycznym, cyberprzestępczość długo nie była postrzegana jako oddzielny obszar zagrożeń, wymagający dedykowanego podejścia. Zagrożenia tego typu były klasyfikowane jako zdarzenia w obrębie przestępczości gospodarczej. W rezultacie były zwalczane przez komórki pionu przestępczości gospodarczej w Policji. Ponadto wszelkie incydenty związane z wykorzystaniem narzędzi cyfrowych były raczej traktowane jako pewien czynnik ułatwiający popełnianie przestępstw, a więc jako element szerszej perspektywy. Z czasem jednak świadomość organów ścigania dotycząca odrębności cyberprzestępczości i jej rosnącej skali zaczęła się zwiększać, prowokując tworzenie zalążków struktur zajmujących się tymi zagrożeniami. Pierwszym tego zwiastunem było wypracowanie, zaakceptowanej przez Komendanta Głównego Policji „Koncepcji technicznego wsparcia zwalczania cyberprzestępczości". Na podstawie tego dokumentu powołano w czerwcu 2007 r., w strukturze Biura Kryminalnego Komendy Głównej Policji, Sekcję Wsparcia Zwalczania Cyberprzestępczości. Do zadań tej komórki należało przede wszystkim monitorowanie cyberzagrożeń, wdrażanie zaawansowanych narzędzi, służących zwalczaniu cyberprzestępczości, a także wspieranie funkcjonariuszy w całym kraju, w przypadku skomplikowanych spraw związanych z wykorzystaniem technologii informatycznych. W następnych latach ranga tego zagadnienia nieustannie rosła, znajdując odzwierciedlenie w kolejnych zmianach organizacyjnych. Wymusiło to podjęcie strategicznej decyzji o utworzeniu zupełnie nowej struktury, która uzyskała scentralizowany i w dużym stopniu samodzielny wymiar w obszarze zwalczania cyberprzestępczości. W efekcie w dniu 12 stycznia 2022 r. zostało utworzone Centralne Biuro Zwalczania Cyberprzestępczości (CBZC).

Wspomniane procesy adaptacyjne do zagrożeń w cyberprzestrzeni zostały również podjęte, znacznie wcześniej, na poziomie europejskim. Wiodącą rolę w tym zakresie pełni Agencja Unii Europejskiej do spraw Współpracy Organów Ścigania (Europol). To właśnie w strukturze tej Agencji w styczniu 2013 r. utworzono Europejskie Centrum ds. Cyberprzestępczości (EC3, European Cy-

bercrime Center). Rolą Centrum jest wspieranie państw członkowskich UE oraz państw trzecich w zwalczaniu zaawansowanych form cyberprzestępczości o zasięgu globalnym. Podobna współpraca realizowana jest także na forum Międzynarodowej Organizacji Policji Kryminalnych (INTERPOL). W ramach tej organizacji również funkcjonuje Centrum ds. Cyberprzestępczości (**Cybercrime Directorate**). Polskie organy ścigania, w tym w szczególności CBZC, ściśle współpracują ze wspomnianymi organizacjami.

Katalog cyberprzestępstw

Jak zostało to zasygnalizowane we wstępie, cyberprzestępczość stanowi w istocie szeroki katalog zagrożeń, których wspólnym mianownikiem jest wykorzystanie technologii cyfrowych jako narzędzia popełnienia przestępstwa bądź też potraktowanie środowiska cyfrowego jako celu przestępstwa. Poniżej wymieniono najpoważniejsze obecnie zagrożenia w tym obszarze.

Ataki i oszustwa motywowane finansowo, bądź ukierunkowane na kradzież danych

- **Phishing** – metoda, w której cyberprzestępcy próbują uzyskać poufne informacje, takie jak nazwy użytkowników, hasła i dane kart kredytowych, imitując zaufane podmioty w komunikacji elektronicznej.
- **Ransomware** – złośliwe oprogramowanie, które szyfruje pliki ofiary; atakujący żąda następnie okupu od ofiary w zamian za przywrócenie dostępu do danych po dokonaniu płatności.
- **Hacking** – nieautoryzowany dostęp do systemów komputerowych lub sieci; hakerzy mogą wykorzystywać luki w systemie do kradzieży, modyfikacji lub niszczenia danych.
- **Kradzież tożsamości** – kradzież danych osobowych w celu popełnienia oszustwa, takiego jak dokonywanie nieautoryzowanych zakupów lub otwieranie nowych kont na nazwisko ofiary.
- **Oszustwa internetowe** – różnorodne schematy przestępcze realizowane w sieci Internet w celu oszukania osób, tak aby przekazały pieniądze, dane osobowe lub inne wartościowe aktywa. Tego rodzaju przestępstwami są oszustwa metodą „na pracownika banku", „na policjanta" i „na prokuratora", gdzie sprawcy, wykorzystując m.in. metody socjotechniczne, uzyskują od swoich ofiar dane dostępowe do kont bankowych bądź też prowokują je do transferów pieniężnych.
- **Oszustwa inwestycyjne** – oszustwa, które polegają na wyłudzaniu środków poprzez nakłonienie ofiary do udziału w inwestycjach kapitałowych.
- **Oszustwa metodą Business Email Compromise (BEC) CEO Fraud** – to metoda oszustwa, w której cyberprzestępcy przejmują kontrolę nad firmowymi kontami e-mail lub tworzą bardzo podobne adresy e-mail, aby oszukać pracowników firmy. Atakujący najczęściej podszywają się pod osoby o wysokim statusie w firmie, np. dyrektorów, menedżerów lub dostawców, aby nakłonić ofiary do wykonania nieautoryzowanych przelewów finansowych lub ujawnienia poufnych informacji.
- **Kradzież własności intelektualnej** – kradzież lub używanie cudzej własności intelektualnej (takiej jak oprogramowanie, muzyka, filmy i inne treści cyfrowe) bez zgody właściciela.

Ataki na infrastrukturę i cyberprzestrzeń

- **Cryptojacking** – nieautoryzowane użycie komputera innej osoby do wydobywania kryptowaluty. Zasoby systemu ofiary są wykorzystywane do generowania cyfrowych walut dla atakującego.
- **Ataki hybrydowe –** szczególnie groźne ataki wymierzone w bezpieczeństwo państwa i obejmujące infrastrukturę krytyczną, instytucje publiczne i gospodarcze, a także akty cyberszpiegostwa.
- **Ataki typu DoS (Denial of Service) i DDoS (Distributed Denial of Service)** – ataki przeciążające system, sieć lub stronę internetową poprzez generowanie dużego ruchu sieciowego, przez co czynią te systemy i usługi niedostępnymi dla użytkowników.

Działania szkodliwe dla osób i społeczności

- **Cyberstalking** – wykorzystywanie sieci Internet lub innych środków elektronicznych do nękania lub prześladowania osoby, grupy osób lub organizacji.
- **Wykorzystywanie dzieci** – wykorzystywanie sieci Internet do produkcji oraz dystrybucji treści pornograficznych z udziałem małoletnich.
- **Inżynieria społeczna (Social Engineering)** – manipulowanie ludźmi w środowisku cyfrowym poprzez wykorzystanie narzędzi socjotechnicznych w celu sprowokowania ich do określonych zachowań bądź przyjęcia fałszywych informacji lub ujawnienia informacji poufnych.

Charakterystyka współczesnej cyberprzestępczości

W rzeczywistości jednak cyberprzestępczość to bardzo skomplikowana struktura powiązań i zależności, która przyjmuje cechy dojrzałego rynku, oferującego potężny zakres usług przestępczych i generującego ogromne dochody finansowe. W praktyce cyberprzestępstwa stanowią wieloetapowe i niezwykle złożone przedsięwzięcia, które obejmują wiele kroków, np. od początkowego włamania do systemu po wykradanie danych, przy udziale różnych aktorów na różnych etapach tego procesu.

W rezultacie usługi cyberprzestępcze stanowią obecnie profesjonalny rynek, charakteryzujący się wysoką specjalizacją i strukturą współpracy. Dostępne są usługi, takie jak brokery dostępu początkowego (Initial Access Broker) i droppery (programy służące do dostarczenia złośliwego oprogramowania do urządzenia końcowego), które są kluczowe dla ataków ransomware i oszustw, i zapewniają monitorowanie i dostarczanie złośliwego oprogramowania. Ponadto dostępne są wyspecjalizowane metody ukrywania, takie jak cryptery i usługi przeciwko oprogramowaniu antywirusowemu (CAV), które pomagają ukryć złośliwe działania i unikać wykrycia przez programy antywirusowe. Przestępcy również używają sieci VPN (Virtual Private Networks) do maskowania swojej tożsamości i lokalizacji. Narzędzia te wymagają infrastruktury odpornej na zakłócenia i infiltrację ze strony organów ścigania. Niektórzy dostawcy usług internetowych (Internet Service Providers) i dostawcy hostingu, często używani przez przestępców, nie prowadzą szeroko zakrojonego monitoringu i nie przestrzegają prawnych

wniosków o informacje. Popularny jest w tym przypadku Bulletproof, czyli usługa hostingu internetowego, odporna na skargi dotyczące nielegalnych działań i służąca przestępcom jako podstawowy budulec do usprawnienia różnych cyberataków.
Obrona przed cyberprzestępczością jest tak silna, jak najsłabsze ogniwo, którym często jest czynnik ludzki. Wiadomości phishingowe, złośliwe pliki, techniki socjotechniczne i nieaktualizowane oprogramowanie stanowią najczęstsze punkty wejścia do systemu dla cyberprzestępców. Metody socjotechniczne, a w szczególności phishing, są szeroko stosowane do manipulowania ludźmi w celu ujawnienia poufnych informacji. Ponieważ regulacje UE utrudniły oszustwa z użyciem kart płatniczych, przestępcy coraz częściej skupiają się na użytkownikach. W rezultacie phishing pozostaje główną metodą oszustw online i ataków złośliwego oprogramowania.
Wykorzystanie fałszywych tożsamości jest również powszechne w kontekście seksualnego wykorzystywania małoletnich w sieci, gdzie przestępcy na szeroką skalę korzystają z mediów społecznościowych. Ponadto powszechne stały się oszustwa związane z działalnością charytatywną, wykorzystujące kryzysy, takie jak pandemia COVID-19, inwazja Rosji na Ukrainę czy klęski żywiołowe. Kolejne zagrożenie to spoofing, czyli technika stosowana do zdobycia zaufania ofiar poprzez fałszowanie identyfikatorów dzwoniących. Oszustwa online dotyczą również manipulowania systemami płatności. Złośliwe oprogramowanie może być instalowane w bankomatach, aby wypłacać pieniądze lub przejmować systemy płatności cyfrowych w celu kradzieży danych kart poprzez tzw. digital skimming.
Głównym towarem w kontekście cyberprzestępczości są skradzione dane. Dane te, uzyskane poprzez skompromitowane bazy danych i techniki socjotechniczne, są sprzedawane na nielegalnym rynku. Przestępcy seksualni wykorzystują natomiast informacje wrażliwe do szantażu. Ponadto skradzione dane wspierają liczne, pozostałe działania przestępcze, w tym np. szpiegostwo i wymuszenia.
Dobrym przykładem rozwoju rynku usług przestępczych jest jedno z największych forów hakerskich RaidForums, służące do handlu skradzionymi danymi, które zostało zamknięte w kwietniu 2022 r. Bez wątpienia, skradzione dane napędzają oszustwa przeciwko systemom płatności i kradzież tożsamości. Rozwój ekosystemu handlu danymi zwiększył zagrożenie przejęcia konta (ATO, Account Takeover Fraud), które polega na nielegalnym uzyskaniu przez przestępców dostępu do kont online w celu osiągnięcia korzyści finansowych lub dalszego handlu danymi. ATO stało się łatwiejsze dzięki dostępności dedykowanych narzędzi.
Ogromną rolę w ułatwianiu funkcjonowania rynku związanego z cyberprzestępczością odgrywa środowisko tzw. ciemnego Internetu (Darknet). Fora w tej sieci są intensywnie wykorzystywane przez cyberprzestępców do komunikacji, wymiany wiedzy i doświadczeń, handlu cyfrowymi aktywami, a także rekrutowania specjalistów. W szczególności grupy hakerskie korzystają z tychże forów do rekrutowania wszelkiego rodzaju specjalistów, których można zaangażować na poszczególnych etapach schematu przestępczego. Przestępcy seksualni używają natomiast forów do nawiązywania kontaktów, dzielenia się wiedzą i wymiany materiałów przedstawiających wykorzystywanie seksualne dzieci (CSAM – *Child Sexual Abuse Material*).
Na tych platformach sprzedawane są różne usługi przestępcze, w tym skradzione dane i usługi typu „crime-as-a-service". Fora dostarczają informacji na temat bezpieczeństwa operacyjnego (OpSec), metod oszustw, wykorzystywania dzieci, prania pieniędzy, phishingu i złośliwego oprogramowania. Informacje i wskazówki dotyczące operacji na rynkach dark web są powszechnie dostępne. Niemniej jednak działania organów ścigania i ataki DDoS spowodowały niestabilność na tych rynkach, co doprowadziło do zamknięcia kilku znanych platform w ostatnich latach.

Struktura i zadania CBZC

CBZC stanowi obecnie wiodącą jednostkę Policji w zakresie zapobiegania i zwalczania cyberprzestępczości. Biuro ma charakter scentralizowany. Oznacza to że na poziomie centralnym funkcjonuje kierownictwo oraz wydziały i zarządy centralne. Ponadto w każdym województwie funkcjonują zarządy i wydziały terenowe.
Podstawę działalności Biura określają przepisy prawne, takie jak ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz. U. poz. 2447, z późn. zm.) oraz Regulamin Centralnego Biura Zwalczania Cyberprzestępczości z dnia 14 maja 2024 r. CBZC wypełnia swoje zadania statutowe poprzez podejmowanie działań na rzecz zapewnienia bezpieczeństwa publicznego, będąc tym samym jednostką organizacyjną Policji służącą zwalczaniu cyberprzestępczości. CBZC odpowiedzialne jest za realizację na obszarze całego kraju zadań w zakresie:

- rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw;
- wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw.

Biuro koncentruje się przede wszystkim na zwalczaniu najbardziej zaawansowanych i zorganizowanych form cyberprzestępczości, natomiast w ujęciu globalnym przestępstwa tego rodzaju, w szczególności o mniejszej skali i stopniu skomplikowania, są również zwalczane przez pozostałe jednostki Policji. Ponadto ważną rolą CBZC jest wyznaczanie właściwych standardów i dobrych praktyk w zakresie prowadzenia spraw w obszarze cyberprzestępczości, a także identyfikowanie i wypracowanie odpowiedniej strategii wobec zupełnie nowych zagrożeń, najczęściej związanych z pojawieniem się nowych, przełomowych technologii (np. ChatGPT – technologia przetwarzania języka naturalnego oparta na wykorzystaniu sztucznej inteligencji, mająca na celu naśladowanie ludzkiej konwersacji).
Przedmiotem działania CBZC jest w szczególności zwalczanie dwóch grup przestępstw. Pierwsza grupa to przestępstwa, które można popełnić tylko z wykorzystaniem technologii informatycznych, tj. hacking, ransomware,

ataki DDoS, malware, bulletproof hosting. Druga grupa obejmuje przestępstwa, które można popełnić także z wykorzystaniem technologii cyfrowych, np. oszustwa internetowe, prowadzenie sklepów internetowych z nielegalnym towarem, oszustwa phishingowe i oszustwa inwestycyjne. Obok wspomnianych powyżej grup ważnym obszarem jest również zwalczanie produkcji i dystrybucji treści pornograficznych z udziałem małoletnich.

W ujęciu merytorycznym metodyka działania CBZC w obszarze zapobiegania i zwalczania cyberprzestępczości opiera się na kilku podstawowych filarach. Zaliczamy do nich:

- prowadzenie spraw operacyjnych i postępowań przygotowawczych;
- monitorowanie i analiza cyberprzestępczości w ujęciu statystycznym oraz w zakresie identyfikowanych trendów, w tym analiza transakcji z wykorzystaniem kryptowalut;
- informatyka śledcza;
- realizacja programów zapobiegania przestępczości i kampanii profilaktycznych;
- reagowanie na nagłe incydenty w sieci, w szczególności związane z zagrożeniem życia i zdrowia ludzkiego;
- współpraca międzynarodowa organów ścigania.

Działalność CBZC w 2023 r. w liczbach

W celu zobrazowania skali działania CBZC warto zapoznać się z podstawowymi danymi statystycznymi, które wskazują, że tylko w 2023 r. Biuro prowadziło 617 postępowań przygotowawczych. Ponadto zatrzymano 501 osób oraz zabezpieczono mienie w wysokości ponad 441 000 000 PLN. W obszarze informatyki śledczej dokonano zabezpieczenia danych z 2500 telefonów komórkowych, sporządzono 808 analiz danych z telefonów komórkowych i 1331 analiz dysków, wykonano 1000 kopii binarnych oraz zabezpieczono 2000 TB materiału dowodowego. Ponadto udzielono wsparcia (w szczególności technicznego) w ramach 440 spraw prowadzonych przez pozostałe jednostki Policji. Przy czym wsparcie obejmowało także analizy w zakresie transakcji kryptowalutowych, jak również działalność szkoleniową w zakresie wybranych aspektów zwalczania cyberprzestępczości. W obszarze reagowania na nagłe incydenty zrealizowano 2380 spraw związanych z zagrożeniem życia i zdrowia ludzkiego, w ramach których ustalono 2303 osoby, z czego 1887 osób wymagało hospitalizacji bądź przekazano je pod opiekę najbliższych.

Współpraca międzynarodowa

Istotnym elementem, bez którego nie byłoby możliwe skuteczne zwalczanie cyberprzestępczości, jest międzynarodowa współpraca organów ścigania. Obecnie najbardziej kluczowe znaczenie ma współpraca ze wspomnianymi wcześniej instytucjami, tj, Europolem i Interpolem.

W ramach współpracy z Europolem realizowany jest szereg poważnych spraw operacyjnych o charakterze międzynarodowym, w które zaangażowane są także inne państwa członkowskie UE. W celu zoptymalizowania tej współpracy CBZC jest także członkiem specjalnej grupy zadaniowej państw członkowskich przy Europolu J-CAT, która skupia oficerów łącznikowych na co dzień zajmujących się koordynacją współpracy w ramach wspólnych spraw w obszarze cyberprzestępczości.

CBZC jest ponadto uczestnikiem operacji realizowanych pod egidą Interpolu. Organizacja ta oferuje wiele zaawansowanych narzędzi i form współpracy ułatwiających zwalczanie cyberprzestępczości. Współpraca z Interpolem jest szczególnie cenna z uwagi na zasięg geograficzny, obejmujący wszystkie kontynenty. Ponadto Interpol zapewnia ogromne wsparcie i wiedzę w zakresie wykorzystania najnowszych technologii do celów przestępczych. CBZC było m.in. uczestnikiem Grupy ds. Metaverse[1], która na przełomie lat 2023 i 2024 opracowała raport dotyczący przestępczości w światach wirtualnych metaverse i metodyki działania organów ścigania w metaverse.

Współpraca międzynarodowa to jednak nie tylko wspomniane powyżej organizacje i agencje, ale także wiele innych narzędzi i regulacji ułatwiających współpracę organów ścigania. Najlepszym tego przykładem jest Konwencja Budapesztańska, która stanowi potoczną nazwę Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r., obowiązującej w Polsce od 1 czerwca 2015 r. (Dz. U. z 2015 r. poz. 728). Jej celem jest poprawa współpracy międzynarodowej związanej ze zwalczaniem cyberprzestępczości m.in. poprzez przyjęcie wspólnej terminologii, określenia czynów, które uznawane będą za przestępstwa (art. 2–11 konwencji), określenie zasad współpracy pomiędzy państwami ratyfikującymi konwencję i ujednolicenie ich systemów prawnych, np. w zakresie zabezpieczania przed utraceniem danych teleinformatycznych (tzw. mrożenie danych, art. 16 i 29 konwencji) oraz przekazywanie informacji z własnej inicjatywy (art. 26 konwencji).

Konwencja budapesztańska daje podstawy do zabezpieczania danych informatycznych w firmach działających na terenie innych państw, które ratyfikowały konwencję. Zgodnie z jej zapisami **mrożenie następuje na okres dziewięćdziesięciu dni (90 dni)**, od daty, kiedy „nakaz mrożenia danych" za pośrednictwem partnera zagranicznego otrzyma firma, od której chcemy uzyskać dane. W przepisach konwencji znajduje się zapis o możliwości przedłużenia przedmiotowego nakazu o kolejne dziewięćdziesiąt dni (90 dni). Wnioski o mrożenie danych przesyłamy tylko do spraw procesowych.

Bardzo ważnym aspektem w kontekście skutecznego zwalczania cyberprzestępczości jest współpraca w zakresie wymiany informacji z dostawcami usług internetowych (Internet Service Providers), a w szczególności z globalnymi graczami (np. Google, Meta, X itp.). Uzyskiwanie informacji na potrzeby prowadzonych postępowań i spraw operacyjnych może odbywać się w różnoraki sposób. Najszybciej uzyskiwane są informacje poprzez zapytania bezpośrednie (za pomocą interaktywnych formularzy dostawców usług) oraz z wykorzystaniem międzynarodowych policyjnych kanałów wymiany informacji (np. aplikacja wymiany informacji SIENA, udostępniana przez Europol). Przy czym tą drogą uzyskujemy tylko podstawowe informacje (tzw. Basic Subscriber Information, czyli np. dane rejestracyjne i „wykazy logowań"). Nie uzyskamy natomiast treści wiadomości (tzw. content). W takim przypadku konieczne jest wystąpienie z międzynarodową pomocą prawną.

Kierunki rozwoju CBZC

Z uwagi na fakt, że środowisko cyfrowe i technologie informatyczne podlegają gwałtownemu rozwojowi, ta sama prawidłowość ma również zastosowanie do cyberprzestępczości. Wymusza to ciągły rozwój i adaptację instytucji zwalczających to zjawisko. W rezultacie priorytetem CBZC na najbliższe lata jest ewoluowanie Biura w kierunku jednostki zaawansowanej technologicznie i organizacyjnie, która skutecznie zapobiega i zwalcza najbardziej zaawansowane formy cyberprzestępczości.
Najważniejsze priorytety obejmują:

- rozpoznawanie cyberprzestępczości przez budowanie przestrzeni cyberbezpieczeństwa oraz właściwej komunikacji wraz z zaangażowaniem społeczeństwa w zakresie przeciwdziałania cyberprzestępczości – działalność prewencyjna i komunikacyjna za pośrednictwem dostępnych kanałów, a także współpraca międzyinstytucjonalna,
- zoptymalizowanie pracy operacyjnej i procesowej w ramach CBZC – wypracowanie jednolitych, wystandaryzowanych w skali całego Biura wzorców realizacji spraw, w wymiarze operacyjnym i procesowym,
- zacieśnienie współpracy z krajowymi podmiotami publicznymi i prywatnymi oraz instytucjami międzynarodowymi,
- gromadzenie informacji w zakresie danych dotyczących cyberprzestępczości – pełnienie roli hubu informacyjnego w zakresie cyberprzestępczości w celu budowania pełnego obrazu zjawiska, w kontekście jego charakterystyk, a w efekcie traktowania tego jako fundamentu przyszłych, ukierunkowanych działań,
- wdrażanie i rozwijanie nowoczesnych technologii i innowacji – rozwijanie bądź pozyskiwanie najnowszych technologii wspierających zwalczanie cyberprzestępczości i przetwarzanie dużych zbiorów danych,
- stałe podnoszenie kompetencji funkcjonariuszy i pracowników CBZC w zakresie zwalczania cyberprzestępczości oraz w zakresie cyberprofilaktyki, **a także realizowanie podobnych szkoleń dla pozostałych funkcjonariuszy i pracowników w Policji.**

Przykłady operacji CBZC

Likwidacja i zajęcie infrastruktury przestępczej „EXCLU CHAT"

Policjanci CBZC w ramach międzynarodowej operacji z udziałem organów ścigania z Niemiec i Holandii, a także przy wsparciu Eurojustu i Europolu zlikwidowali infrastrukturę służącą do działalności przestępczej, poprzez wyłączenie szyfrowanego komunikatora Crypto-Messenger Exclu. Funkcjonariusze CBZC wraz z niemieckimi kolegami oraz przy pomocy pracowników Państwowego Instytutu Badawczego NASK dokonali 6 przeszukań na terenie RP. Równocześnie realizowane były przeszukania na terenie Niemiec, Holandii i Belgii. W realizacji na terenie Niemiec brał udział funkcjonariusz CBZC odpowiedzialny za koordynację działań. Policja holenderska przeprowadziła 79 przeszukań, zatrzymano 42 osoby, ujawniono dwa laboratoria narkotykowe oraz palarnię kokainy, zabezpieczono znaczne ilości narkotyków i ponad 4 mln euro w gotówce. Przejęta aplikacja używana była do wymiany informacji w zakresie handlu narkotykami i bronią palną w znacznych ilościach. Funkcjonariusze CBZC w wyniku przeprowadzonych czynności zabezpieczyli 6 serwerów o pojemności 30 TB, 32 sztuk pamięci masowej o pojemności 30 TB oraz inny sprzęt wykorzystywany do popełniania przestępstw. W wyniku operacji Policji serwis nie jest już dostępny[2].

Operacja „POWER OFF”

Policjanci CBZC we współpracy z Prokuraturą Okręgową w Bydgoszczy zatrzymali 2 osoby zajmujące się wytwarzaniem i udostępnianiem płatnej usługi do przeprowadzania ataków DDoS. Korzystanie z usługi możliwe było po dokonaniu opłaty w kryptowalucie. Przeprowadzane cyberataki w istotny sposób zakłócały pracę systemów informatycznych ulokowanych na terenie całego świata. Usługa ta funkcjonowała od 2013 r. i została skutecznie zablokowana w ramach międzynarodowej operacji „Power Off”.
Operacja prowadzona była przy ścisłej współpracy z Europolem, FBI, policją Holandii, Niemiec i Belgii oraz koordynowana przez Grupę Zadaniową ds. Cyberprzestępczości J-CAT. W postępowaniu uzyskano dane z serwera sprawców zlokalizowanego w Szwajcarii. Ustalono ponad 35 tys. kont użytkowników, 76 tys. zapisów logowań do platformy i ponad 320 tys. unikalnych adresów IP zaatakowanych serwerów. Ustalono również 11 tys. zapisów dotyczących wykupionych „planów ataku” wraz z adresem e-mail kupującego usługę (na łączną sumę około 400 tys. USD) oraz ponad tysiąc zapisów dotyczących wykupionych „planów ataków” (na łączną sumę około 44 tys. USD).
W ramach przeprowadzonej przez policjantów CBZC realizacji zatrzymano 2 osoby i przeprowadzono 10 przeszukań. Na komputerze jednego z podejrzanych ujawniono i zabezpieczono dowody prowadzenia i administrowania przestępczej domeny. Zabezpieczono sprzęt elektroniczny w postaci 15 twardych dysków, 5 komputerów stacjonarnych i 6 przenośnych, 10 telefonów, 5 pamięci USB, 3 karty SIM oraz wydruk portfela kryptowalutowego z kluczem prywatnym[3].

Podsumowanie

Reasumując, należy podkreślić, że zapobieganie i zwalczanie cyberprzestępczości jest zadaniem niezwykle złożonym, którego nie da się mierzyć miarą właściwą dla zwalczania tradycyjnej przestępczości. Mierzenie się z tym zagrożeniem wymaga bowiem nie tylko ogromnej wiedzy technicznej, ale wiedzy interdyscyplinarnej obejmującej, obok aspektów technologicznych, także zagadnienia społeczne, ekonomiczne, a nawet geopolityczne. Cyberprzestępczość stanowi bowiem pewien horyzontalny system, który przenika wszystkie obszary ludzkiej aktywności. Tak wymagające wyzwanie wymaga podejścia opartego na ciągłym doskonaleniu, uczeniu się i inwestowaniu w odpowiednie narzędzia i metodyki.

[1] Metaverse – wirtualne środowisko on-line, które łączy w sobie rzeczywistość rozszerzoną (świat rzeczywisty łączony z generowanym komputerowo, np. grafika 3D nakładana na obraz z kamery), rzeczywistość wirtualną, rzeczywistość mediów społecznościowych, gier on-line, a także kryptowalut [przyp. red.].
[2] Centralne Biuro Zwalczania Cyberprzestępczości, Aktualności, https://cbzc.policja.gov.pl/bzc/aktualnosci/ [dostęp: 2.07.2024 r.].
[3] Tamże.

Summary

Combating cybercrime by the Polish Police

This article defines the concept of cybercrime, and presents a catalog of the most serious threats in this area. It characterizes contemporary cybercrime and emphasizes that it is a complex phenomenon and already has the character of a “mature market”, which requires law enforcement agencies to have an interdisciplinary approach and makes it difficult to combat. Furthermore, the genesis of the creation of a specialized Polish unit — the Central Cybercrime Bureau — is explained, as well as its tasks, structure, and international cooperation, in particular within the framework of Europol and INTERPOL. An interesting and important addition to the article is data on the evidence secured by the CCB, as well as descriptions of exemplary operations carried out by the Bureau in cooperation with the police of other countries.

Tłumaczenie: Katarzyna Olbryś