KG: Czym jest Centralne Biuro Zwalczania Cyberprzestępczości (CBZC)?

MP: Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) jest jednostką organizacyjną Policji, która działa prawie od 2,5 roku na obszarze całego kraju, ale też współpracuje ze służbami innych państw. Odpowiedzialne jest za realizacje 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 oraz wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw. W skrócie – policjanci CBZC zwalczają cyberprzestępczość.

Funkcjonariusze CBZC mogą prowadzić działania operacyjno – rozpoznawcze oraz dochodzeniowo – śledcze na zasadach wynikających z ustawy o Policji.

Centralnym Biurem Zwalczania Cyberprzestępczości kieruje Komendant Centralnego Biura Zwalczania Cyberprzestępczości, który podlega Komendantowi Głównemu Policji.
W skład CBZC wchodzą komórki organizacyjne – zarządy, wydziały i zespoły. W każdym mieście wojewódzkim jest komórka CBZC w randze wydziału lub zarządu.

KG: Czy pracuje u Was dużo kobiet?

MP: Na dzień dzisiejszy (27 grudnia) w CBZC na 777 funkcjonariuszy pracuje 168 policjantek. Pamiętajmy jednak, że w policji są również pracownicy cywilni – na 36 pracowników, 30 to kobiety.

KG: Jakie wykształcenie i kompetencje trzeba mieć żeby zostać funkcjonariuszem CBZC i jak wygląda proces rekrutacyjny?

MP: W głównej mierze od kandydatów wymagana jest wiedza informatyczna, wiedza na temat nowoczesnych technologii teleinformatycznych. Procedura kwalifikacyjna dla osób ubiegających się o przyjęcie do służby w Policji w Centralnym Biurze Zwalczania Cyberprzestępczości nie zawiera testu sprawności fizycznej oraz testu wiedzy ogólnej – tak, jak to jest podczas przyjęcia się ogólnie do służby.
Postępowanie kwalifikacyjne do CBZC składa się z kilku etapów. Najpierw kandydaci podchodzą do testu z wiedzy i umiejętności z zakresu informatyki i języka obcego. Następnie przechodzą badanie psychologiczne i badanie psychofizjologiczne. Kolejnym etapem jest rozmowa kwalifikacyjna i komisja lekarska. Przed przystąpieniem do służby kandydat przechodzi również postępowanie sprawdzające.

KG: Jak wygląda typowy dzień policjanta Centralnego Biura Zwalczania Cyberprzestępczości?

MP: Dużą rolę stawiamy na pracę operacyjną. Nie mogę zdradzić, jak od kuchni wyglądają ich działania, ale mogę powiedzieć, że ich praca ma ogromne znaczenie w zwalczaniu cyberprzestępczości. Nie ma dwóch takich samych dni. Jednego dnia, z potrzeby służby, pracuje się za

biurkiem, innego wyjeżdża w teren na różne czynności, np. obserwacje, bądź zatrzymanie przestępców.
Policjanci CBZC monitorują sieć Internet, dzięki czemu ujawniają i zapobiegają przestępstwom w cyberprzestrzeni. Analizują sposoby działania sprawców, identyfikują je i zbierają materiał dowodowy, żeby na końcowym etapie zatrzymać cyberoszustów. Narzędzia i metody pracy operacyjnej zawsze są dostosowywane do danej sprawy. Warto też zaznaczyć, że specyfika tej pracy wymaga dyspozycyjności 24 godziny na dobę i często polega na współpracy z innymi jednostkami, także spoza naszego kraju.
Policjanci CBZC w wyniku pracy operacyjnej, przejmują inicjatywę wszczęcia postępowania przygotowawczego, nie czekają na złożone zawiadomienie, bo wtedy często jest już po prostu za późno, ponieważ oszuści mogą przejąć nasze konta.

KG: Jakie rodzaje cyberprzestępstw są do Was najczęściej zgłaszane?

MP: Przede wszystkim musimy powiedzieć o tym, że powinno się zgłaszać przestępstwa i to jak najszybciej – w najbliższej jednostce policji.
Zajmujemy się zwalczaniem przestępstw w cyberprzestrzeni na dużą skalę. To są sprawy duże, ciężkie i trudne technicznie. W wyniku często długoterminowej pracy, rozbijamy całe grupy przestępcze. Zatrzymujemy sprawców przestępstw, którzy wyrządzili szkodę na setki tysięcy, a nawet w milionach złotych. To sprawy o dużym kalibru. I takie właśnie do nas trafiają. Pamiętajmy, że każde (drobne i większe) oszustwo można zgłosić w najbliższej jednostce policji.
Na naszej stronie internetowej (https://cbzc.policja.gov.pl/bzc/zglos-cyberprzestepstwo/464,Zglos-cyberoszustwo.html) umieściliśmy algorytm postępowania, w którym szczegółowo opisaliśmy, co zrobić, gdy zostaniemy oszukani, jak zgłosić CYBERoszustwo i co potrzebne będzie przy zgłoszeniu zawiadomienia.

KG: Jakie są według Was największe wyzwania w ściganiu cyberprzestępców?

MP: Może zacznę od tego, że przestępcy niestety są o „jeden krok" przed nami. Gdyby tak nie było, to nie byłoby cyberprzestępczości. Możemy jednak śmiało dodać, że depczemy im po piętach. Przestępcy robią wszystko, żeby nie dać się złapać – wymyślają coraz to nowe sposoby na oszustwa w cyberprzestrzeni. Codziennym wyzwaniem dla nas (policjantów) jest to, żeby nie odstawać od nich „na drugi" i „dalszy krok", tzn., żeby cały czas czuli nasz oddech na plechach. Policjanci CBZC systematycznie szkolą się pod kątem cyberprzestępczości. Każdego dnia zdobywają wiedzę i nabierają nowe umiejętności, właśnie po to, żeby skutecznie zwalczać cyberprzestępczość.

KG: Jakie działania podejmujecie, aby zapobiegać cyberprzestępczości? Jakie działania skierowane do obywateli prowadzicie?

MP: Na co dzień działamy, aby zapobiegać cyberprzestępczości. Samo to, że jesteśmy widoczni w social mediach, sprawia, że docieramy z informacjami do setek osób. Często umieszczamy informacje profilaktyczne, które przede wszystkim uświadamiają. W ten sposób zapobiegamy oszustwom, a wiadomo, że „lepiej zapobiegać, niż leczyć".

W social mediach i na naszej stronie internetowej umieszczamy komunikaty dotyczące naszych realizacji – zatrzymań osób, a nawet całych grup przestępczych. Mieliśmy już kilka takich dużych spraw. Jedną z nich była operacja ENOLA GAY, w wyniku której zatrzymano 75 osób podejrzanych o posiadanie, rozpowszechnianie i produkowanie materiałów przedstawiających seksualne wykorzystanie małoletnich osób.

Inną dużą realizacją była międzynarodowa współpraca CBZC z organami ścigania Ukrainy, która pozwoliła na likwidację infrastruktury fałszywych platform inwestycyjnych na terenie Charkowa. Była

to likwidacja biura Call Center, którego pracownicy dokonywali oszustw na szkodę obywateli Rzeczypospolitej Polskiej.

Jeszcze inną dużą sprawą było rozbicie dwóch zorganizowanych grup przestępczych. Jedna z grup zajmowała się udostępnianiem cyberprzestępcom z całej Polski infrastruktury informatycznej, umożliwiającej dokonywanie oszustw przez podsyłanie linków do fałszywych ogłoszeń sprzedaży sprzętu elektronicznego, a druga oszukiwała, wysyłając wiadomości od rzekomych członków rodziny z prośbą o zapłatę zaległych rachunków. W wyniku tych działań, 26 osób usłyszało 224 zarzuty karne za kierowanie i udział w grupie przestępczej, pranie pieniędzy i oszustwa.

To są przykłady tylko z ostatnich miesięcy. Jest tego więcej. A o każdej z tych spraw można poczytać na naszej stronie i w social mediach. Przekazywane przez nas informacje pokazują, że oszuści nie są bezkarni. Takie komunikaty również uświadamiają o zagrożeniach w sieci, ale i ostrzegają przed nimi. To, że niestety ktoś w sieci został oszukany, wcale nie oznacza, że my też mamy dać się oszukać. Wręcz przeciwnie – uczmy się na czyichś błędach i wyciągajmy wnioski. Informując o zagrożeniach społeczeństwo, zwiększamy ich świadomość na temat zagrożeń w sieci oraz wskazujemy na socjotechnikę, którą przestępcy stosują do manipulowania ludźmi.

Warto zwrócić uwagę na to, że ściśle współpracujemy z różnego rodzaju jednostkami i instytucjami. Zależy nam na tym, żeby działać na wielu obszarach i dotrzeć do jak największej liczby osób. Nie tylko my (CBZC) staramy się zapobiegać zagrożeniom w sieci. Dzięki współpracy i ogromnemu zaangażowaniu m.in. NASK – PIB oraz Związku Banków Polskich (ZBP) docieramy do ludzi w każdym wieku. ZBP konsekwentnie dąży do podnoszenia poziomu świadomości klientów w zakresie ochrony przed cyberprzestępstwami. Realizowane wspólne projekty i kampanie znacząco poszerzają widzę dotyczącą cyberbezpieczeństwa. Ważne jest świadome korzystanie z technologii, ale i wyrabianie w sobie poprawnych nawyków.

Jeżeli chodzi o kampanie, to jak najbardziej mamy czym się pochwalić. Np. razem z NASK – PIB w ramach Europejskiego Miesiąca Cyberbezpieczeństwa przygotowaliśmy kampanię informacyjną poświęconą osobom wykorzystywanym do prania pieniędzy, tzw. „mułom finansowym". Przy współpracy z NASK powstał webinar, dzięki któremu mogliśmy jeszcze lepiej przybliżyć wskazany problem społeczeństwu.

W innej kampanii wzięły udział trzy instytucje: NASK – PIB, Warszawski Instytut Bankowości i my – CBZC. Łącząc siły, przygotowaliśmy kompleksowy poradnik „#Halo! Tu cyberbezpieczny Senior!". Dzięki tej kampanii starsze osoby zyskują wiedzę, która pomaga im bezpiecznie korzystać z Internetu i unikać oszustów internetowych. Wiemy, że wykorzystują oni brak świadomości użytkowników sieci, dlatego chcemy, by seniorzy mieli odpowiednie narzędzia i wiedzę, aby skutecznie chronić się przed internetowymi pułapkami.

Kolejną naszą kampanią jest działanie przy użyciu Google Adds. Dzięki niej, osoby wyszukujące informacje dotyczące ataków DDoS, uzyskują rzetelną i obszerną wiedzę na ten temat, bo po wpisaniu „atak DDoS", jako pierwszy wynik wyszukiwania, wyświetla się strona internetowa przygotowana właśnie przez nas.
Tak, jak mówiłam – mamy się czym pochwalić.

KG: Czym są dla Was najnowsze technologie, narzędzia? Jak wspierają Waszą pracę?

MP: Skuteczna walka z zagrożeniami płynącymi z sieci możliwa jest wyłącznie w warunkach, gdy organy ścigania nie ustępują cyberprzestępcom zarówno w technologii jak i w umiejętnościach. Cyberprzestępczość jest jednym z największych i najbardziej rozwijających się zagrożeń – rozwija się z biegiem czasu, dlatego też policjanci stale szkolą się i kształcą z cyberprzestępczości. Oszuści

wykorzystują wszystkie możliwe sposoby, żeby tylko osiągnąć swój cel. Od socjotechniki, po różnego rodzaju technologie i narzędzia. Daleko nie trzeba szukać. Weźmy pod uwagę chociażby sztuczną inteligencję. Genialna technologia! Przydatna w wielu dziedzinach życia. Poniekąd niestety ułatwiła też działalność oszustom, którzy podszywając się pod znane osoby, sieją dezinformacje lub wyłudzają pieniądze. Przestępcy nie potrzebują najnowszych technologii , ani narzędzi, żeby kogoś oszukać. Wystarczy skutecznie zmanipulować swoją ofiarę. Edukacja społeczeństwa i uświadamianie o zagrożeniach w sieci jest bardzo ważne. Świadomy użytkownik sieci, to bezpieczny użytkownik.

KG: Jakie są najważniejsze wyzwania, które stoją przed Wami?

MP: Oprócz wyzwań w ściganiu cyberprzestępców, warto dodać, że jednym z codziennych wyzwań policjantów CBZC jest właśnie uświadamianie społeczeństwa o zagrożeniach w cyberprzestrzeni. Świadomy zagrożenia użytkownik nie da się tak łatwo oszukać. Wiadomo, że wszystko zależy też od okoliczności – gdy w grę wchodzą emocje, to ciężko jest myśleć racjonalnie. Wtedy też mimo, że mamy wiedzę, to możemy dać się „złapać". Niemal każdego dnia informujemy społeczeństwo w naszych social mediach i stronie internetowej o kolejnych metodach oszustów oraz o wykorzystywanych przez nich sposobach działania. Wiemy, że nawet jeśli nie każdy zobaczy nasz post, czy komunikat, to jest szansa, że tzw. drogą pantoflową, informacja się rozejdzie. Głównym celem policjantów CBZC jest tworzenie bezpieczniejszej cyberprzestrzeni.

KG: Dziękuję za wyczerpujące odpowiedzi. Mam nadzieję, że dzięki Waszym działaniom, a także działaniom innych instytucji, w tym również NASK świadomość cyberzagrożeń będzie stale rosła, a działania cyberprzestępców, będą coraz mniej skuteczne.

MP: Dziękuję!