KURS SPECJALISTYCZNY

w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową

Fot. 1. https://pixabay.com/pl/photos/e-commerce-zakupy-karta-kredytowa-2607114/.

mł. asp. dr Paweł Tomaszewski

Zakład Kryminalny CSP

Skokowy postęp wysoko wyspecjalizowanej technologii sprawia, iż organy ścigania, chcąc nadążyć za wysoko wykwalifikowanymi przestępcami, muszą na bieżąco doskonalić swój warsztat umiejętności i narzędzi. Często działania te pozostają i tak niewystarczające w skali ogólnej, co determinuje powołanie do działania niewielkich etatowo, ale bardzo profesjonalnych jednostek organizacyjnych w strukturach Policji. Taką jednostką jest na przykład Centralne Biuro Zwalczania Cyberprzestępczości.

Pomimo ciągłego dostosowywania metod działania do stale zmieniającej się rzeczywistości, organy ścigania pozostają w tyle za sektorem prywatnym, który błyskawicznie reaguje na wszelkie nowinki rynkowe i techniczne, mając do wykorzystania ogromne budżety korporacyjne. Ponadto wyspecjalizowane branże wolnego rynku mogą sobie pozwolić na wielokrotne przelicytowanie sektora publicznego w zakresie płac, co pozwala im na ściągnięcie najlepszych specjalistów danej branży.

Tam, gdzie pojawiają się ogromne pieniądze, z czasem w sposób naturalny pojawiają się też środowiska przestępcze, które w sposób nielegalny starają się wszelkimi sposobami pozyskać dla siebie część udziałów. W obecnej rzeczywistości cyberświata staje się to paradoksalnie dużo prostsze niż kiedykolwiek w przeszłości. Po pierwsze dlatego, iż osobami organizującymi taki proceder są często osoby posiadające ponadprzeciętne umiejętności, nierzadko zdobyte w czasie uprzedniej pracy dla konkretnych korporacji. Po drugie dlatego, że do popełniania przestępstwa coraz częściej nie jest już potrzebny bezpośredni kontakt z ofiarą, co umożliwia środowisku kryminalnemu sieć Internet czy pośrednictwo w zakupach cy-

frowych platform handlowych wspieranych przez firmy kurierskie.
W lawinie niejawnych zagrożeń pojawia się dla konsumentów nadzieja, że w trosce o ich bezpieczeństwo dostawcy usług świadczonych drogą elektroniczną coraz częściej dostrzegają potrzebę kooperacji z organami ścigania celem ograniczenia liczby zagrożeń, a finalnie dostarczenia także materiału dowodowego przeciwko sprawcom cyberprzestępstw.
Potrzebę bieżącej współpracy między Policją a podmiotami prywatnymi dostrzega także Centrum Szkolenia Policji w Legionowie, organizując cykliczne edycje kursu specjalistycznego w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową[1]. W trakcie niniejszego kursu pogłębiana jest wiedza specjalistyczna funkcjonariuszy prowadzących postępowania dotyczące obszaru cyber. Zajęcia odbywają się we współpracy z pracownikami firm, którzy pomagają organom ścigania w identyfikacji przestępców oraz zabezpieczają materiał dowodowy.
Pierwszym obszarem poruszanym w trakcie kursu jest kwestia sprzedaży podrobionych produktów opatrzonych oryginalnym oznakowaniem znanej marki. W zwalczaniu tego rodzaju przestępczości pośredniczą krajowe kancelarie prawnicze, których zadaniem jest stać na straży znaków towarowych i jakości artykułów dystrybuowanych przez światowych potentatów różnych branż[2].
Przykładem omawianym w ramach zajęć na tym kursie jest między innymi branża alkoholowa. Według oficjalnych statystyk co trzecia butelka renomowanych marek jest wytwarzana poza właściwą, legalną destylarnią koncernów alkoholowych[3]. Najczęściej spotykaną formą podrabiania trunków jest ponowne napełnianie oryginalnych butelek cieczą gorszej jakości. W skrajnych sytuacjach podrobiony alkohol może zawierać w sobie substancje trujące, pochodne z procesu produkcji paliwa lub płynów do mycia okien samochodowych. Na rynku polskim notorycznie pojawiają się sobowtóry autentycznych butelek różniące się od pierwowzorów jedynie małymi szczegółami nieznanymi przeciętnemu konsumentowi. Należy także pamiętać, że bardzo częstą praktyką jest skup oryginalnych butelek celem ponownego napełnienia tym razem już podrobioną cieczą[4].
Nadrzędną zasadą oszustów jest dźwignia przebitki cenowej stanowiąca, że im droższa jest zawartość butelki, tym wyższą marżę można osiągnąć na popełnionym przestępstwie. Dla przykładu – w 2024 r. Komenda Stołeczna Policji we współpracy z kancelarią radców prawnych zarekwirowała podrobione butelki Chateau Margaux i Chateau Lafite o wartości 6 500 000 zł. Koszt podrobienia niniejszego wina to niespełna 10 zł za butelkę, podczas gdy w oryginalnej dystrybucji butelka Chateau Margaux oscyluje na poziomie 6500 zł, zaś Chateau Lafite szacowana jest aktualnie na 10 000 zł.
Jeszcze dekadę temu światowi producenci starali się ukryć przed klientami fakt występowania podróbek ich artykułów na rynku w obawie o utratę zaufania i prestiżu. Obecnie walczą z fałszerzami o swoje znaki towarowe, zatrudniając do tego najlepsze kancelarie prawne i wykorzystując nowoczesne technologie. Już nie tylko wysublimowany wzór butelki, nakrętki czy naklejki stanowi zabezpieczenie samo w sobie[5]. Producenci prestiżowych alkoholi coraz częściej sięgają bowiem po najprostszą i ogólnodostępną metodę walki z podróbkami, którą umożliwia wykorzystanie smartfonów. Aktualnie większość telefonów, nawet z niższej półki cenowej, posiada możliwość skanowania kodów QR, które umieszczane są na butelkach trunków. Klient indywidualny może zatem sprawdzić oryginalność produktu przed zakupem za pomocą licencjonowanej aplikacji telefonicznej weryfikującej te kody.
W trakcie kursu funkcjonariuszom prezentowane są istotne elementy odróżniające oryginał od towaru podrobionego, jednak z wyłączeniem kluczowych zabezpieczeń fizycznych i cyfrowych, które pozostają jedną z najbardziej pilnie strzeżonych tajemnic, znanych jedynie kilku wybranym osobom z całej firmy.
Do elementów, na które należy zwrócić uwagę w przypadku produktów alkoholowych, z pewnością należą[6]:
– konieczność zakupu alkoholu tylko w wiarygodnych miejscach,
– cena, która w wypadku alkoholu luksusowego nie będzie się znacząco różnić w sieciach dystrybucji na terenie całego kraju,
– poddanie lustracji butelki, korka, nakrętki i etykiety pod kątem jakości wykonania, koloru farby czy nawet błędów ortograficznych,
– obecność odpowiedniej banderoli,
– odpowiednio uszczelnione czapki na szyjkach butelki,
– fałszywe kody kreskowe,
– fałszywe kody QR.

Nie mniej istotne od analizy zabezpieczeń opakowania jest analiza samej cieczy znajdującej się w butelce. Jeśli chodzi o alkohole wysokoprocentowe, to nie powinny one zawierać żadnych białych cząsteczek czy osadu w butelce. Analiza organoleptyczna może także zasugerować klientowi, że nie spożywa on oryginalnego trunku.
Niestety branża alkoholowa była, jest i będzie obszarem podrabiania trunków, gdyż proceder ten jest niezwykle lukratywny[7]. Przy całej specyfice omawianego zjawiska nie należy zapominać, iż prawie 80% ceny wysokoprocentowego alkoholu stanowią podatki i akcyzy, zaś koszt wyprodukowania butelki 0,5 l wódki wynosi przy masowej produkcji poniżej 2 zł.
Dla światowych korporacji i organów ścigania nie mniejszym problemem od podrabianego alkoholu jest czarny rynek związany z imitacją markowej odzieży, galanterii czy perfum i kosmetyków. Zwalczaniem takiej przestępczości, podobnie jak w przypadku alkoholi, zajmują się z reguły wydziały do walki z przestępczością gospodarczą[8]. Działania samych funkcjonariuszy byłyby jednak dużo mniej skuteczne, gdyby nie kancelarie prawne, które na zlecenie producentów penetrują rynek w poszukiwaniu podróbek uszczuplających prestiż firm i ich dochody.
W wypadku odzieży dla odróżnienia oryginału od podróbki kluczowe są: kroje, wielkość logo i jego specyfika, a także bardzo często perfekcja końcowego wykonania, z uwzględnieniem kombinacji indywidualnego układu nici. Ponadto opakowania zewnętrzne posiadają zabez-

pieczenia w postaci hologramów. Przykładem zaawansowanego i unikalnego oznakowania towaru przy pomocy ciągu nici i oznaczeń markowych[9] jest odzież jeansowa firm Levi Strauss & Co czy Lee[10].

Warto przytoczyć jedną z najbardziej problematycznych kwestii w tematyce podróbek, jaką jest rozpoznawanie oryginalności produktów marki odzieżowej Louis Vuitton. W Polsce tylko pojedyncze egzemplarze sygnowane niniejszą marką towarów są produkowane i dostarczane przez oryginalnego producenta. Produktów tej marki nigdy nie znajdziemy na wyprzedaży końcówki serii, w promocji 2 za 1 czy posezonowej wyprzedaży. Oryginalne towary Louis Vuitton, które nie zostaną sprzedane za pośrednictwem nielicznych wyznaczonych sklepów partnerskich, na koniec sezonu zostają odebrane z butików przez producenta i zniszczone. W Warszawie znajduje się aktualnie tylko jeden markowy sklep, a oryginalnych towarów Louis Vuitton nie da się kupić na bazarze czy poprzez zwykły sklep internetowy.

Należy mieć na uwadze, że marka Louis Vuitton ma szereg znaków towarowych, które podlegają ochronie, i na które szczególnie należy zwrócić uwagę:

- ***Monogram Canva*** – rozpoznawalny wzór marki – brązowe tło ze specyficznymi, jasnymi znakami i monogramem LV, wykonany jest z płótna winylowanego, które ma większą wytrzymałość od samej skóry.
- ***Monogram Multicolor*** – jest wersją kolorystyczną, w której na białym lub czarnym tle znajdują się kolorowe oznaczenia. Obicia oraz chwyty zrobione są z jasnej naturalnej skóry.
- ***Cherryblossom*** – znane wzornictwo marki, którego specyfiką jest różowe tło i kwiecisty wzór.
- ***DamierEbene*** – płótno bazujące na systemie szachownicy z odcieniami brązu, zawierające wewnątrz kwadratów symetrycznie logo produktu[11].

Należy pamiętać, że zwalczanie plagi podrobionych towarów jest bardzo trudne i w praktyce jej eliminacja może się okazać niemożliwa. Przepisy prawne wielu państw dopuszczają wytwarzanie podróbek, co jest swoistym ratunkiem dla ich trudnej sytuacji gospodarczej. Ponadto sami klienci końcowi, nie posiadając wystarczających zasobów pieniężnych, często świadomie dokonują zakupu podrobionego produktu imitującego markowy oryginał.

Warto też zaznaczyć, że rozwój podrabiania produktów wspiera nowoczesna technologia, np. handel internetowy z opcją wysyłki towaru do klienta odbywającej się z drugiego końca świata bardzo utrudnia lokalizację zakładu produkcyjnego i złożenie stosownego pozwu.

W krajach rozwiniętych, gdzie prawo gwarantuje ochronę dla własności intelektualnej, w tym przypadku znaków towarowych i wzornictwa[12], sytuacja również nie jest korzystna dla producentów luksusowych marek. Powodem jest hurtowy import podróbek z zagranicy i ich dystrybucja na terenie hal targowych czy chińskich centrów handlowych. Na przykład w Polsce, podczas akcji Policji na terenie takiego obiektu, w której bierze udział kilku lub kilkunastu funkcjonariuszy, poprzez komunikat wygłoszony w językach znanych jedynie kupcom, piraci są ostrzegani o rozpoczętej obławie, co minimalizuje ich straty, bowiem natychmiast zamykają swoje punkty sprzedażowe, a następnie usuwają z nich nielegalny towar. Często finałem takich działań jest więc przewrotny przekaz z głośników, który informuje klientów, że na terenie obiektu nie są dystrybuowane żadne podrobione artykuły należące do znanych marek.

Niestety, w najbliższym czasie na terenie Polski sytuacja raczej nie ulegnie zasadniczej poprawie. Zwalczanie podróbek nie jest priorytetem przeciążonych pracą organów ścigania, a sporadyczne akcje kilku czy kilkunastu funkcjonariuszy przeprowadzane wobec kilkuset straganów na terenie licznych obiektów handlowych są kroplą w morzu potrzeb. Należy przyjąć za pewnik, że dopóki handel podrobionymi towarami będzie bardzo lukratywny, a sankcja karna, która grozi za jego propagowanie, będzie niska, to proceder ten będzie rozkwitał. Nie oznacza to jednak, że producenci markowych produktów mają tolerować nielegalną konkurencję, a Policja ma zaniechać swoich działań w zakresie przeciwdziałania łamaniu prawa oraz ścigania sprawców przestępstw. Wręcz przeciwnie – konieczna jest tu coraz lepsza współpraca i przeprowadzenie bilateralnych szkoleń w oparciu o kluczowe informacje kancelarii prawnych posiadających pełnomocnictwa do reprezentowania interesów znanych marek. Z pewnością zwiększy to skuteczność działań organów ścigania

Bardzo ważnym blokiem tematycznym kursu zwalczania cyberprzestępczości jest obszar szeroko pojętej kooperacji pomiędzy dostawcami Internetu a Policją, uwzględniający niuanse i nowinki techniczne branży IT. Przekazywana wiedza obejmuje w tym zakresie przede wszystkim kwestie identyfikacji użytkownika u *providera* – operatora. Po otrzymaniu informacji od dostawcy konieczne jest ustalenie *providera*, który zrealizował kontakt sprawcy z siecią Internet. Przedmiotową czynność można wykonać między innymi za pośrednictwem bezpłatnych, ogólnodostępnych baz danych, jak chociażby https://www.ripe.net.

Po wprowadzeniu danych adresu IP w wyszukiwarce wyżej wymienionych baz otrzymuje się informację zwrotną w postaci nazwy konkretnego operatora połączenia. Sam operator na podstawie danych zgromadzonych na jego serwerach jest w stanie wskazać konkretną osobę, na którą są zarejestrowane usługi teleinformatyczne pozwalające na połączenie z siecią Internet[13]. Należy tu zauważyć, że zgodnie z obowiązującym w Polsce prawem każdy operator prowadzący działalność telekomunikacyjną jest zobligowany przez 12 miesięcy do przechowywania danych pozwalających na identyfikację abonenta końcowego korzystającego z usługi telekomunikacyjnej (do danych tych zaliczają się m.in. adresy IP)[14].

Kolejnym etapem następującym po uzyskaniu informacji od operatora telekomunikacyjnego jest próba identyfikacji faktycznego użytkownika końcowego. Następuje to poprzez doprecyzowanie informacji od operatora dotyczących abonenta, który w określonym dniu i czasie korzystał ze wskazanego adresu IP, z uwzględnieniem danych, z jakich stacji BTS[15] nastąpiło połączenie z siecią oraz jakie urządzenie było wykorzystane do połączenia (np. numer IMEI). Posiadając wyżej wymienione informacje, można pokusić się o próbę identyfikacji użytkownika końcowego. Jest to

proces skomplikowany, gdyż na podstawie danych przekazanych przez operatora telekomunikacyjnego o konkretnym abonencie oraz o określonym połączeniu można uzyskać informacje dotyczące tego:
– kim był klient, tj. osoba korzystająca w danej chwili z łącza internetowego,
– gdzie mniej więcej znajdował się użytkownik,
– z jakiego sprzętu korzystał.

Po tych ustaleniach policjant prowadzący sprawę na etapie postępowania przygotowawczego może podjąć już decyzję, w jaki sposób pozyskane informacje zostaną wykorzystane. Oczywistą sprawę można jednak potraktować dwojako. W pierwszym, łatwiejszym, wariancie dane bezsprzecznie wskażą sprawcę. W wariancie drugim konieczne będzie podjęcie dalszych czynności identyfikujących sprawcę. W takim wypadku prawdopodobnie niezbędne będą czynności w zakresie przesłuchania świadków (abonenta), przeprowadzenia analizy pozostałych usług współpracujących z ustalonymi urządzeniami czy też weryfikacji danych obejmujących współrzędne logowania się do sieci[16].

Zdobyta w ten sposób wiedza staje się następnie kanwą do rozważań w zakresie trzeciego z kolei bloku tematycznego kursu, obejmującego poszukiwanie użytkownika za pośrednictwem podmiotu świadczącego usługi drogą elektroniczną. Tematyka ta jest bardzo aktualna, ponieważ dotyczy przede wszystkim sklepów internetowych oraz portali aukcyjnych, które z roku na rok notują kilkunastoprocentowe wzrosty obrotów sprzedaży. Podobnie jak w uprzednio omówionym obszarze dla umożliwienia zadowalającego poziomu wykrycia sprawców przestępstw konieczny jest stały rozwój współpracy pomiędzy Policją a kluczowymi graczami na rynku handlu internetowego. Zaproszeni eksperci ze spółek Allegro Sp. z o.o. oraz OLX Sp. z o.o. podczas zajęć prezentują najnowsze i najbardziej popularne mechanizmy działania oszustów wykorzystujących elementy socjotechniki, jak i aktualne luki proceduralno-administracyjne. Przekazywana wiedza ma charakter poufny z racji tego, że jej treść może mieć kluczowe zastosowanie w zwalczaniu tego rodzaju przestępczości oraz stanowić bardzo cenne wskazówki dla osób trudniących się tego typu procederem, co mogłoby utrudnić ściganie tego rodzaju przestępstw[17].

Z problematyki, którą w celach edukacyjnych możemy otwarcie poruszyć na łamach niniejszego czasopisma, na uwagę zasługuje schemat obejmujący współpracę prowadzącego postępowanie z administratorem usługi świadczonej drogą elektroniczną[18].

Policjant prowadzący sprawę uzyskuje zdalnie, poprzez profil zaufany, od operatora konkretnej usługi następujące informacje:
– nazwisko i imiona usługobiorcy/klienta;
– numer PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość klienta;
– adres zameldowania na pobyt stały lub adres do korespondencji, jeżeli jest inny;
– dane służące do weryfikacji podpisu elektronicznego usługobiorcy;
– adresy elektroniczne usługobiorcy, numer telefonu komórkowego;
– inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną[19].

Z pozoru tak duża ilość informacji gromadzona przez administratorów na mocy obowiązującego w Polsce prawa często może okazać się niewystarczająca do wskazania konkretnego sprawcy. Żeby móc pokusić się o jego ustalenie, operator usługi musiałby podjąć się gromadzenia i przechowywania danych związanych z połączeniem usługobiorcy z usługami w postaci wykorzystanych adresów IP (najlepiej wraz z portami) oraz datą i godziną. Istnieje możliwość dążenia do ustalenia „osoby będącej po drugiej stronie sieci", co aktualnie nie jest obowiązującą praktyką.

Ostatnim, czwartym, blokiem omawianym w czasie kursu jest tematyka przestępstwa sharingu polegającego na nielegalnym rozdzieleniu uprawnień karty abonenckiej i udostępnieniu tych uprawnień osobom do tego nieuprawnionym przy użyciu urządzeń niedozwolonych, za pośrednictwem sieci Internet. Jest to proceder pozwalający na odbiór kanałów telewizji satelitarnej w czasie rzeczywistym w wyniku bezprawnego uzyskania uprawnień przysługujących klientom nadawców telewizyjnych. W procederze sharingu biorą udział dawca – oferujący nielegalną usługę i odbiorca – osoba, której udostępniana jest telewizja.

Należy zauważyć, że zarówno dawca pirackiego sygnału, jak i biorca popełniają przestępstwo. Ta kategoria przestępstw posiada niezwykle wysoką specjalizację, a jej skuteczne zwalczanie jest możliwe praktycznie tylko dzięki zaangażowaniu komórek bezpieczeństwa platform telewizji cyfrowych, które w ramach Stowarzyszenia „Sygnał" współpracują z Policją, dostarczając danych zarówno o samym przestępstwie, miejscu jego popełnienia, jak i o osobie potencjalnego sprawcy.

Podsumowując omawiane wyżej zagadnienia, należy zauważyć, że zwalczanie nowoczesnej przestępczości wymaga zastosowania wiedzy oraz sił i środków, których Policja nie posiada na wystarczającym poziomie. Jedyną drogą dającą szanse na skuteczne zwalczanie takich naruszeń prawa jest kooperacja pokrzywdzonych z organami ścigania oraz systematyczne podnoszenie kwalifikacji policjantów.

Kurs specjalistyczny z zakresu uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową jest obecnie jednym z najbardziej nowoczesnych szkoleń przeprowadzanych przez Centrum Szkolenia Policji w Legionowie i cieszy się bardzo dużym zainteresowaniem policjantów. Jego formuła jest rozwijana i uzupełniania z edycji na edycję. Największą zaletę tej formy doskonalenia zawodowego stanowi jednak unikalność i hermetyczność przekazywanej wiedzy, której nie sposób pozyskać z Internetu, z literatury czy innych źródeł.

[1] Kurs specjalistyczny w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową (decyzja nr 322 Komendanta Głównego Policji z dnia 24 października 2018 r. w sprawie programu nauczania na kursie specjalistycznym w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową, Dz. Urz. KGP z 2018 r. poz. 109).

[2] Polskie Radio RDC, *Podróbki światowych marek warte blisko 30 mln zł. Wielka akcja policji w Nadarzynie,* https://www.rdc.pl/aktualnosci/mazowsze/podrobki-nadarzyn-wolka-kosowska-ubrania-podrabiane-policja-zatrzymania_XX3Kg6pKxs5fb6IchAkA [dostęp: 27.10.2024 r.].
[3] J. Fundowicz, K. Łapiński, B. Wyżnikiewicz, *Szara Strefa 2024*, Warszawa 2024, s. 17.
[4] Tamże, s. 18.
[5] Tamże, s. 19.
[6] Tamże.
[7] Tamże.
[8] Tamże.
[9] Specyficzny kształt kieszeni i naszywek.
[10] YouNeedit.pl, *Oryginalne jeansy, czyli jakie? Jak rozróżnić?*, https://youneedit.pl/Oryginalne-jeansy-czyli-jakie-Jak-rozroznic-blog-pol-1667848577.html [dostęp: 27.10.2024 r.].
[11] Komis Label, M. Szymański, *Jak rozpoznać autentyczność torebki Louis Vuitton: Przewodnik dla kolekcjonerów*, https://komislabel.pl/blog/-jak-rozpoznac-autentycznosc-torebki-louis-vuitton-przewodnik-dla-kolekcjonerow-b47.html [dostęp: 27.10.2024 r.].
[12] W Polsce kwestie te reguluje ustawa z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (Dz. U. z 2023 r. poz. 1170).
[13] P. Gwizd, *Analiza danych w informatyce śledczej. Ataki na strony internetowe*, Kraków 2013, s. 50.
[14] Wśród przechowywanych informacji znajdują się: dane osobowe, okresy nawiązywania połączeń, czas trwania, numery identyfikujące urządzenia inicjujące połączenia oraz stacje nadajnikowe wykorzystywane podczas nawiązywania połączeń.
[15] Stacja BTS – z ang. *Base Transceiver Station*, stacja przekaźnikowa umożliwiająca komunikację urządzenia mobilnego z siecią operatora.
[16] Analizując odpowiedź przesłaną przez operatora, należy mieć na względzie, że usługa polegająca na dostępie do Internetu świadczona ustalonemu abonentowi może mieć charakter personalnie indywidualny, ale często też dostęp do sieci jest przekazywany przez router dzielący sygnał na kilka urządzeń czy też router bez zabezpieczeń – wtedy mamy do czynienia z tzw. siecią otwartą, z której może korzystać wiele anonimowych osób (jak w przypadku usługi typu *hot-spot)*. W takich przypadkach niezbędna może się okazać analiza dotycząca urządzenia wykorzystanego podczas logowania do sieci (może to się wiązać z koniecznością procesowego zabezpieczenia, a następnie zbadania routera). Dodatkowo użytkownicy poruszający się w sieci Internet mogą podejmować próby ukrycia swojego położenia poprzez maskowanie wykorzystywanego adresu IP czy jego zmianę – wówczas ustalenie abonenta jest znacznie utrudnione, a czasem wręcz niemożliwe. To samo dotyczy pozyskiwania informacji dotyczących użytkowników korzystających z zagranicznych operatorów – w takich przypadkach w celu ustalenia abonenta niezbędne jest skorzystanie z międzynarodowej pomocy prawnej, co implikuje wiele trudności praktycznych.
[17] M. Grabowski, *Dropshipping: instrukcja obsługi,* Gliwice 2023, s. 21.
[18] Administratorami usług świadczonych drogą elektroniczną są np. właściciele sklepów internetowych i portali aukcyjnych, administratorzy portali ogłoszeniowych, społecznościowych, poczty e-mail, forów dyskusyjnych itd.
[19] M. Grabowski, *Dropshipping: instrukcja obsługi*, s. 27.

Bibliografia

Publikacje

Fundowicz J., Łapiński K., Wyżnikiewicz B., *Szara Strefa 2024*, Warszawa 2024.
Grabowski M., *Dropshipping: instrukcja obsługi*, Gliwice 2023.
Gwizd P., *Analiza danych w informatyce śledczej. Ataki na strony internetowe*, Kraków 2013.

Źródła internetowe

Polskie Radio RDC, *Podróbki światowych marek warte blisko 30 mln zł. Wielka akcja policji w Nadarzynie*, https://www.rdc.pl/aktualnosci/mazowsze/podrobki-nadarzyn-wolka-kosowska-ubrania-podrabiane-policja-zatrzymania_XX3Kg6pKxs5fb6IchAkA [dostęp: 27.10.2024 r.].
Komis Label, M. Szymański, *Jak rozpoznać autentyczność torebki Louis Vuitton: Przewodnik dla kolekcjonerów,* https://komislabel.pl/blog/-jak-rozpoznac-autentycznosc-torebki-louis-vuitton-przewodnik-dla-kolekcjonerow-b47.html [dostęp: 9.02.2025 r.].
YouNeedit.pl, *Oryginalne jeansy, czyli jakie? Jak rozróżnić?,* https://youneedit.pl/Oryginalne-jeansy-czyli-jakie-Jak-rozroznic-blog-pol-1667848577.html [dostęp: 27.10.2024 r.].

Summary

Specialist course in obtaining information from the Internet for police officers fighting computer crime

This article synthetically presents issues from a specialist course on obtaining information from the Internet for police officers fighting computer crime, conducted by the Criminal Department of the Police Training Centre in Legionowo.
The 4 main blocks of the course were discussed chronologically. First, the specificity of prosecuting crimes related to the counterfeit branded goods, was presented.
The second course block presents mechanisms and methods of prosecuting cyber crimes from the point of view of law enforcement agencies.
The third block highlighted the methods of cooperation with non-police entities and its scope in combating crimes committed via auction portals.
The last, fourth part presents the methods of Police cooperation with the „Signal" Association in combating piracy against digital television.
The article emphasizes the innovation of the course and the often underestimated role of synergy between the activities of private companies and the Police in the area of combating specific and sophisticated crime.
The author of the study emphasizes that some of the course issues were only indicated in the article, because the specificity of the knowledge provided by the lecturer during the classes does not allow it to be described in detail in professional magazines due to the possibility of it being used by the criminals to eliminate mistakes made while committing crimes.

Tłumaczenie: Beata Pepłowska