Zapobieganie fizycznym atakom na bankomaty

OPRACOWANIE SKUTECZNEGO PODEJŚCIA

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

EMPACT

EUROPOL

“

It is only a matter of time before MOs emerging in one country spread to other countries. This clearly indicates the need for adoption of the preventive and operational measures at the European level with private, public and law-enforcement partners working closely together.

”

PODZIĘKOWANIE

Niniejszy dokument jest owocem współpracy między Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (Europolem) a Sekretariatem Europejskiej Sieci Zapobiegania Przestępczości (EUCPN). Chcielibyśmy podziękować ekspertom ds. fizycznych ataków na bankomaty, którzy poświęcili swój czas i wysiłek, wspierając tworzenie tego dokumentu rekomendacyjnego. Brali oni udział w konferencji na temat zapobiegania fizycznym atakom na bankomaty (styczeń 2019 r. w Brukseli) i dostarczyli wiele istotnych informacji. W szczególności chcielibyśmy podziękować organom ścigania z krajów UE i spoza UE („krajów trzecich"), przedstawicielom sektora prywatnego, w tym ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, panelowi ekspertów European Association for Secure Transactions ds. fizycznych ataków na bankomaty i automaty kasjerskie (EAST EGAP), European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security oraz ministerstwom spraw wewnętrznych Belgii, Chorwacji, Niemiec i Hiszpanii.

Citation
© Agencja Unii Europejskiej ds. Współpracy Organów Ścigania 2019
© Europejska Sieć Zapobiegania Przestępczości 2019

Obwieszczenie prawne
Treść niniejszej publikacji niekoniecznie odzwierciedla oficjalną opinię jakiegokolwiek państwa członkowskiego UE ani jakiejkolwiek agencji lub instytucji UE bądź Wspólnot Europejskich.

Zezwala się na powielanie pod warunkiem podania źródła. W celu wykorzystania lub powielenia poszczególnych zdjęć należy zwrócić się o pozwolenie bezpośrednio do posiadacza praw autorskich. Niniejsza publikacja oraz dodatkowe informacje na temat Europolu są dostępne w internecie.

This brochure was funded by the European Union's Internal Security Fund — Police.

SPIS TREŚCI

KONTEKST

Wraz z rosnącą liczbą fizycznych ataków na bankomaty i rosnącą liczbą państw europejskich, których ten problem dotyczy, Europejska Sieć Zapobiegania Przestępczości (EUCPN) i Europol zorganizowały konferencję (styczeń 2019 r.), podczas której organy ścigania wspólnie z partnerami publicznymi i prywatnymi skupiły się na kwestii zapobiegania tego typu przestępczości. Niniejszy dokument rekomendacyjny podsumowuje wnioski wyciągnięte podczas tej konferencji i ma na celu podniesienie świadomości organów prawnych w zakresie fizycznych ataków na bankomaty oraz środków zapobiegawczych.

Ograniczona, ale jednocześnie rosnąca liczba państw Unii Europejskiej ma obawy związane z fizycznymi atakami na bankomaty. W 2017 r. straty finansowe w Europie oszacowano na ponad 30 mln euro. W niektórych krajach nadal obserwuje się znaczną liczbę ataków fizycznych na bankomaty, a w innych odnotowano znaczny wzrost liczby tych incydentów w ciągu ostatnich 2 lat. Ten obszar przestępczości ewoluuje w szybkim tempie. Niektóre kraje odniosły sukces w radzeniu sobie z fizycznymi atakami na bankomaty, a w ostatnim czasie odnotowały znaczny spadek ich liczby. Z drugiej strony, w 2018 r. kraje wcześniej niedotknięte tym problemem spotkały się z nagłym wzrostem liczby fizycznych ataków na bankomaty w związku z terytorialną ekspansją zorganizowanych grup przestępczych (ZGP). Problem dotyczy nie tylko banków – coraz częściej atakowane są bankomaty niezależnych dostawców, gdyż często znajdują się one w bardziej podatnych obiektach lub miejscach.

Bogaty wachlarz metod działania (modus operandi), z jakich kryminaliści korzystają do ataków na bankomaty można podzielić na dwie główne kategorie: fizyczne ataki na bankomaty oraz oszustwa związane z bankomatami (w tym ataki logiczne i przy użyciu złośliwego oprogramowania). Niniejszy dokument koncentruje się na fizycznych atakach na bankomaty: włamaniach do bankomatów z użyciem środków fizycznych w celu zrabowania znajdującej się w nich gotówki. Metody włamań:

> **użycie materiałów wybuchowych:** włamywacze używają gazowych lub stałych materiałów wybuchowych w celu fizycznego wtargnięcia do bankomatowego sejfu i uzyskania dostępu do gotówki;

> **atak poprzez wyrwanie/staranowanie:** włamywacze fizycznie usuwają bankomat ze środowiska instalacyjnego, często korzystając ze specjalnego pojazdu;

> **atak in-situ:** włamywacze rozcinają sejf z użyciem brutalnej siły, często za pomocą narzędzi do cięcia lub rozrywania/kruszenia, takich jak szlifierki kątowe, młoty kowalskie lub palniki acetylenowo-tlenowe.

01 CZYNNIKI DECYDUJĄCE O SUKCESIE FIZYCZNYCH ATAKÓW NA BANKOMATY

Wskaźnik powodzenia ataków na bankomaty jest niski – tylko jedna trzecia z nich kończy się sukcesem. Jednak nawet jeśli atak nie powiódł się, szkody wyrządzone w budownictwie (np. przez ładunki wybuchowe) są równie istotne, gdyż stanowią niebezpieczeństwo dla mieszkańców, zespołów szybkiego reagowania i przechodniów. Powodzenie ataku fizycznego zależy od wielu czynników, w tym charakterystyki i umiejscowienia bankomatu oraz doświadczenia i eksperckiej wiedzy sprawców.

1. Podatność bankomatów na zagrożenia

Najbardziej narażone bankomaty to te, które znajdują się na zewnątrz (w ścianie) lub które ustawiono wewnątrz budynków. W przypadku ataku na bankomaty wewnętrzne (wolnostojące), ZGP preferują bankomaty zlokalizowane w pomieszczeniach komercyjnych, zamiast bankomatów znajdujących się w pomieszczeniach banku, gdzie nadzór jest zazwyczaj większy. Banki obsługują głównie bankomaty zlokalizowane wewnątrz lub na zewnątrz budynku banku. Odległe lokalizacje bankowe na ulicy lub w komercyjnych pomieszczeniach handlowych, takich jak stacje benzynowe,

supermarkety, hotele, kasyna, lotniska itp., stopniowo stają się coraz ważniejsze ze względu na zamykanie oddziałów banków. Dostawcy niezależni oferują bankomaty jako samodzielną usługę. Ich urządzenia są często zlokalizowane w punktach handlowych, hotelarskich i rekreacyjnych, miejscach transportu (dworce kolejowe, lotniska itp.), budynkach publicznych oraz na ulicy.

Wraz ze wzrostem popularności bankowości internetowej wiele oddziałów bankowych prawdopodobnie zostanie zamkniętych w nadchodzących latach, co doprowadzi do ogólnego spadku liczby dostępnych bankomatów[1]. Mogłoby to jednak pociągnąć za sobą wzrost liczby bankomatów oddalonych od banków oraz bankomatów niezależnych dostawców zlokalizowanych w bardziej podatnych miejscach.

2. Przygotowanie ataku na bankomat

Przygotowanie ataku może potrwać kilka tygodni, a nawet miesięcy. Sprawcy muszą zebrać niezbędne **narzędzia i zasoby**, takie jak pojazdy, sprzęt i punkty kontaktowe. **Pojazdy** są niezbędnym narzędziem w fizycznych atakach na bankomaty – sprawcy podróżują głównie nimi, a po ataku uciekają najczęściej, korzystając z szybkiego pojazdu. Są one często kradzione, ale mogą być też wynajęte lub kupione (np. przez internet). Większość **sprzętu** do fizycznych ataków na bankomaty jest łatwo i legalnie dostępna w normalnych sklepach. To dodatkowo obniża próg wejścia w ten obszar przestępczości. Wyśledzenie pochodzenia narzędzia jest trudne dla organów ścigania, więc ryzyko ponoszone przez sprawców jest ograniczone. ZGP zajmujące się fizycznymi atakami na bankomaty na poziomie międzynarodowym prawie zawsze mają punkty kontaktowe w kraju docelowym (osoby, które przebywają tam przez pewien czas) lub alternatywnie mogą stosować technikę ucieczki z miejsca zdarzenia. Kontakty te wspierają ZGP w logistyce, jak wynajem zakwaterowania, zorganizowanie pojazdu lub innego sprzętu, a także przeprowadzenie zwiadu związanego z celem. Niektórzy przestępcy międzynarodowi pozostawiają logistykę i obserwacje całkowicie lokalnym kontaktom i po prostu przybywają drogą naziemną lub powietrzną na miejsce przeprowadzania ataku na bankomat.

ZGP często przeprowadzają szeroko zakrojone **działania zwiadowcze** w celu zidentyfikowania odpowiednich celów – ustalają porę dnia uzupełniania bankomatu, oceniają otoczenie bankomatu, weryfikują specyfikację techniczną urządzenia, drogi ucieczki i stosowane środki bezpieczeństwa, takie jak system nadzoru telewizyjnego (CCTV), czujniki alarmowe i rolety.

Niektóre ZGP podejmują szereg działań, aby przed atakiem **uprzykrzyć życie wymiarowi sprawiedliwości i służbom ochroniarskim**. Ingerują w systemy alarmowe i publiczną sieć oświetlenia, używają technik dywersyjnych, ustawiają blokady drogowe lub próbują ingerować w pojazdy służb ścigania.

3. Doświadczenie i know-how sprawców

Fizyczne ataki na bankomaty są atrakcyjne dla przestępców, ponieważ pieniądze są dostępne natychmiastowo i nie ma potrzeby korzystania z rozległej sieci sprzedaży skradzionych towarów. Jest to dogodna alternatywa dla przestępców już aktywnych w zorganizowanej przestępczości przeciwko mieniu.

ZGP muszą zebrać **potrzebną fachową wiedzę i know-how**, ponieważ są one czynnikiem decydującym o sukcesie bądź niepowodzeniu ataku. Wymagana fachowa wiedza i know-how zależą w dużym stopniu od **rodzaju ataku**. Ataki poprzez wyrwanie/staranowanie oraz ataki *in situ* mają prostą zasadę działania (głównie zuchwałość i użycie brutalnej siły), więc generalnie nie wymagają szczególnych umiejętności. Ataki z użyciem palnych gazów i materiałów wybuchowych wymagają wyższego poziomu wiedzy.

Sprawcy charakteryzują się różnymi **poziomami kompetencji**. Z jednej strony, wysoce zorganizowane i doświadczone grupy mogą przeprowadzić udany atak fizyczny na bankomat w ciągu kilku minut. Mają one kontrolę nad całym procesem i są w stanie ograniczyć ryzyko tylko do siebie, ograniczając tym samym szkody uboczne. Z drugiej strony, mniej zorganizowane i oportunistyczne grupy często zawodzą w swoich próbach i mogą spowodować znaczne szkody w atakowanych lokacjach i sąsiednich budynkach. Uważa się, że niektóre z mniej zorganizowanych ZGP wracają do tradycyjnej działalności związanej z przestępczością zorganizowaną na skutek zniechęcania środkami zapobiegawczymi, których nie są w stanie pokonać podczas ataku na bankomaty.

02 POTRZEBA PODEJŚCIA ZAPOBIEGAWCZEGO

Kraje, w których wskaźnik skuteczności fizycznych ataków na bankomaty lub w których liczba takich ataków zmniejsza się, pokazują, że skuteczne podejście do zwalczania tego typu aktywności przestępczej polega na połączeniu środków operacyjnych i zapobiegawczych. Ponieważ liczba aktywnych ZGP w tym obszarze jest ograniczona, aresztowania i kary dla członków ZGP znacznie zmniejsza liczbę ataków. Jednak po wypuszczeniu na wolność wielu włamywaczy wznawia swoją działalność. Co więcej, zdarza się, że grupa szybko zastępuje zatrzymanego włamywacza innym. W związku z tym istnieje silna potrzeba skorzystania ze środków zapobiegawczych, najlepiej wbudowanych w ramy prawne. Ponadto doświadczenie pokazuje, że środki zapobiegawcze stosowane w jednym kraju mogą skłonić poszczególne ZGP do skoncentrowania się na bardziej wrażliwych celach w innych krajach. Jest tylko kwestią czasu, zanim metody działania z jednego kraju rozprzestrzenią się na inne. Wskazuje to wyraźnie **na potrzebę zaadaptowania środków zapobiegawczych i operacyjnych na szczeblu europejskim** z udziałem ściśle ze sobą współpracujących prywatnych i publicznych partnerów oraz organów ścigania.

03 ZAPOBIEGANIE

Aby zapobiegać tego rodzaju przestępstwom i odpowiednio zwalczać je, potrzebna jest klarowna strategia. W tym rozdziale przedstawimy przegląd trzech kroków, które są zazwyczaj podejmowane w obliczu fizycznych ataków na bankomaty lub podczas przygotowywania się do ich prewencji.

Przede wszystkim należy przeprowadzić **ocenę sytuacji**: należy określić profil ryzyka dotyczący bankomatów i ich otoczenia, biorąc pod uwagę ilość dostępnych środków pieniężnych (możliwy łup), ryzyko wystąpienia szkód ubocznych i ryzyko odniesienia obrażeń ciała. Po drugie, należy opracować **strategię zapobiegawczą** w oparciu przeprowadzoną ocenę ryzyka. Na końcu należy wdrożyć **środki zapobiegawcze.**

1. Ocena sytuacji

ZGP z reguły obierają za cel określone rodzaje bankomatów lub bankomaty konkretnych dostawców mające cechy, które ułatwiają przeprowadzenie ataku. W związku z tym konieczne jest przeprowadzenie szczegółowej oceny ryzyka ataków, obejmującej najlepiej cały łańcuch zabezpieczeń gotówki, od tranzytu przez dostawę po składowanie w bankomacie. W celu określenia profilu ryzyka dla każdego bankomatu należy przeanalizować szereg elementów.

- Charakterystyka lokalizacji i otoczenia bankomatu, w tym: rodzaj lokalizacji (miejska lub wiejska), gęstość zaludnienia, bliskość posterunków policji, znajdujące się w sąsiedztwie systemy kamer automatycznego rozpoznawania tablic rejestracyjnych (ANPR), pobliskie systemy CCTV itp.
- Umiejscowienie bankomatu:
  - wewnątrz lub na zewnątrz budynku, w oddziale banku lub w lokalizacji zdalnej (np. komercyjnej), wbudowanie w ścianę lub przymocowanie do budynku;
  - w przypadku bankomatu wolnostojącego: czy jest on zakotwiczony czy nie;
  - w przypadku bankomatów wbudowanych lub przymocowanych do budynku: czy istnieją słabe punkty architektoniczne, w jaki sposób organizowane jest przechowywanie gotówki itp.
- Rodzaj bankomatu.
- Funkcje bezpieczeństwa oferowane przez bankomat.
- Ilość gotówki znajdująca się w bankomacie.
- Rodzaje ataku na bankomat i sposoby działania, których należy się spodziewać w celu przyjęcia najstosowniejszych środków zapobiegawczych w pierwszej kolejności.
- Podjęte już środki bezpieczeństwa i środki zapobiegawcze (inteligentne systemy neutralizacji banknotów (IBNS), systemy CCTV, systemy zabezpieczające do generowania mgły (ograniczania widoczności) itp.).

Dalsze elementy podlegające ocenie to stan współpracy z partnerami i zainteresowanymi stronami oraz prawodawstwo. Należy ocenić współpracę między organami ścigania oraz partnerami prywatnymi i publicznymi w celu zbudowania sojuszy do zwalczania przestępczości. Możliwe, że każdy partner posiada interesujące informacje, które przydadzą się w ocenie sytuacji. Szczególnie ważne są w tym kontekście lokalne władze i policja. Przepisy muszą zostać ocenione pod kątem ustanowienia ram prawnych w zakresie zapobiegania, podejmowania obowiązkowych środków zapobiegawczych, wydawania wyroków za ataki na bankomaty itp.

2. Opracowanie praktyk zapobiegawczych

Po dokonaniu oceny sytuacji i określeniu głównych obszarów ryzyka oraz słabych i mocnych punktów w zabezpieczeniach bankomatu można opracować strategię (często opartą na współpracy publiczno-prywatnej) oraz wprowadzić środki zapobiegawcze i operacyjne. Środki zapobiegawcze powinny mieć na celu ostudzenie zamiarów i zmniejszenie możliwości włamywaczy. W tym celu proponuje się trzy osie działań zapobiegawczych opartych na trzech z pięciu strategii zapobiegania przestępczości sytuacyjnej proponowanych przez Clarke'a[2]; zmniejszenie korzyści, zwiększenie ryzyka ponoszonego przez sprawców i zwiększenie wysiłków potrzebnych na dostanie się do łupu.

Przestępcy dokonują rachunku spodziewanych zysków względem potencjalnego ryzyka (np. przy ataku na bankomat). Zmniejszenie szans na zdobycie łatwego łupu i zwiększenie ryzyka, z jakim muszą liczyć się sprawcy, obniża ich oczekiwania i chęć zaangażowania w fizyczny atak na bankomat. Kolejne środki, które wymagają zwiększenia wysiłku niezbędnego do uzyskania dostępu do bankomatu, wpływają na możliwości sprawców. Włamywacze oportunistyczni, których próby włamań często kończą się niepowodzeniem, przestają angażować się w ataki na bankomaty. Dla profesjonalnych włamywaczy wskaźnik sukcesu zostaje zmniejszony, również wpływając na bilans zysków/ryzyka.

Co więcej, strategię prewencyjną można uzupełnić o środki równoległe, jak skuteczna strategia medialna, wczesne zapobieganie społeczne, wdrażanie środków mających zmniejszyć ryzyko wystąpienia szkód ubocznych w budynkach oraz zapewnienie bezpieczeństwa okolicznym mieszkańcom, zespołom szybkiego reagowania i przechodniom.

Możliwe są inne sposoby ustrukturyzowania tego podejścia. Władze holenderskie stosują tzw. model barier[3]. Określa on kroki, które przestępca musi podjąć w celu popełnienia przestępstwa. Określa również partnerów i możliwości, które umożliwiają popełnienie

przestępstwa, a także jest użytecznym narzędziem, dzięki któremu można przygotować proces gromadzenia informacji w obszarze przestępstwa. Identyfikując każdy krok niezbędny do przeprowadzenia fizycznego ataku na bankomat, można określić bariery, które utrudnią popełnienie przestępstwa, jak również najlepszych partnerów, którzy te bariery przygotują. Model barier pozwala również określić sygnały ostrzegające o atakach dla publicznych i prywatnych partnerów oraz sygnały, które partnerzy mogą wysyłać, aby powiadomić władze o swoich podejrzeniach.

Potrzebna jest dobrze rozwinięta strategia, która pozwoli złagodzić ryzyko związane ze wzmocnieniem praktyk zapobiegawczych. Środki zapobiegawcze, które są bardzo skuteczne w zniechęcaniu amatorów i naśladowców, przynoszą czasami niepożądane efekty. Niektóre grupy decydują się na zastosowanie metody prób i błędów w celu znalezienia podatnych bankomatów, uszkadzając w ten sposób wiele takich urządzeń. Bardziej niebezpieczne i bezwzględne ZGP zaczynają korzystać z brutalniejszych metod działania, zastępując np. palne gazy stałymi materiałami wybuchowymi.

Aby opracować skuteczny zestaw środków zapobiegawczych, najlepszą praktyką jest ustanowienie organu krajowego, który będzie uprawniony do stosowania szczególnych środków w odniesieniu do wysoce zagrożonych bankomatów, robiąc to z wykorzystaniem gruntownej analizy sytuacji. Podejście to okazało się skuteczne we Francji, zwłaszcza w przypadku ustanowienia ram prawnych i wdrożenia tych środków wraz ze środkami operacyjnymi.

3. Wdrożenie środków zapobiegawczych

Omówione w tym rozdziale środki, które wprowadzono w celu zapobiegania fizycznym atakom na bankomaty, okazały się przydatne w różnych krajach. Opierają się one na wnioskach z konferencji dotyczącej działań prewencyjnych oraz na środkach zapobiegawczych aktywnie promowanych przez organizacje międzynarodowe zajmujące się bezpieczeństwem bankomatów. Wiele środków jest dobrze znanych. Kilka krajów z powodzeniem wdrożyło już kilka z nich. Często jednak proponowane środki są wdrażane tylko częściowo i nie są włączane do prawodawstwa.

Jak wspomniano powyżej, proponuje się trzy osie działań zapobiegawczych: zmniejszenie korzyści, zwiększenie ryzyka ponoszonego przez sprawców oraz zwiększenie wysiłków potrzebnych na dostanie się do łupu.

3.1 Zmniejszenie korzyści

Zmniejszenie korzyści płynących z działań przestępczych jest pierwszą osią zapobiegania fizycznym atakom na bankomaty. Dopóki wizja „łatwych pieniędzy" utrzymuje się, przestępcy będą angażować się w tego rodzaju przestępstwa. Zmniejszenie ilości dostępnej gotówki oraz jej usunięcie bądź zniszczenie sprawią, że potencjalny łup nie będzie tak interesujący. Mniejsze oczekiwania obniżają chęć kryminalisty do angażowania się w tego typu przestępstwa.

Zmniejszenie ilości gotówki

Jednym ze środków mających na celu zmniejszenie korzyści jest obniżenie ilości gotówki dostępnej w bankomacie. W idealnym przypadku kwota ta powinna być ograniczona do ilości niezbędnej tylko na jeden dzień operacji. Współpraca między bankami mogłaby zapewnić opłacalność. W Holandii kilka banków nawiązało współpracę na rzecz utworzenia niezależnej sieci bankomatów zwanej „Geldmaat". Celem współpracy jest zapewnienie dostępności, przystępności cenowej i bezpieczeństwa gotówki. Działania te doprowadzą najprawdopodobniej do zmniejszenia liczby bankomatów. Jednakże każdy bankomat będzie zawierał mniej gotówki, ale będzie ona częściej uzupełniana. Liczba uzupełnień zostanie dostosowana do potrzeb.

Ponieważ przestępcy atakują najczęściej między 3:00 a 4:00, zdecydowanie zaleca się, aby na koniec dnia opróżniać bankomaty wolnostojące (znajdujące się głównie w pomieszczeniach komercyjnych i publicznych, gdzie są bardziej narażone) i przenosić gotówkę do sejfu. Stosując odpowiednie oznaczenie, można poinformować użytkowników, że w nocy w bankomacie nie ma żadnej gotówki. Następnego dnia bankomat powinien zostać uzupełniony poza zasięgiem wzroku klientów i przy zamkniętym pomieszczeniu. System ten jest wdrażany we Francji, gdzie przepisy zobowiązują sprzedawców detalicznych, aby wyjmowali na noc gotówkę z autonomicznych bankomatów w swoich sklepach, pozostawiając urządzenia otwarte. W przypadku innych bankomatów można zmniejszyć ilość gotówki i zwiększyć częstotliwość jej uzupełniania.

Dewaluowanie łupów i sprawianie, że pieniądze można namierzyć

Inteligentne systemy neutralizacji banknotów (IBNS) są pierwszą linią dewaluowania łupów. Systemy te plamią banknoty tuszem, by oznaczyć je jako skradzione. Do tuszu IBNS można dodać znaczniki i markery. W tej chwili znaczniki te są wykorzystywane głównie do celów analizy kryminalistycznej, która pozwala połączyć banknoty z miejscem zbrodni, zwiększając tym samym prawdopodobieństwo złapania sprawców. Mimo że IBNS jest skutecznym środkiem zapobiegawczym, pojawiają się pewne problematyczne kwestie.

Europejski Bank Centralny nie wymienia zabarwionych banknotów[4] (od 2003 r.), choć nadal robi to wiele krajowych banków centralnych państw członkowskich UE. Zabarwione banknoty są również ponownie wprowadzane do legalnego obiegu za pośrednictwem kasyn. Systemy IBNS są dodatkową przeszkodą dla przestępców, ale byłyby znacznie bardziej skuteczne, gdyby przestępcy nie mogli wykorzystać zabarwionych banknotów na terenie UE. W tym celu krajowe banki centralne nie powinny akceptować zabarwionych pieniędzy. Wyjątki mogłyby dotyczyć szczególnych okoliczności, takich jak zabarwienie banknotów na skutek przypadkowej aktywacji systemu. Ważne jest również, aby doradzić opinii publicznej, aby nie przyjmowała zabarwionych banknotów. Z perspektywy długoterminowej akceptory banknotów powinny wykrywać zabarwione banknoty i powinny być instalowane w bankach i w placówkach komercyjnych, takich jak kasyna, myjnie samochodowe itp. Wykrywanie tuszu jest trudne i kosztowne, jednak opłacalnym rozwiązaniem może okazać się instalacja systemów na podczerwień, które wykrywają banknoty zabarwione markerami podczerwieni. Systemy te potwierdziły swoją skuteczność i są uznawane za najlepszą praktykę w Belgii i Francji. Po umieszczeniu w bankomacie banknotów z markerami podczerwieni urządzenie przyjmie („połknie") je, ale nie zaksięguje ich na koncie. System powinien również zarejestrować osobę wpłacającą zabarwione banknoty.

Podczas instalacji rozwiązań IBNS pojawia się jeszcze kilka innych kwestii. Kilku producentów oferuje szereg różnych rozwiązań IBNS z różnymi mechanizmami aktywacji i różnymi rodzajami tuszów. Pierwsza kwestia dotyczy faktu, że nie każdy rodzaj technologii aktywacyjnej IBNS jest w stanie przeciwdziałać wszystkim zagrożeniom. Niektóre systemy IBNS działają bardzo dobrze w przypadku prób wyrwania/staranowania, ataków *in situ* oraz ataków z użyciem gazu, ale nie są skuteczne w przypadku użycia stałych materiałów wybuchowych, lub odwrotnie. Dlatego też wybór technologii powinien być dokładnie przemyślany.

Inną kwestią jest rodzaj dostępnego tuszu. W Belgii ustanawia się minimalne wymogi krajowe dotyczące IBNS (bezpieczeństwo, procentowy zakres zabarwienia, możliwość zmycia itp.), a niezależne testy potwierdzają, że system spełnia normy krajowe i działa zgodnie z oświadczeniami producenta. Ważne jest, aby przeprowadzić test na prawdziwych banknotach, ponieważ na rynku dostępne są tańsze tusze, które dobrze sprawdzają się z podrobionymi/fałszywymi banknotami, ale nie z prawdziwymi, z których tusz można zmyć. Ponadto zaleca się dodanie do tuszu markera identyfikacyjnego, umożliwiającego powiązanie zabarwionych banknotów z konkretnym miejscem zbrodni.

Najlepsze praktyki pokazują, że systemy IBNS mogą być bardzo skuteczne, zwłaszcza w połączeniu z innymi środkami zapobiegawczymi. W 2015 r. Francja wprowadziła nowe przepisy, w tym paragrafy dotyczące instalacji IBNS z zastosowaniem tuszu z unikalnym DNA. To francuska policja wojskowa (żandarmeria) decyduje na podstawie oceny ryzyka, gdzie należy wdrożyć system IBNS oraz inne środki. Ponieważ nowe prawodawstwo wzmocniło podejście prewencyjne i operacyjne, liczba ataków spadła z 300 w 2013 r. do 50 w 2018 r.

Inną rozwijaną techniką dewaluacji łupu są systemy korzystające z **kleju**. Skuteczność kleju została udowodniona w Holandii, ale obecnie koszty wdrożenia i eksploatacji są dość wysokie. Ponadto klej może stanowić zagrożenie pożarowe, jeżeli system nie zostanie aktywowany przed atakiem, ponieważ uwolnienie cząstek kleju do powietrza może doprowadzić do powstania palnej mieszaniny. Metoda ta nie jest jeszcze gotowa do wprowadzenia na rynek, ale może być jednym z przyszłych rozwiązań.

3.2 Zwiększenie ryzyka

Druga oś zapobiegania fizycznym atakom na bankomaty polega na powstrzymaniu sprawców przed popełnianiem potencjalnego przestępstwa poprzez zwiększanie ryzyka wykrycia i ukarania. Oprócz ryzyka odniesienia fizycznych obrażeń podczas używania materiałów wybuchowych do ataku, głównym zagrożeniem dla przestępcy jest kara więzienia, jeśli został on złapany na gorącym uczynku lub po udanym śledztwie. Aby ostudzić zapędy potencjalnych sprawców, należy zwiększyć ryzyko

wykrycia i ukarania. W kontekście społecznym złapanie i skazanie przestępców jest oczywiście bardzo skuteczną metodą zapobiegania, jeśli w następstwie wymierzona zostanie odpowiednia kara, jak można to zaobserwować w niektórych krajach.

Wymiana informacji

Kluczem do wykrywania i karania osób włamujących się do bankomatów jest wymiana informacji między wszystkimi stronami zainteresowanymi walką z tego rodzaju atakami, w tym dostawcami bankomatów, organami ścigania (policją, prokuraturą itp.), organami publicznymi, producentami bankomatów i urządzeń bezpieczeństwa/ochrony, stowarzyszeniami zawodowymi, dostawcami bankomatów (bankami i jednostkami niezależnymi), firmami ochroniarskimi oraz centrami alarmowymi. Najlepszym rozwiązaniem jest współpraca zarówno na szczeblu krajowym, jak i międzynarodowym.

Wczesne wykrycie zbliżającego się fizycznego ataku na bankomat jest trudne. Jest to możliwe jedynie w przypadku niemal bezbłędnej wymiany informacji na szczeblu międzynarodowym między organami ścigania a partnerami prywatnymi (firmami ochroniarskimi i dostawcami bankomatów). Należy monitorować szeroki zakres wskaźników, w tym komunikaty ostrzegawcze między organami ścigania dotyczące ruchów ZGP, informacje o poszukiwanych pojazdach używanych w atakach, informacje od firm ochroniarskich lub straży sąsiedzkich na temat podejrzanych zachowań w okolicy bankomatów, podejrzane transakcje wykryte przez dostawców bankomatów oraz inne metody wykrywania. Inne możliwe działania policji pozwalające na wczesne wykrycie to monitorowanie skradzionych samochodów, producentów i dystrybutorów materiałów wybuchowych oraz firm upoważnionych do używania takich materiałów. Działania niezbędne do wczesnego wykrycia są wymagające i nie dają gwarancji sukcesu, dlatego interwencje organów ścigania przed atakami są rzadkością.

Jeśli wczesne wykrycie nie jest możliwe, w razie fizycznego ataku na bankomat centra alarmowe są w stanie szybko wydać ostrzeżenie. Aby umożliwić interwencję, należy uzgodnić i wdrożyć krajowe przepisy i protokoły dotyczące szybkiej komunikacji między centrami alarmowymi a organami ścigania. W przypadku wczesnego wykrywania oraz podawania informacji w czasie rzeczywistym organy ścigania zawsze będą musiały ocenić możliwości czasowe i ustalić najlepszy moment do interwencji. Łapanie przestępców na gorącym uczynku jest bardzo trudne i może prowadzić do niebezpiecznych sytuacji, ponieważ niektóre ZGP są bardzo brutalne i używają ciężkiej broni.

Aby przeprowadzić udane dochodzenie po fizycznym ataku na bankomat, funkcjonariusze organów ścigania muszą skomunikować się ze wszystkimi zainteresowanymi stronami, gdyż każda z nich może posiadać informacje, które przełożą się na powodzenie śledztwa. Oczywiście niezbędna jest komunikacja i współpraca z głównymi ofiarami, czyli bankami lub innymi dostawcami bankomatów – strony te mają dostęp do danych istotnych dla dochodzenia. W przypadku dostawcy bankomatu informacje otrzymane od organów ścigania przyczynią się do poprawy środków zapobiegawczych. Przydatne okazują się także kontakty ze stowarzyszeniami zawodowymi i producentami wysyłającymi często komunikaty alarmowe, z których korzystać mogą inne zainteresowane strony. Producenci bankomatów mają dobry wgląd w różne rodzaje ataków oraz związane z nimi słabe i mocne strony środków zapobiegawczych. Są oni bardzo chętni udzielić wsparcia policji, przekazując informacje na temat technicznych aspektów bankomatów i stosowanych metod działania.

Zasadnicze znaczenie ma współpraca transgraniczna: państwa powinny wymieniać się informacjami (o podejrzanych, skazanych włamywaczach do bankomatów, metodach działania, podejrzanych pojazdach, materiałach obrazujących ataki itp.), nie tylko w celu wsparcia śledztwa, ale również dlatego, że przestępcy skazani w innym kraju mogą zostać skazani za ponowne przestępstwo/recydywę.

Wreszcie, dzięki utworzeniu na szczeblu europejskim bazy danych dostępnej dla organów ścigania, zawierającej dane kryminalistyczne (np. na temat różnych rodzajów tuszów IBNS, znaczników i markerów lub szkła ochronnego do bankomatów), mogłoby zdecydowanie wesprzeć procedury dochodzeniowe oraz możliwość łączenia podejrzanych z konkretnymi miejscami zbrodni. Standaryzacja technologii na szczeblu międzynarodowym jest często niewystarczająca: podczas konferencji w styczniu 2019 r. uczestnicy wskazali, że funkcjonująca na poziomie UE normalizacja standardów obejmujących tusze i identyfikatory mogłaby znacznie ułatwić prowadzenie śledztw.

Systemy CCTV i urządzenia podsłuchowe

Dane obrazowe i dźwiękowe pochodzące z systemów CCTV oraz urządzeń podsłuchowych mogą wspierać zarówno proces wykrywania ataku w czasie rzeczywistym (np. w celu ochronienia przed odniesieniem obrażeń zespołów szybkiego reagowania przybywających na miejsce zbrodni), jak i późniejsze śledztwa (np. w celu identyfikacji sprawców i ich metod działania). Obrazy CCTV można łączyć z obrazami z publicznych i pozostałych systemów CCTV w sąsiedztwie bankomatu oraz nagraniami z radarów drogowych, aby zapewnić dokładniejszy obraz sytuacji – sprawców i sposobu ich działania.

Niestety obrazy CCTV są często słabej jakości lub są niewłaściwie przechowywane. Obrazy powinny być wystarczająco wysokiej jakości, aby umożliwić identyfikację danej osoby. Ustanowienie europejskich standardów systemów CCTV do celów ochrony ułatwiłoby prowadzenie dochodzeń. Ponieważ sprawcy często wyłączają kamery CCTV przed atakiem, można również rozważyć instalację ukrytych kamer CCTV lub urządzeń do podsłuchu w czasie rzeczywistym.

Karanie i resocjalizacja przestępców

Okazuje się, że konsekwentne i surowe kary stanowią swoisty środek zapobiegawczy. Aresztowanie ZGP ma natychmiastowy wpływ na liczbę ataków na bankomaty. Jednak zwolnienie z więzienia sprawców włamań do bankomatów często prowadzi do ponownego zwiększenia liczby ataków. Oznacza to, że krótkie wyroki doprowadzają sprawców do bardzo szybkiego, ponownego uaktywnienia się. Minimalne i maksymalne kary dla przestępców, skazanych za dany rodzaj fizycznego ataku na bankomat, różnią się w poszczególnych państwach członkowskich. Niektórzy uważają, że wyższe kary powstrzymają potencjalnych sprawców. Badania naukowe[5] wskazują jednak, że zwiększenie surowości kar niekoniecznie wpływa na zwiększenie efektu odstraszającego. Dlatego warto przyjrzeć się programom resocjalizacyjnym (skupiającym się na przestępcach) w celu ograniczenia wysokiego poziomu recydywy.

3.3 Zwiększenie wysiłków

Trzecia oś zapobiegania fizycznym atakom na bankomaty obejmuje działania, które utrudnią włamywaczom dokonanie przestępstwa.

Stworzenie środowiska odpornego na przestępstwa

Jeżeli ocena ryzyka (patrz powyżej) wykaże, że bankomat znajduje się w środowisku wysokiego ryzyka, należy rozmontować taką instalację, a bankomat przenieść w obszar niskiego lub średniego ryzyka. Takie działanie powinno mieć miejsce np. wtedy, gdy analiza wykaże, że budynek może się zawalić, jeśli bankomat zostanie zaatakowany przy użyciu materiałów wybuchowych. Można by wprowadzić przepisy egzekwujące zastosowanie takich środków w przypadkach wysokiego ryzyka. Oprócz zmniejszenia liczby bankomatów w środowiskach wysokiego ryzyka, powinno się zachęcać ludzi do płatności bezgotówkowych w celu zmniejszenia samego zapotrzebowania na bankomaty.

Jeżeli przeniesienie bankomatu nie jest możliwe, należy podjąć maksymalne środki bezpieczeństwa, stosując np. słupki zabezpieczające, latarnie i inne wyposażenie uliczne w celu ograniczenia dostępu do budynku, systemy zatrzymywania pojazdów, instalacje z odpowiednim oświetleniem ulicy, zwiększony nadzór jawny/niejawny oraz urządzenia zapobiegające kradzieży, jak systemy neutralizacji banknotów. W przypadku ataku na miejsce, które nie zostało uznane za środowisko wysokiego ryzyka, należy je za takowe uznać i wprowadzić dodatkowe środki bezpieczeństwa. Nowe czynniki należy uwzględnić w narzędziu oceny ryzyka, aby dokonać jego aktualizacji. Ponowna ocena tego ryzyka powinna być operacją powtarzaną cyklicznie.

Wzmocnienie bankomatów

Producenci oferują standardową gamę bankomatów posiadających szereg zabezpieczeń, które są oceniane według klas bezpieczeństwa ustanowionych przez Europejski Komitet Normalizacyjny (CEN). Na ogół bankomaty posiadają oznaczenie CEN z zakresu od niższej klasy CEN1 do najwyższej, CEN4. Klasę określa się na podstawie takich cech jak wytrzymałość obudowy czy odporność na ataki. Odporność na włamania z użyciem gazu jest najczęściej oferowana jako opcja (CEN-GAS). Zabezpieczenia standardowych modeli można rozszerzyć o dodatkowe środki ochronne. Zazwyczaj strony trzecie instalują te opcje w celu zapewnienia zgodności z lokalnym prawodawstwem i dostosowania podstawowego modelu do wymagań lokalnych klientów. Dodatkowe zabezpieczenia obejmują różne czujniki uruchamiające system neutralizacji gazów lub system IBNS w przypadku ataku *in situ* bądź ataku z użyciem materiałów wybuchowych, a także wzmocnione

rolety i zamki zapobiegające nieuprawnionemu dostępowi do sejfu w przypadku naruszenia rolety głównej. W przypadku mobilnych, wolnostojących bankomatów ważne jest zastosowanie systemów kotwiczenia, które zapewniają dodatkową ochronę przed atakami poprzez wyrwanie/staranowanie. Bankomat można wyposażyć w systemy śledzenia, aby wesprzeć organy śledcze w przypadku przetransportowania urządzenia w inne miejsce przed otwarciem.

Środki architektoniczne

Montując bankomat, zaleca się zastosowanie maszyn umożliwiających dostęp od tyłu. W takim przypadku sprawca, który chce ukraść gotówkę, musi wejść do budynku i uzyskać dostęp do tylnej części maszyny. Przenośne, samodzielne bankomaty są najbardziej podatne na zagrożenia. Zmniejszenie liczby tych urządzeń zwiększyłoby stopień bezpieczeństwa. Obowiązek instalowania bankomatów w pomieszczeniach odpornych na włamania automatycznie ograniczyłby korzystanie z wariantów wolnostojących.

System generowania mgły

Armatka mgłowa szybko wypełnia pomieszczenie gęstą mgłą, więc intruz nic nie widzi. Generator mgły często uniemożliwia przeprowadzenie ataku na bankomat. W najgorszym wypadku system spowolni sprawcę, dając policji czas na interwencję. System generowania mgły jest podłączony do układu alarmowego i może być aktywowany na dwa sposoby. Uruchomienie może nastąpić automatycznie dzięki czujnikom alarmowym, takim jak czujniki ruchu (w nocy) lub czujniki ingerencji w roletę bankomatu. System może być również aktywowany przez centrum alarmowe, co pozwala uniknąć zbyt wielu fałszywych alarmów. W przypadku zewnętrznych bankomatów ściennych można zastosować system mgłowy montowany w pomieszczeniu z tyłu urządzenia, co w razie aktywacji pozwoliłoby zmniejszyć do zera widoczność przestępcy.

Systemy mgłowe mogą zapewnić ochronę punktową bankomatu znajdującego się na otwartych przestrzeniach na stacjach benzynowych, supermarketach itp. Pozwala to uniknąć sytuacji, w której mgła wypełniłaby całą przestrzeń. Zabezpieczenie mgłowe jest najbardziej skuteczne, gdy mgła uwalniana jest z różnych kierunków lub gdy wypełnia przestrzeń za bankomatem w przypadku ataku poprzez staranowanie. Trwają badania w celu sprawdzenia, czy armatki mgłowe mogą być instalowane w samym bankomacie, zamiast w pomieszczeniu, w którym urządzenie się znajduje. Mgłę można wzbogacić o markery DNA, które poplamią sprawców i ich ubrania.

3.4 Środki równoległe

W celu zapewnienia wydajnego i skutecznego wdrożenia środków zapobiegawczych, o których mowa powyżej, należy rozważyć szereg środków równoległych. Środki te są niezbędne do umożliwienia lub wzmocnienia całościowego podejścia zapobiegawczego i operacyjnego pozwalającego walczyć z fizycznymi atakami na bankomaty.

Ustawodawstwo

W wielu krajach przepisy zobowiązują dostawców bankomatów do podejmowania środków zapobiegawczych. W innych krajach dobre podejście do przeciwdziałania fizycznym atakom na bankomaty zapewniają zawierane umowy i porozumienia między bankami a organami ścigania. Obszary, w których można rozważyć środki regulacyjne, obejmują:

- wprowadzanie środków zapobiegawczych;
- ramy prawne umożliwiające współpracę między organami ścigania a partnerami publicznymi i prywatnymi;
- ponowne opracowanie procedur skazywania, jeśli kary dla sprawców fizycznych ataków na bankomaty są zbyt łagodne.

Często jednak tylko instytucje bankowe są zobowiązane do przestrzegania przepisów i umów, a niezależne podmioty świadczące usługi bankomatowe nie są nimi objęte. Jest to wspólny słaby punkt ram prawnych.

Niektóre kraje nie wdrażają żadnych regulacji, lecz starają się przekonać dostawców bankomatów do podjęcia środków zapobiegawczych poprzez podnoszenie świadomości na temat obszarów przestępczości i panujących tendencji – w krajach o dużej liczbie niezależnych banków okazuje się to szczególnie trudne.

Należy koniecznie zapewnić, aby skuteczne wdrożenie środków zapobiegawczych obejmowało zmiany w prawodawstwie i regulacjach, zarówno na szczeblu krajowym, jak i międzynarodowym, wiążąc tym samym wszystkie typy dostawców bankomatów.

Najlepszym rozwiązaniem byłoby dostosowanie prawodawstwa na szczeblu UE, aby uniknąć sytuacji, w której zdecydowane środki zapobiegawcze zawarte w prawodawstwie jednego kraju nie zachęcały ZGP do przenoszenia się do innych krajów o mniej rygorystycznych przepisach.

Strategia medialna

Inną ważną osią strategii zapobiegawczej jest ugruntowana strategia medialna mająca na celu zmniejszenie oczekiwań i chęci przestępców do angażowania się w ataki na bankomaty. Należy położyć nacisk na niskie wskaźniki powodzenia i wysokie ryzyko ponoszone przez sprawców, natomiast należy unikać informowania o korzyściach („łupie") oraz szczegółach dotyczących ataku, takich jak rodzaj bankomatu czy sposób działania. Z drugiej strony konieczne są szeroko zakrojone kampanie informacyjne o aresztowaniach podejrzanych oraz karach, jakie muszą odbyć po skazaniu.

Rozszerzona współpraca

Rozszerzona współpraca i wymiana informacji zostały już wspomniane wiele razy, jednak należy podkreślić je jeszcze raz. Wymiana informacji operacyjnych na szczeblu międzynarodowym jest podstawą działalności Europolu. Oprócz niej, podczas konferencji prewencyjnej wykazano wyraźną potrzebę zwiększenia wielodyscyplinarnej i wielopoziomowej współpracy i wymiany informacji między wszystkimi zainteresowanymi stronami, w tym organami ścigania, organami publicznymi, producentami bankomatów oraz urządzeń bezpieczeństwa i ochrony, stowarzyszeniami zawodowymi, dostawcami bankomatów (bankami i dostawcami niezależnymi), firmami ochroniarskimi i centrami alarmowymi. Musi to dotyczyć szczebla lokalnego, krajowego i międzynarodowego.

Zmniejszenie ryzyka wystąpienia szkód ubocznych

W przypadku ataków z użyciem materiałów wybuchowych, niektóre ZGP pozostawią je na miejscu przestępstwa. Może to stwarzać niebezpieczeństwo dla zespołów szybkiego reagowania lub cywilów (mieszkających w sąsiedztwie lub przechodzących w pobliżu). Należy zapewnić im bezpieczeństwo. Tak jak ma to miejsce w Belgii, protokoły i procedury, które mają być przestrzegane przez zespoły szybkiego reagowania (zarówno organy ścigania, jak i podmioty świadczące usługi bankomatowe), muszą być opracowane tak, aby były do siebie dopasowane. Inną najlepszą praktykę w tym kontekście prezentuje Holandia, gdzie do oceny sytuacji wykorzystuje się nagrania ataków na bankomaty z kamer CCTV. W celu natychmiastowego udostępnienia tych obrazów można zawrzeć umowy z centrami alarmowymi.

Prewencja społeczna

Często ZGP rekrutują w swoje szeregi młodych ludzi. Można by przygotować projekty mające na celu osłabienie tego typu rekrutacji na wczesnym etapie. Policja lub pracownicy socjalni powinni zwracać uwagę na takie procedery i mogą interweniować, nawiązując osobisty kontakt z potencjalnych sprawcami.

04 WNIOSKI

W ciągu ostatnich 2 lat wzrosła liczba państw europejskich dotkniętych fizycznymi atakami na bankomaty. Europol i EUCPN nawiązały w tym zakresie współpracę, aby opracować najlepsze środki zwalczania i zapobiegania tego typu przestępczości.

Skuteczne podejście do zwalczania fizycznych ataków na bankomaty polega na połączeniu środków operacyjnych i zapobiegawczych, preferowanie wbudowanych w ramy prawne. Aby uniknąć sytuacji, w której zdecydowane środki stosowane w jednym kraju zachęcą ZGP do przeniesienia się do krajów bardziej narażonych, zaleca się przyjęcie tych środków na szczeblu europejskim.

Aby zapobiegać tego rodzaju przestępstwom i zwalczać je odpowiednio, należy opracować jasną strategię, bazując na trzech etapach: ocenie sytuacji, opracowaniu podejścia zapobiegawczego opartego na ocenie ryzyka i wdrożeniu środków zapobiegawczych.

Ocena ryzyka dotyczącego fizycznych ataków na bankomaty powinna obejmować cechy urządzenia i charakterystykę jego otoczenia, współpracę z partnerami i zainteresowanymi stronami mającą na celu zwalczanie tego typu przestępczości oraz ocenę ram prewencyjnych i prawnych. Po dokonaniu oceny sytuacji należy ustanowić strategię opartą na współpracy publiczno-prywatnej oraz środkach zapobiegawczych i operacyjnych. Celem środków zapobiegawczych jest obniżenie intencji i zdolności sprawcy do przeprowadzenia fizycznego ataku na bankomat. W tym celu proponuje się trzy osie działań zapobiegawczych: zmniejszenie korzyści, zwiększenie ryzyka i zwiększenie wysiłków. Dopełnieniem strategii zapobiegawczej powinny być środki równoległe. Najlepszą praktyką jest ustanowienie organu krajowego, uprawnionego do wdrożenia tych niezbędnych środków.

Zmniejszając korzyści, obniża się chęć kryminalisty do angażowania się w tego typu przestępstwo. Zmniejszenie ilości gotówki w bankomacie poprzez ograniczenie procesu jej uzupełniana tylko do kwoty wystarczającej na 1 dzień obrotu lub opróżnianie (najbardziej narażonych) bankomatów na noc to jedna z praktyk mających na celu zmniejszenie oczekiwań przestępców. Inną metodą jest dewaluacja łupu oraz sprawienie, że pieniądze można wyśledzić. W tym kontekście można zastosować system IBNS, który plami banknoty, oznaczając je jako skradzione. Metoda ta jest najskuteczniejsza, gdy przestępcy nie mogą wydać tych pieniędzy ani wprowadzić ich ponownie do legalnego obrotu gotówkowego. Jest to możliwe wtedy, gdy banki i społeczeństwo nie akceptują zabarwionych banknotów jako środka płatniczego oraz poprzez instalację akceptorów pieniędzy, które mogą wykrywać i odrzucać banknoty pokryte tuszem. Pod tym względem opłacalnym rozwiązaniem w Belgii i Francji okazały się inwestycje w systemy podczerwieni, które wykrywają banknoty ze znacznikami podczerwieni. Instalując systemy IBNS, kraje powinny dokładnie rozważyć dostępne mechanizmy aktywacji, minimalne wymagania dotyczące neutralizacji banknotów oraz dodanie do atramentu znacznika identyfikacyjnego.

Środki, które zniechęcają potencjalnych sprawców do popełniania przestępstw poprzez **zwiększenie ryzyka** wykrycia i ukarania, są drugą osią zapobiegania fizycznym atakom na bankomaty. Kluczowym elementem wykrywania i karania osób atakujących bankomaty jest gromadzenie i wymiana informacji między wszystkimi zainteresowanymi stronami, zarówno na szczeblu

krajowym, jak i międzynarodowym. Wymiana wysokiej jakości obrazów CCTV i danych dźwiękowych może zwiększyć szanse na wczesne wykrycie i pomyślne dochodzenie. Aby uniknąć ryzyka wyłączenia przed atakiem systemów CCTV lub urządzeń podsłuchowych działających w czasie rzeczywistym, można rozważyć instalację ich ukrytych wariantów. Stworzenie kryminalistycznej bazy danych i standaryzacja technologii na szczeblu europejskim mogłyby znacznie ułatwić międzynarodową współpracę i procedury śledcze. Jeśli przestępcy zostaną złapani i skazani, warto zastanowić się nad programami resocjalizacji (skupiającymi się na przestępcach) w celu ograniczenia wysokiego poziomu recydywy.

Trzecia oś zapobiegania fizycznym atakom na bankomaty obejmuje środki mające na celu **zwiększenie wysiłku**, jaki sprawca musi podjąć, aby popełnić przestępstwo. Zainstalowanie bankomatu w środowisku odpornym na przestępstwa i o maksymalnym poziome zabezpieczeń sprawi, że przestępcom znacznie trudniej będzie dokonać ataku. Ponadto standardowa ochrona bankomatu może zostać wzmocniona o szereg dodatkowych zabezpieczeń. Dopełnieniem całości jest instalacja systemu generującego mgłę, która może powstrzymać sprawcę lub przynajmniej spowolnić jego działania.

Wzmocnieniem wyżej wymienionych praktyk jest wprowadzenie szeregu **środków równoległych**, jak stworzenie ram prawnych, które zobowiążą wszystkich dostawców bankomatów do wdrożenia środków zapobiegawczych, opracowanie ugruntowanej strategii medialnej, zacieśnienie współpracy na szczeblu lokalnym, krajowym i międzynarodowym, określenie wytycznych dla zespołów reagowania w celu zmniejszenia ryzyka wyrządzenia szkód ubocznych oraz zainwestowanie w praktyki zapobiegania społecznego w celu osłabienia procesów rekrutacji w przestępczym świecie.

Factsheet

ZALECENIA DOTYCZĄCE PODEJŚCIA ZAPOBIEGAWCZEGO: PRZEGLĄD

Opracowanie skutecznej odpowiedzi mającej zapobiec fizycznym atakom na bankomaty

Ocena sytuacji

> Ustalenie profilu ryzyka związanego z bankomatami w danym kraju/regionie.

> Identyfikacja partnerów i zainteresowanych stron w walce z fizycznymi atakami na bankomaty oraz ocena współpracy.

> Ocena ram prawnych dotyczących zwalczania fizycznych ataków na bankomaty na szczeblu krajowym i międzynarodowym.

Opracowanie praktyk zapobiegawczych

> Określenie (głównego) ryzyka, przed którym należy się zabezpieczyć, oraz związanych z tym priorytetów.

> Określenie najlepszych środków zapobiegawczych dla tych zagrożeń poprzez rozważenie trzech głównych osi.

> Określenie środków równoległych niezbędnych do wzmocnienia podjętych środków zapobiegawczych.

Środki zapobiegawcze, które można podjąć w danej kategorii:

01

Zmniejszenie korzyści

> Zmniejszenie ilości gotówki.
  - Opróżnianie bankomatów na noc.
  - Zwiększenie częstotliwości uzupełniania gotówki.
> Dewaluacja łupu.
  - Inteligentne systemy neutralizacji banknotów (IBNS).
  - Znaczniki podczerwieni w tuszu IBNS do wykrywania zabarwionych pieniędzy przez akceptory banknotów.
  - Rozwijane rozwiązanie: klej.

02

Zwiększenie ryzyka

> Transgraniczne dzielenie się informacjami w celu:
  - wczesnego lub realizowanego w czasie rzeczywistym wykrywania potencjalnych ataków na bankomaty,
  - wzmocnienia podejścia operacyjnego,
  - skazywania osób ponownie popełniających przestępstwo,
  - wymiany danych kryminalistycznych na poziomie europejskim.
> Systemy CCTV i urządzenia podsłuchowe.
> Wymierzanie odpowiednich kar i resocjalizacja przestępców.

03

Zwiększenie wysiłków

> Tworzenie środowisk odpornych na przestępczość.
  - Zmienianie lokalizacji bankomatów wysokiego ryzyka.
  - Środki bezpieczeństwa: przeszkody fizyczne, nadzór itp.
> Wzmacnianie bankomatów o rolety, zabezpieczanie ich przed gazami i materiałami wybuchowymi itp.
> Środki architektoniczne, takie jak maszyny umożliwiające dostęp do tyłu urządzenia.
> Systemy ochrony generujące mgłę.

Środki równoległe umacniające podejście zapobiegawcze

> Skuteczne prawodawstwo, w tym środki zapobiegawcze przed fizycznymi atakami na bankomaty, wiążące się z nimi wyroki skazujące itp.

> Skuteczna strategia medialna zniechęcająca przestępców.

> Zacieśnienie współpracy między wszystkimi zainteresowanymi stronami (publicznymi, prywatnymi, organami ścigania) w walce z fizycznymi atakami na bankomaty.

> Zmniejszenie ryzyka wystąpienia szkód ponoszonych przez zespoły szybkiego reagowania oraz osoby cywilne (np. mieszkające w sąsiedztwie lub przejeżdżające obok).

> Prewencja społeczna uniemożliwiająca werbowanie młodzieży do tego typu grup przestępczych.

ENDNOTES

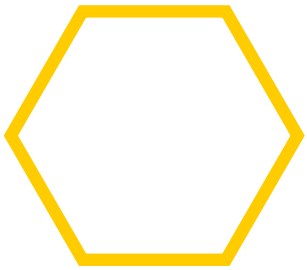
1 Willem Pieter de Groen, Zachary Kilhoffer i Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*, raport CEPS, 2018

2 Derek Cornish i Ronald V. Clarke, „*Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention*", Crime prevention Studies 16 (2003), 41-96.

3 Centrum voor Criminaliteitspreventie, barrieremodellen, www.barrieremodellen.nl

4 Decyzja Europejskiego Banku Centralnego w sprawie nominałów, parametrów, reprodukcji, wymiany i wycofywania banknotów euro, 2003.

5 David Weisburd, David P. Farrington i Charlotte Gill, „Conclusion: *What Works in Crime Prevention Revisited"*, David Weisburd, David P. Farrington i Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Cambridge: Springer, 2016, 311.



CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org, www.europol.europa.eu

TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN