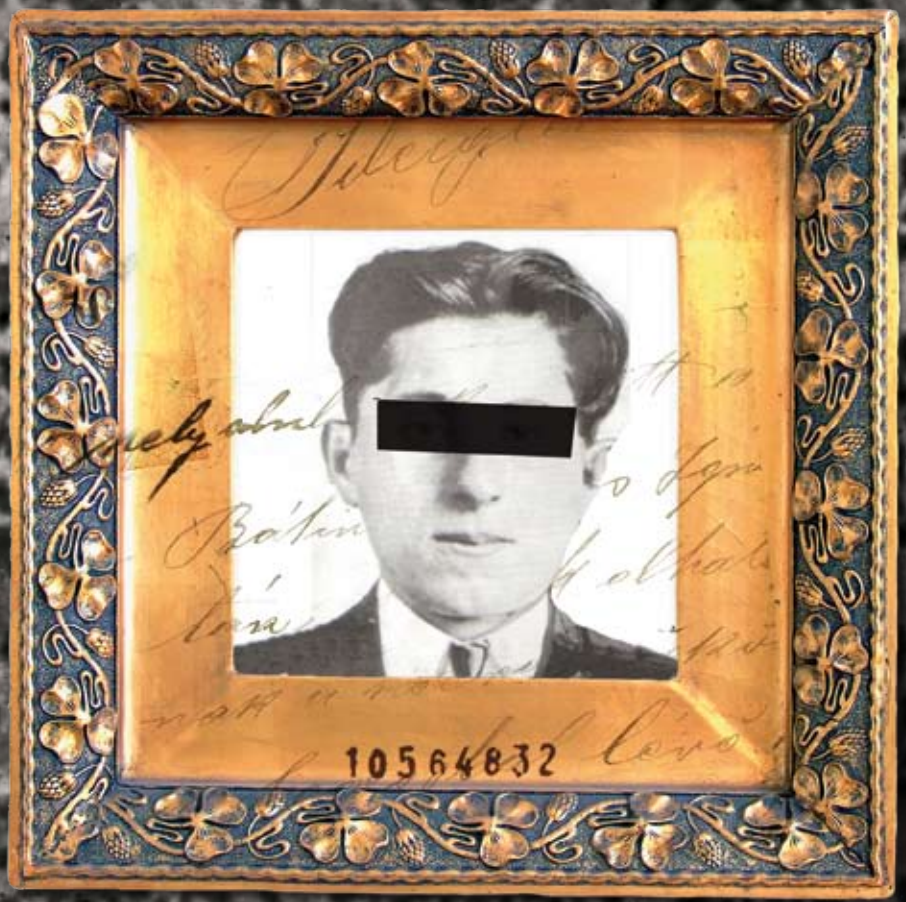
10564832

Autor
Justyna Sikorska

Ilustracja
Maciej Grzesiak

Pieniądz na wyciągnięcie ręki

Coraz łatwiejszy dostęp do usług finansowych kusi przestępców

Napady na banki to nie tylko fikcja amerykańskich filmów akcji czy westernów. Coraz częściej o takich przypadkach, mających miejsce w naszym kraju, słyszymy w mediach. W ostatnim miesiącu usłyszeliśmy o napadzie w jednym dniu na placówki bankowe w Warszawie i Łodzi, gdzie napastnik z bronią w ręku zmusił obsługę do oddania pieniędzy. W Rzeszowie zaś mężczyzna dokonał rabunku w SKOK-u terroryzując pracowników siekierą. Statystyki policyjne jednoznacznie wskazują, że nie są to sporadyczne przypadki. Problem przestępczości w polskim sektorze bankowym jest coraz poważniejszy.

Przestępca kalkuluje

Napadów przybywa, a przyczyn zjawiska podaje się kilka. Z jednej strony może to być sytuacja gospodarcza kraju skutkująca bezrobociem i biedą, czy też po prostu odwieczna żądza szybkiego i łatwego zysku. Z drugiej zaś strony rozzuchwala brak poważnych konsekwencji prawnych za działalność w grupach przestępczych.

– Niska wykrywalność czy przewlekłość prowadzonych spraw powoduje poczucie bezkarności i zachęca lub przynajmniej nie zniechęca kolejnych potencjalnych sprawców do napadów – mówi Mirosław Dembiński, wiceprezes Zarządu ds. Operacyjnych i Inwestycyjnych Spółdzielczej Kasy Oszczędnościowo Kredytowej im. Franciszka Stefczyka w Gdyni.

– Oczywiście dochodzi do tego łatwość przekraczania granic kraju po wejściu do Unii Europejskiej, co nie tylko zwiększa napływ ludności, ale i umożliwia łatwą ucieczkę – dodaje Wojciech Mikołajków, właściciel Agencji Ochrony Atos, zajmującej się ochroną placówek finansowych w mniejszych miejscowościach.

Kolejny element to łatwiejszy dostęp do pracowników instytucji finansowych, ułatwiający kontakt klientom. W reklamach wykorzystuje się często motyw załatwiania spraw przy kawie w bezpośred-

niej rozmowie z kasjerką. Zlikwidowano więc bariery, takie jak boksy kasowe czy okienka z szybami kuloodpornymi. Bywa i tak, że poszczególne placówki rezygnują z ochroniarzy, by klienci czuli się swobodniej. To wszystko zachęca potencjalnych sprawców do ataku – pieniądz wydaje się być niemal na wyciągnięcie ręki.

– Duże banki albo były budowane jeszcze w czasach, gdy bardziej dbano o bezpieczeństwo, albo w większości, ze względu na to, że obracają większą gotówką, muszą mieć zatwierdzony przez komendy wojewódzkie policji plan, który szczegółowo określa wszystkie kwestie bezpieczeństwa i ochrony placówki – wyjaśnia W. Mikołajków. – Małe oddziały nie mają takiego obowiązku i tylko spełniają podstawowe warunki firm ubezpieczeniowych.

Jak twierdzi szef ochrony, sprawca często kalkuluje zanim podejmie decyzję o napadzie. Najpierw obserwuje placówkę pod względem możliwości finansowych, ilości klientów (potencjalnych świadków, a może ofiar), odległości od policji, agencji ochrony, ewentualnych dróg ucieczki, no i czy jest monitoring, kamery, szyby kuloodporne, uzbrojona ochrona.

– Przy takiej kalkulacji małe oddziały bankowe stają się zdecydowanie łatwiejszym łupem dla przestępców – wnioskuje.

W 2007 r. policja odnotowała 89 napadów na placówki bankowe (w tym także na SKOK-i). W 2008 r. takich przypadków było 88 zaś w 2009 już 141. Tendencja wzrostowa niestety nadal się utrzymuje.

Rozzuchwala brak poważnych konsekwencji prawnych za działalność w grupach przestępczych

– Bezpieczeństwo placówek bankowych w Polsce to sprawa złożona i dotyka wielu obszarów. Jednym z nich jest bezpieczeństwo fizyczne takich miejsc. O ile duże jednostki praktycznie nie mają z tym problemu, o tyle te mniejsze, np. agencje czy małe oddziały, są bardziej narażone i najczęściej stają się celem przestępców. Nieduże to często jedno- lub dwuosobowa obsługa kasjerska, która ma bezpośredni dostęp do pieniędzy, ale niestety pracuje bez ochrony osobistej ani zabezpieczeń technicznych – wyjaśnia mł. asp. Agnieszka Hamelusz z Wydziału Prasowego Komendy Głównej Policji w Warszawie.

Drugą ważną kwestią jest bezpieczeństwo w bankowości internetowej oraz obszaru kart kredytowych.

Warto jednak pamiętać, że pieniądze są ubezpieczone. Klienci nie muszą się martwić o swoje fundusze zgromadzone w konkretnej jednostce finansowej.

Nie każda kamera widzi

W 2008 r. Centralne Laboratorium Kryminalistyczne przeprowadziło 17 ekspertyz zapisu monitoringu bankowego w ramach prowadzonych postępowań, ale niestety nadesłany materiał w znikomym stopniu pozwolił na identyfikację lub rozpoznanie osób czy przedmiotów zarejestrowanych podczas przestępstwa. Główną przyczyną jest instalowanie kamer niezgodnie z zaleceniami normy PN-EN-50132-7, która określa rozmiar obiektu na ekranie monitora.

– Zapisane na nośnikach wizyjnych obrazy sprawców są zbyt małe i nie nadają się do identyfikacji lub rozpoznania. Dodatkowym elementem, zdecydowanie pogarszającym jakość zapisów, jest nagminne stosowanie zbyt dużych współczynników kompresji zapisu, zmniejszenie rozdzielczości obrazu lub jednoczesne zastosowanie obu powyższych metod. Dzieje się tak ze względów finansowych lub z uwagi na potrzebę zmniejszenia objętości danych do celów archiwizacji. W wyniku takiego postępowania na jednym dysku twardym lub kasecie video umieszcza się zapis z kilku kamer z okresu obejmującego nawet kilka tygodni – mówi A. Hamelusz.

Stwierdzono również, że nagrania video dotyczą najczęściej zapisu o charakterze użytkowym, który przeznaczony jest dla służb ochrony obiektu i swoim zasięgiem obejmuje jak największe obszary. W przeważającej ilości badanych przypadków sprawcy zostali zarejestrowani przez systemy wizyjne, których zadaniem była obserwacja innych obiektów niż tych, gdzie nastąpiło zdarzenie.

Jak ważna jest dobra jakość systemu monitoringu, podkreśla także firma ochroniarska.

– W czasie samego napadu sprawcy są zamaskowani. Możliwe jest jednak, że któryś z nich robił rozeznanie w obiekcie tydzień, dwa lub miesiąc wcześniej i mógł się nagrać. Gdy się czymś interesujesz to na to patrzysz i nie ma lepszego ujęcia jak spojrzenie prosto w obiektyw kamery – mówi W. Mikołajków.

Poza tym kamery zewnętrzne mogły nagrać długo stojący samochód pod bankiem tydzień wcześniej i możliwe, że to nie był jeszcze ten kradziony, ale kogoś z rodziny sprawcy. Niestety, mimo iż dostępny jest w tej chwili bardzo dobry sprzęt, to jednak jego koszty sprawiają, że małe banki nie zawsze mogą sobie na niego pozwolić.

W ubiegłym roku komendant główny policji poprosił prezesa Związku Banków Polskich o rozważenie podjęcia konkretnych działań: poprawienie stanu technicznego telewizji przemysłowej, zapewnienie ochrony osobowej, zastosowanie rozwiązań umożliwiających zapobieżenie napadom tj.: umieszczanie w widocznym miejscu informacji o

zamontowanie systemu alarmowego oraz systemów zapisu wizualnego również na zewnątrz, zainstalowanie pomieszczeń przejściowych (śluz bezpieczeństwa), w których istnieje możliwość zatrzymania sprawcy bezpośrednio po napadzie, zastosowanie zabezpieczeń technicznych uniemożliwiających wejście sprawcy do pomieszczenia kasowego czy też zastosowanie rozwiązań umożliwiających ustalenie napastników przez przekazanie wraz z gotówką pakietów kontrolnych z farbą lub nadajnikiem GPS.

– Pomimo wzrostu liczby napadów na banki, wśród personelu i klientów nie odnotowano żadnych ofiar. Sprawdzają się zatem zastosowane środki organizacyjne, jak i procedury postępowania. Są one ciągle doskonalone, podobnie jak systemy zabezpieczeń, na które banki wydają rocznie miliony złotych. Niesłuszne są zatem opinie o ich słabości, gdyż w tej mierze banki stosują wszystko to co sprawdza się w Europie i na świecie. Trzeba pamiętać, że zabezpieczenia techniczne, chociaż mogą, acz nie muszą oddziaływać prewencyjnie na potencjalnego sprawcę, nie chronią przed samym napadem, o czym decyduje bandyta. Przydatne są natomiast w trakcie zdarzenia i pomagają w wykryciu sprawcy – komentuje propozycje komendanta Ryszard Woźniak, doradca prezesa NBP.

O dość dobrze funkcjonujących zabezpieczeniach w swoich placówkach przekonany jest także Mirosław Dembiński.

– Od wielu lat dbamy o wysoki standard urządzeń i systemów bezpieczeństwa, w tym także dla TV przemysłowej. Zapisy z naszych kamer zewnętrznych bywają także pomocne w schwytaniu sprawców rozbojów i napadów dokonywanych na terenie sąsiednich obiektów. Muszę przyznać, że mieliśmy ok. 120 zarejestrowanych tego typu zdarzeń, które przekazaliśmy policji w ramach dobrej współpracy.

W SKOK Stefczyka dla każdej placówki indywidualnie rozpatrywane jest ryzyko zagrożenia i na tej podstawie dostosowywane są systemy zabezpieczeń. Wykorzystywane są m.in. urządzenia spowalniające wypłatę gotówki, informacje o stosowaniu takich urządzeń w widocznych miejscach, systemy ukrytych kamer pomocnych w ujęciu sprawców, TV przemysłowa, kamery zewnętrzne.

– Instalowanie śluz bezpieczeństwa, w których istnieje możliwość zatrzymania sprawcy bezpośrednio po napadzie, to jednak nie jest najlepszy pomysł dla SKOK-ów. To rozwiązanie może być zasadne tylko dla dużych oddziałów bankowych czy skarbców i to zarówno z uwagi na koszty wykonania, jak i uwarunkowania lokalowe z koniecznością spełnienia wymogów ppoż. i BHP – wyjaśnia wiceprezes. – W przypadku małych placówek finansowych śluzy są mało praktyczne lub wręcz niewykonalne. Ponadto ich zastosowanie mogłoby generować ryzyko sytuacji, w której pracownicy lub klienci staliby się zakładnikami.

Wyodrębniono jednak tzw. pomieszczenie dużych wypłat, gdzie obsługuje się klientów przeprowadzających większe operacje finansowe. Jest tam monitoring telewizyjny i inne elementy systemów zabezpieczeń. Powszechnie stosowane są też dyskretne przyciski powiadomienia napadowego na wszystkich stanowiskach pracy, które przy odpowiedniej i niezwłocznej reakcji personelu skutecznie uniemożliwiają dokonanie napadu czy też przyczyniają się do schwytania sprawcy zdarzenia.

– Nadal funkcjonuje system kontroli wejść. Zabezpieczenia takie miały jednakże większą skuteczność w przypadku aranżacji placówek kasowych o wydzielonych, zabudowanych stanowiskach kasowych. Była wtedy szyba oddzielająca kasjerów od obsługiwanych osób, co utrudniało wtargnięcie napastnikowi – dodaje M. Dembiński. – Obecnie jednak, gdy standardem stają się tzw. otwarte stanowiska obsługi, to ograniczone wejścia koncentrują się na zapleczu obiektów, w tym pomieszczeń skarbcowych, gdzie przechowywane są warto-

1067D

ści pieniężne. Tu zastosowanie ma wydłużony czas zwłoki otwarcia, nawet do 1 godziny, system zdalnego monitorowania i kontroli dostępów do sejfów oraz wyodrębniony system ukrytych kamer.

Na stanowiskach kasjersko-dysponenckich stosuje się także urządzenia do czasowego przechowywania gotówki w formie dyspenserów, multisejfów bądź wrzutni gotówkowych.

Pakiety barwiące banknoty są już od kilku lat stosowane przez banki także w mniejszych miejscowościach. Niczym się nie różnią od zwykłej paczki. Działają po kilku minutach od momentu aktywacji, czyli odczepienia magnesu (czas przeznaczony, by sprawca zdążył opuścić bank). Wytwarzają potężne ilości dymu i proszku barwiącego. Dla banku jest to wystarczające zabezpieczenie, gdyż taka placówka dostaje 100 proc. zwrotu skradzionych pieniędzy z ubezpieczalni, zaś sprawcę łatwiej schwytać chociażby dlatego, że proszek jest trudno zmywalny. Pakiety z GPS są kosztowniejsze i nie wszystkie jednostki stać na taki wydatek.

– Jestem przeciwny różnym pułapkom na bandytów typu śluzy czy blokady. To niepotrzebne narażanie klientów i pracowników na niebezpieczeństwo i dalszy stres – komentuje W. Mikołajków.

Internet i karty

Bezpieczeństwo w bankowości to także obszar działalności internetowej, a przestępców kusi pozorna często anonimowość.

– Trzeba wyraźnie zaznaczyć, że najsłabszym punktem całego systemu jest klient, który nie sprawdza dokładnie strony, na którą wchodzi (a czasami jest to klon oficjalnej strony banku) i podaje nieuprawnionym dane ułatwiające dostęp do konta, umożliwiając im pobranie pieniędzy – informuje mł. asp. Agnieszka Hamelusz z KGP. – Jeśli chodzi o fałszywe strony internetowe to z reguły banki nie zgłaszają policji takich ataków. We własnym zakresie blokują tego typu strony broniąc się przed utratą wiarygodności

> Zapisane na nośnikach obrazy sprawców często są zbyt małe i nie nadają się do identyfikacji

O zachowaniu ostrożności mowa jest w materiałach informacyjnych serwisów internetowych, podręcznikach użytkownika i w umowach czy regulaminach usług.

– Informujemy o zagrożeniach technologicznych i zalecamy np. instalowanie oryginalnego oprogramowania czy programów antywirusowych, jak i profilaktyczne sprawdzanie adresu panelu logowania i stanu szyfrowania sesji – wyjaśnia M. Dembiński.

Próby wyłudzenia danych to w ostatnim czasie coraz częstsze metody przestępców. Dlatego instytucje finansowe, oferujące swoje usługi drogą internetową, coraz częściej informują, że nie będą przesyłały do użytkowników e-maili, w których będzie prośba o podanie jakichkolwiek danych osobowych oraz danych dostępu do konta. Podobny problem dotyczy dbałości o dane kart kredytowych i bankomatowych. Tych jest coraz więcej i ci, którzy nieumiejętnie, niezgodnie z zasadami posługują się „plastikowymi pieniędzmi", pozwalają wykonać kopię karty bądź dokonać transakcji przez osoby nieuprawnione.

– Notujemy również przypadki wyrobienia fałszywych kart przy współpracy z nieuczciwym pracownikiem banku. To jest jednak margines – dodaje A. Hamelusz.

Warto zachować także szczególną ostrożność przy wypłatach pieniędzy z bankomatów. Specjalne nakładki, kamery czy wręcz fikcyjne bankomaty – to narzędzia już znane przestępcom. Bardziej zagrożone są bankomaty, które rzadziej kontrolują pracownicy banków.

Psychologia złodzieja

– Jest wiele teorii mówiących, że rodzaj temperamentu, budowa ciała lub typ urody wpływa na zachowanie ludzi i na ich skłonności do popełniania różnych przestępstw – mówi Angelika Chiliczkowska, psycholog. – Psychiatra Kreatschmer wyróżnia cyklotymiców, czyli osoby o temperamencie zwróconym ku światu zewnętrznemu. Ich choroby psychiczne to najczęściej psychozy (np maniakalno-depresyjne). Natomiast schizotymicy, czyli osoby o temperamencie skoncentrowanym na swoim wnętrzu, chorują najczęściej na schizofrenie. Tacy ludzie popełniać będą różne przestępstwa. Darwin upatruje przyczynę przestępczości w genach. To one mają decydować o tym czy ktoś będzie bandytą i jakie przestępstwa popełni a jakich nie.

Te teorie wnoszą dużo do dalszych badań w dziedzinie psychologii, ale nie można na nich do końca polegać. Przestępczość jest zjawiskiem, które powstaje z wielu przyczyn, np. ekonomicznych, gdy zacierają się granice między wartościami i małe dzieci nie wiedzą czy cnotą jest bycie uczciwym, czy posiadanie fajnego samochodu. W zależności od wychowania w różnych środowiskach (tu jest też kolejny powód przestępczości) młodzi ludzie wybiorą czy chcą być uczciwi, czy nie. Wpływ też mają elementy losowe.

Nie ma polskiego portretu przestępcy – może być nim potencjalnie każdy. Ojciec, który chce znaleźć pieniądze na operację chorego dziecka, chłopak, który chce zaimponować kolegom, czy też pracująca w banku mama, której zamarzyły się zagraniczne wakacje. Ale niewątpliwie osoby planujące skoki na bank (zwłaszcza, gdy są to udane napady czyli nie zostali złapani), to osoby o wysokim ilorazie inteligencji, jak również psychopaci – bez skrupułów. Mogą to też być hakerzy. ■