doc. dr Jerzy KUCK
Tomasz PRAGACZ

Wyższa Szkoła Zarządzania Marketingowego i Języków Obcych w Katowicach

BEZPIECZEŃSTWO ŚRODKÓW PIENIĘŻNYCH W BANKACH I BANKOMATACH

Streszczenie. W opracowaniu zaprezentowano obszary zastosowania nowoczesnych technologii informatycznych do realizacji elektronicznego obiegu środków pieniężnych w bankach i bankomatach. Przedstawiono rolę jaką pełni Bankowy Fundusz Gwarancyjny, instytucja odpowiedzialna za zarządzanie systemem gwarantowania depozytów w Polsce. Ponadto omówiono zabezpieczenia w transporcie wartości pieniężnych i bezpieczeństwo w bankach i urządzeniach samoobsługowych. Proceder nielegalnego wyłudzania pieniędzy oraz współczesne metody kradzieży gotówki z kont klientów, omówiono prezentując równocześnie działania jakie podejmują banki aby zapobiec tym zagrożeniom.

SAFETY OF MONETARY MEANS IN BANKS AND CASH POINTS

Abstract. The fields where modern IT systems can be adopted for an electronic cash flow in banks and cash points are discussed here. The role of General Banking Risk Reserve as the institution responsible for management of guaranteed deposit system in Poland, as well as transport security of monetary means and safety systems in banks and self-service facilities are presented. Practices of obtaining money under false pretences and modern methods of stealing money from clients' accounts are described together with precautionary measures against them taken by banks.

Bezpieczeństwo w bankach

W dzisiejszych czasach ze względu na ogromny wzrost liczby rozliczeń pieniężnych oraz wymóg szybkiego ich przeprowadzania, elektroniczne przetwarzanie danych w bankach stało się koniecznością. Pomocną stała się nowoczesna technologia, w tym systemy informatyczne, które dają dużą oszczędność czasu pracy, ułatwiają gromadzenie wszelkiego rodzaju informacji, umożliwiają szybki dostęp do bazy danych. Dalsze korzyści to w powiązaniu z teletransmisją - stworzenie warunków do przekazywania danych między oddziałami, bankami, a także w obrocie zagranicznym[1]. Funkcjonujące w czasie rzeczywistym (on-line) systemy w bankach i bankomatach są narażone na ataki przestępców.

Współczesne zabezpieczenia w bankach i bankomatach utrudniają ale całkowicie nie wykluczają zagrożeń. Spektrum zagrożeń i zabezpieczeń ulega ciągłym zmianom. Obecnie znacznie częściej występują ataki z wykorzystaniem nowoczesnych narzędzi teleinformatycznych. Aby mieć możliwość porównania na wstępie przedstawiony zostanie przykład napadu z lat sześćdziesiątych. A dokładnie z 1962 roku gdzie w miejscowości Wołów na Dolnym Śląsku miał miejsce napad na bank. Plan napadu był przygotowany perfekcyjnie, nie była to jakaś oszalała improwizacja kilku narwańców. Złodzieje weszli do skarbca przez dziurę wyciętą w stropie. Do zrobienia dziury użyli samochodowego podnośnika. Z kasy zabrali 12 i pół miliona złotych w banknotach o nominałach 500 i 100 złotych. To była suma oszałamiająca, tak wielka, że nikt właściwie nie mógł sobie jej wyobrazić. Wygrana w Totolotka – największej grze loteryjnej w tym czasie wynosiła milion złotych i dla wszystkich był to szczyt marzeń. Skradzionych pieniędzy było tyle, że ówczesne władze zastanawiały się nad wycofaniem z obiegu wszystkich banknotów o tych nominałach. Miałoby to pomóc w ustaleniu sprawców. Ostatecznie odrzucono ten pomysł. Policja rozpoczęła intensywne poszukiwania. Sprawie nadano kryptonim W62. Policjanci spisali numery serii skradzionych banknotów i rozesłali je do wszystkich placówek handlowych na terenie polski. Na efekt nie trzeba było długo czekać. Kiedy schwytano złodziei, społeczeństwo przeżyło prawdziwy szok. Złodziejami okazali się spokojni obywatele, ojcowie rodzin, ludzie dobrze zarabiający i nie narzekający na nic. Po prostu chcieli spełnić marzenia z amerykańskich filmów. Mózgiem operacji był Stanisław J. elektryk, który w oddziale banku zakładał instalację elektryczną. Pan Stanisław dobrał sobie kilku kompanów. Był między innymi ślusarz do otworzenia kasy i kierowca, byli także trzej panowie mający za zadanie obezwładnić strażników, którzy stanowili jedyny istotny system bezpieczeństwa. Po skoku ustalono, że przez kilka lat żaden z członków

[1] W. Jaworski, *Bankowość, Zagadnienia podstawowe*, Poltext, Warszawa 2010.

gangu nie będzie pokazywał, jaki jest bogaty. Żadnych samochodów, nowych domów, żadnych drogich ciuchów. Pieniądze miały spokojnie leżeć pod łóżkiem i czekać, aż ludzie zapomną. Korzystać z nich należało z rozwagą. Plan był idealny, niestety pana Stanisława zawiodła własne małżonka, która od razu chciała poznać siłę swoich pieniędzy. Kiedy tylko poczuła w ręku gotówkę, pobiegła do sklepu na duże zakupy, za które zapłaciła banknotem, który miał spisany numer serii. Innego członka grupy zawiodła siostra, która uznała, że taką ilość gotówki najlepiej wpłacić na konto do banku, wychodząc z założenia, że pieniądze nie mogą leżeć w domu, jeszcze ktoś je ukradnie. Poszła z osiemnastoma tysiącami do banku w Pruszczu Gdańskim. Tam ją od razu zatrzymano. Od akcji do wyroku sądowego upłynęło zaledwie 4 miesiące. Najsłynniejszych złodziei Polski Ludowej skazano na 25 lat więzienia. Historia ta wydarzyła się wiele lat temu. Od tamtej pory kradzieże i system ochrony wartości pieniężnych w bankach uległ radykalnej zmianie[2].

Bankowy Fundusz Gwarancyjny

Na straży bezpieczeństwa w sektorze bankowym stoi Bankowy Fundusz Gwarancyjny. Jest to instytucja odpowiedzialna za zarządzanie systemem gwarantowania depozytów w Polsce. Do jej najważniejszych zadań należy zapewnianie zwrotu klientom depozytów zgromadzonych w bankach krajowych w przypadku ogłoszenia ich upadłości. Wysokość tych gwarancji regulowana jest ustawą o Bankowym Funduszu Gwarancyjnym. Obecnie jest 100% zwrotu, gdy wartość depozytu w złotych nie przekracza równowartości 100 tys. euro. Drugim najważniejszym zadaniem jest udzielanie pomocy bankom, których płynność finansowa została zachwiana. Innym ważnym zadaniem jest prowadzenie stałego monitoringu sytuacji na rynku bankowym, przeprowadzanie analiz oraz informowanie o wszelkich zagrożeniach związanych z prawidłowym funkcjonowaniem sektora. Fundusz ten sprawia, że większość klientów, którzy ulokowali swoje pieniądze na kontach bankowych może być spokojna o swoje oszczędności. Ponad to banki posiadają prywatne umowy ubezpieczeniowe[3].

Rola Państwa w ochronie wartości pieniężnych

Bankowy Fundusz Gwarancyjny to bardzo cenny element w systemie bezpieczeństwa bankowego, ale nie jedyny. Banki muszą chronić wartości pieniężne przed złodziejami oraz zapewniać bezpieczeństwo klientom korzystającym z usług tego rynku. O ten segment również dba Państwo Polskie. To ono wyznacza i narzuca standardy i minimalne poziomy zabezpieczeń między innymi w takich obiektach jak placówka bankowa. W dzisiejszej Polsce najważniejsze normy zostały zawarte w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 7.09.2010 r. Nosi ono tytuł: **„W sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne”**. Opisuje ona szczegółowe wytyczne i określa poziom zabezpieczeń według przechowywanej wartości pieniężnej, że w rozumieniu przepisów prawa wartości pieniężne to nie tylko gotówka, ale między innymi krajowe i zagraniczne znaki pieniężne, czeki, weksle oraz różne inne dokumenty zastępujące w obrocie gotówkę. Wszystkie banki na terenie państwa polskiego są zobowiązane do przestrzegania tych przepisów. Podstawowym i jednocześnie najważniejszym elementem tego rozporządzenia są tzw. „Jednostki Obliczeniowe”. Według definicji jedna jednostka obliczeniowa jest to 120-krotność przeciętnego wynagrodzenia w poprzednim kwartale ogłoszona przez Prezesa Głównego Urzędu Statystycznego w „Monitorze Polskim” czyli Dzienniku Urzędowym. Jako prosty, a zarazem bardzo obrazowy przykład przepisu z tego rozporządzenia można podać przełożenie się jednostek obliczeniowych na ilość konwojentów wymaganych do zabezpieczenia konwojowanej wartości. Aktualnie wygląda to następująco:

- 1 do 8 jednostek – 1 konwojent;
- powyżej 8 do 24 jednostek – 2 konwojentów;
- powyżej 24 do 50 jednostek – 3 konwojentów;
- powyżej 50 jednostek – 4 konwojentów.

Zaznaczyć należy, że konwojentem nie jest kierowca bankowozu ani osoba przenosząca wartość pieniężną. Jednostki te wskazują również na wymagany poziom zabezpieczeń obiektów takich jak placówki bankowe, urządzenia z gotówką oraz pojazdy do przewożenia wartości pieniężnych potocznie nazywane bankowozami[4].

[2] http://www.makbet.pl/artykul/302/skok-po-polsku, (17.03.2013)

[3] http://pl.wikipedia.org/wiki/Bankowy_Fundusz_Gwarancyjny (17.03.2013).

[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne. (Dz.U. 2010 nr 166 poz. 1128)

Zabezpieczenia w transporcie wartości pieniężnych

Zabezpieczenie pojazdów przeznaczonych do przewozu wartości pieniężnych na podstawie wcześniej wymienionego rozporządzenia przedstawia się następująco: banki i firmy konwojowe do przewozu wartości pieniężnych wykorzystują specjalnie przygotowane samochody tzw. bankowozy. Rozporządzenie ministra wskazuje trzy typy takich pojazdów: A, B i C. W bankach wykorzystywany jest typ A – są to pojazdy o najwyższym standardzie bezpieczeństwa. Pojazd typu A musi spełniać co najmniej następujące ogólne wymagania techniczne:

- konstrukcja z wyodrębnionym przedziałem ładunkowym;
- przedział osobowy z pięcioma miejscami do siedzenia oraz osłona zbiornika paliwa;
- kuloodporne oszklenie przedziału osobowego, bez możliwości otwierania;
- wyposażenie w system klimatyzacji i wentylacji wnętrza;
- przedział ładunkowy wzmocniony blachą stalową, tylko z jednymi drzwiami zewnętrznymi (w szczególności w postaci drzwi tylnych dwuskrzydłowych z blokadą ryglowania jednego skrzydła przez drugie i możliwością mocowania do ścian przedziału w położeniu otwartym) z zawiasami o sworzniach zabezpieczonych przed wybiciem oraz wyposażonymi w dodatkowy zamek, co najmniej w klasie A;
- pokrycie i wyłożenie powierzchni ścian, podłogi i sufitu oraz urządzeń i osprzętu wewnątrz przedziału ładunkowego o niskim stopniu palności;
- wyposażenie przedziału ładunkowego w oświetlenie;
- drzwi zewnętrzne z systemem centralnego blokowania oraz sygnalizacją ich niedomknięcia i odblokowania. Odblokowanie i zablokowanie drzwi z zewnątrz pojazdu z użyciem pilota radiowego lub urządzenia równoważnego, otwierającego tylko jedne drzwi i zamykającego równocześnie wszystkie drzwi pojazdu. Możliwość blokowania i odblokowania poszczególnych drzwi z tablicy rozdzielczej pojazdu. Co najmniej 3 drzwi w przedziale osobowym albo wyposażenie kabiny kierowcy oraz przedziału przeznaczonego do przewozu osób w wyjścia w postaci drzwi, okien lub włazów, umożliwiających w razie konieczności wyjście na zewnątrz;
- wyposażenie w monitorowany z zewnątrz system lokalizacji satelitarnej i system sygnalizacji napadu;
- komora silnika powinna mieć automatyczny system gaśniczy oraz zbiornik paliwa wykonany w sposób zabezpieczający przed wybuchem;
- bankowóz typu A powinien być wyposażony w modułowy samochodowy system alarmowy, posiadający co najmniej następujące właściwości:
  - ✓ funkcję "panika" włączaną i wyłączaną jednym przyciskiem pilota radiowego i dodatkowym wyłącznikiem wewnątrz przedziału osobowego;
  - ✓ rezerwowe zasilanie;
  - ✓ dodatkową syrenę alarmową;
  - ✓ czujniki ochrony wnętrza;
  - ✓ blokadę pracy silnika;
  - ✓ tryb serwisowy;
  - ✓ sygnalizację alarmową wszystkimi światłami kierunkowskazów.
- bankowóz typu A powinien być wyposażony w system transmisji alarmu przekazujący co najmniej informacje o:
  - ✓ położeniu i prędkości pojazdu;
  - ✓ otwarciu i zamknięciu drzwi przedziału ładunkowego i osobowego;
  - ✓ stanie alarmowania samochodowego systemu alarmowego;
  - ✓ włączeniu i wyłączeniu silnika pojazdu.
- urządzenia elektroniczne i elektryczne zamontowane w pojeździe powinny spełniać w zakresie kompatybilności elektromagnetycznej wymagania odpowiednich dyrektyw odnoszących się do tłumienia zakłóceń radioelektrycznych wywoływanych przez silniki z zapłonem iskrowym;
- koła pojazdu powinny być wykonane z wkładkami umożliwiającymi po przebiciu opony dalszą jazdę przez 15 km z prędkością około 50 km/godz;
- w bankowozie typu A nie dopuszcza się stosowania instalacji gazowej.

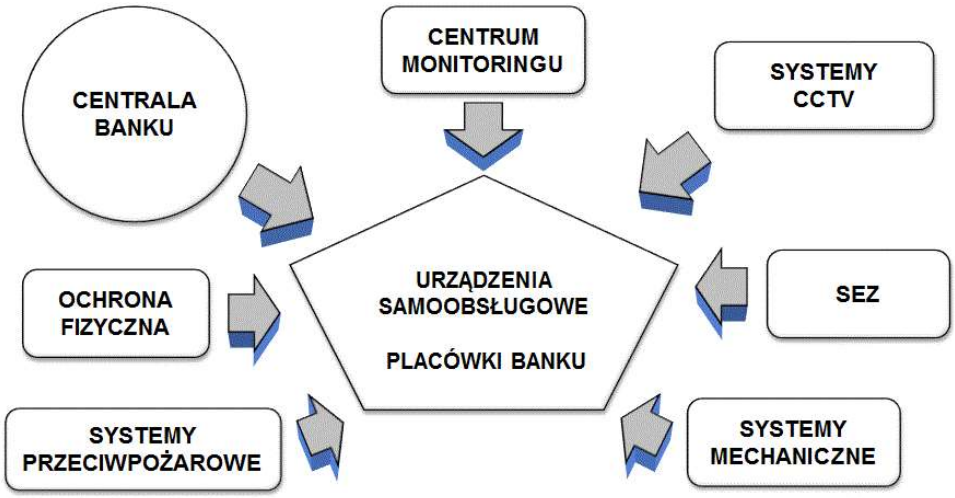
Taki pojazd to prawdziwa forteca na kołach. Dodatkowo podczas transportu wartości powyżej 24 jednostek bankowóz jest wspierany przez pojazdy ubezpieczające. Rozporządzenie mówi również o konieczności przewożenia i przenoszenia wartości pieniężnych za pomocą specjalnych pojemników. Są one podzielone na klasy, a ich poziom zabezpieczeń zależy o kwoty, jaką mają chronić.

- **Klasa A** - Pojemnik zamykany co najmniej jednym zamkiem kluczykowym lub szyfratorem, wyposażony w system paralizatora;
- **Klasa B** - rozszerzona jest o sygnalizacje akustyczną lub dymną;

- **Klasa C** - wyposażony jest dodatkowo w dwa zamknięcia oraz w system uszkadzający przechowywaną wartość;
- **Klasa D** - pojemnik tej klasy musi posiadać podobny system zabezpieczeń, ale o wyższej klasie niż C;
- **Klasa E** - najwyższy standard zabezpieczeń dodatkowo taki pojemnik wyposażony jest w system lokalizujący[5].

Bezpieczeństwo w bankach i urządzeniach samoobsługowych

Placówki bankowe oraz urządzenia samoobsługowe to obiekty wymagające szczególnej ochrony. W ramach wyjaśnienia urządzenia samoobsługowe to: bankomaty, wpłatomaty lub urządzenia dualne, łączące funkcje bankomatu i wpłatomatu ponad to są również wrzutnie online, offline, sejfy transferowe oraz kasomaty, opłatomaty (nowość w ostatnim czasie na polskim rynku). Sprawny system zabezpieczeń dla obiektów bankowych zawiera wiele elementów integrowanych w całość na podstawie tworzonego przez specjalistów planu ochrony danego obiektu. Taki plan dotyczy zarówno ochrony fizycznej, jak i elektronicznych oraz mechanicznych systemów zabezpieczeń. Zawsze musi uwzględniać regulacje prawne odnoszące się do zabezpieczeń placówek bankowych, a także wewnętrzne przepisy obowiązujące w danym banku. Tak jak i podczas transportu i przenoszeniu wartości pieniężnych tak i przy tworzeniu planu ochrony to właśnie jednostki obliczeniowe wyznaczają minimalny poziom zabezpieczeń. Jeszcze kilkadziesiąt lat temu ochrona banków była utożsamiana z uzbrojonymi w broń palną strażnikami, którzy byli jedynymi gwarantami bezpieczeństwa dóbr materialnych oraz zdrowia i życia klientów oraz pracowników. Obecnie banki zdecydowanie częściej stawiają na zabezpieczenia techniczne, a liczba ochroniarzy w placówkach bankowych systematycznie się zmniejsza. Głównym powodem ograniczania ochrony fizycznej są koszty. Zabezpieczenia techniczne są dużo tańsze i zdecydowanie pewniejsze. Bankowcy powołują się również na różne badania, z których wynika, że w trakcie napadu zabezpieczenia elektroniczne nie powodują takiego zagrożenia, jak obecność i możliwe działania pracowników ochrony. Wynika to m.in. z faktu, że obecność ochroniarzy może wywołać wyjątkowo agresywne zachowania napastników, co może obrócić się przeciwko pracownikom i klientom. Stosowane systemy zabezpieczeń są najwyższej klasy, o najlepszej niezawodności.



Opracowanie własne

Rys. 1. Schemat podmiotów uczestniczących w systemie zabezpieczeń placówek bankowych i bankowych urządzeń samoobsługowych.

Na schemacie wyszczególniono najważniejsze elementy systemu bezpieczeństwa stosowane do zabezpieczenia urządzeń samoobsługowych i placówek bankowych. W strukturze występują najczęściej takie elementy jak centrala banku. Centrala posiada wyspecjalizowane departamenty i wydziały zajmujące się monitoringiem różnego rodzaju transakcji. Kolejny element to bankowe centrum monitoringu i ochrona

[5] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne. (Dz. U. 2010, nr 166, poz. 1128).

fizyczna. Dodatkowo system ten wspierają i uzupełniają takie elementy jak: systemy CCTV, czyli telewizja przemysłowa służąca do monitoringu, kolejnym elementem jest SEZ, czyli różnego rodzaju systemy elektronicznych zabezpieczeń, następnymi elementami są zabezpieczenia mechaniczne, czyli różnego rodzaju kraty, szyby pancerne, sejfy, zamki i tym podobne. Całość zamyka system przeciwpożarowy[6]. Ilustruje to schemat przedstawiony na rys. 1.

Elektroniczne systemy zabezpieczeń (SEZ)

Elektroniczny systemem zabezpieczeń zwanym również SEZ'em. W jego skład wchodzą pojedyncze elementy zabezpieczeń elektronicznych, tworzących integralny system przeciwdziałający napadom i kradzieżom. System ten daje znacznie wyższy i pewniejszy poziom bezpieczeństwa pracownikom i klientom banków niż ochrona fizyczna. W skład takich systemów najczęściej wchodzą:

- centrala alarmowa, wyposażona w układ sterujący i integrujący cały system;
- manipulatory kodowe, za pośrednictwem tego urządzenia użytkownik komunikuje się z centralą np. włącza lub wyłącza alarm;
- różnego typu czujniki.

Mogą to być:

- pasywne czujki podczerwieni. Wykrywają zmianę temperatury;
- czujki magnetyczne montowane np. na oknach wykrywające ich otwarcie;
- czujki mikrofalowe inaczej zwane dopplerowskimi. Wysyłają one tak jak radar fale elektromagnetyczne i odbierają falę odbitą;
- czujki ultradźwiękowe odbierające sygnały akustyczne.

W bankach dodatkowo montuję się również:

- czujki sejsmiczne reagujące na drgania mechaniczne na powierzchni, której zostały zamontowane;
- czujki ciśnienia reagujące na zmianę ciśnienia w pomieszczeniu zamkniętym;
- czujki nacisku, montowane w podłożu.

Wykorzystywane są również:

- bariery podczerwieni. Urządzenie takie wysyła wiązkę podczerwieni trafiającą do odbiornika;
- czujki światłowodowe reagujące na próbę przejścia np. nad bramą.

Kolejnymi elementami i zarazem chyba najbardziej kojarzonymi z elektronicznym systemem zabezpieczeń systemu są sygnalizatory (urządzenia akustyczne lub akustyczno-optyczne), systemy wysyłające sygnał alarmowy do centrali monitoringu. Sygnał ten wysyłany jest za pomocą linii telefonicznych, pasm GSM oraz fali radiowych. Zazwyczaj jeden system ochrony posiada, przynajmniej 2 z powyższych sposobów przekazu sygnału. Przyciski i kody antynapadowe, włączane przez pracownika banku. Wysyłają one tzw. cichy alarm do centrali monitoringu. Cały ten system mogą uzupełniać tzw. Blokady, czyli urządzenia uniemożliwiające ucieczkę[7].

Kontrola dostępu

Istotną częścią całego systemu elektronicznych zabezpieczeń w bankach jest system kontroli dostępu. Jego zadaniem jest ograniczenie dostępu (pełnego lub czasowego) do sektorów chronionych przez ten system. Drugim jego zadaniem jest identyfikacja osób. W skład tego systemu wchodzą różnego rodzaju urządzenia np. manipulatory kodowe, czytniki kart, czytniki biometryczne, ale również oprogramowania chroniące nasze systemy komputerowe i różnego rodzaju aplikacje. Urządzenia te zintegrowane są z bazą danych. System na podstawie danych zebranych podczas konfiguracji decyduje o tym, czy w danej chwili użytkownik ma prawo dostępu do sektora i uruchamia procedury mające na celu zidentyfikowanie osoby, a następnie zezwolić lub zabronić przedostanie się użytkownika do danej strefy lub systemu komputerowego. Monitorowany jest również czas pobytu w takiej strefie. Próba wejścia do strefy przez nieuprawnionego użytkownika, może spowodować włączenie alarmu. Ponadto pracownicy firm zewnętrznych dokonujących różnego rodzaju prace np. na terenie placówki są weryfikowani i certyfikowani. Wcześniej bank zawiera z taką firmą umowę. W przypadku wykrycia nieprawidłowości, kradzieży to pracownicy tych firm są w pierwszej kolejności sprawdzani[8].

[6] http://www.zabezpieczenia.com.pl/monitoring/nowe-zabezpieczenia-bankowe-lx20-1ev-i-ex20-1pv (17.03.2013).
[7] http://pl.wikipedia.org/wiki/System_alarmowy (17.03.2013).
[8] http://www.zab-el.pl/?kontrola-dostepu,23&PHPSESSID=44d25f13acc5ef51052cedf55a3b4f1f (18.03.2013).

Zabezpieczenia kart płatniczych

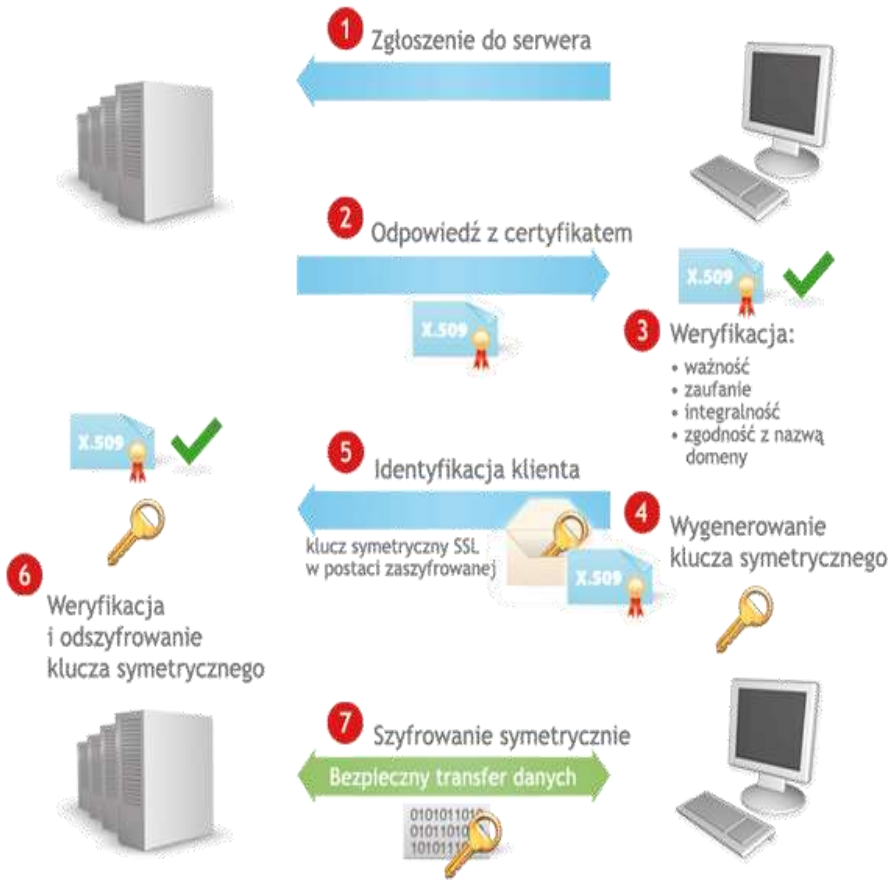
Aktualnie karty, którymi płacimy w sklepach, wypłacamy z bankomatów pieniądze mają kilka zabezpieczeń. Są to:

- 4-cyfrowe kody PIN;
- paski magnetyczne;
- chipy elektroniczne;
- oraz podpis.

Paski magnetyczne i podpisy to przestarzałe formy zabezpieczeń. Obecnie na świecie przechodzi się na technologię z chipami. Jednak na rynku nadal jest dużo terminali starego typu nieobsługujących mikroprocesorów zatopionych w kartach. Dlatego karty, które obecnie otrzymują klienci banków są tzw. kartami hybrydowymi, czyli posiadają obie formy służące do komunikacji z terminalem: pasek magnetyczny i mikroprocesor.

Zabezpieczenia systemu informatycznego

Zabezpieczenia i nadzór systemów przekazywania informacji ma miejsce codziennie.
Klient przychodzi do oddziału i składa dyspozycję wypłaty/wpłaty większej ilości gotówki. Oddział następnie wysyła taką informację elektronicznie do centrali zamawiając w ten sposób niezbędną ilość gotówki lub zapotrzebowanie na odsilenie z gotówki na dany dzień. Centrala banku przesyła tę informację do skarbca, a następnie skarbiec wysyła informację do centrali konwoju. Grupa konwojowa po odebraniu gotówki ze skarbca udaje się do wskazanej placówki.



Źródło: http://ssl.certum.pl/certyfikaty/certy,informacje_co_to_jest_certyfikat_ssl.xml (17.03.2013)

Rysunek 2. Certyfikaty SSL

W przypadku urządzeń samoobsługowych wygląda to nieco inaczej. Urządzenie przesyła sygnał do centrali banku o tym, że powoli kończy się gotówka lub urządzenie zapełnia się. Dalej wygląda to podobnie

jak w przypadku oddziału. Informacja trafia do skarbca, a następnie zostaje wysłana grupa konwojowa. Zanim pieniądze trafią do urządzenia, oddziału, a na końcu do klienta to dane o wysokości zamówienia, terminie realizacji i inne przechodzą przez wiele punktów. By taka poufna informacja nie trafiła w nieodpowiednie ręce w takich instytucjach jak bank stosuje się odpowiednie zabezpieczenia. Przykładem takiego zabezpieczenia jest między innymi poczta szyfrowana. Do szyfrowania służą certyfikaty SSL. Certyfikaty SSL są narzędziem zapewniającym ochronę, a także gwarantem zachowania poufności danych przesyłanych drogą elektroniczną. Pełne bezpieczeństwo jest efektem zastosowania szyfrowania komunikacji pomiędzy komputerami. Certyfikaty SSL rejestrowane są na określoną nazwę domeny, zawierają informacje o właścicielu domeny, jego adresie itp. Dane te są zabezpieczone kryptograficznie i nie można ich samodzielnie zmienić. Pracownikom banków uczestniczącym w obrocie gotówkowym nadawane są certyfikaty najwyższej klasy. Są one czasowe i wymagają odnowienia po upływie ważności[9]. Sposób działania takich certyfikatów ilustruje schemat przedstawiony na rys. 2.

Współczesne metody kradzieży gotówki z kont klientów banków i walka banków z tym procederem.

W obecnie ze względów bezpieczeństwa oraz rozwoju techniki coraz więcej placówek bankowych staje się oddziałami bezkasowymi. Całość transakcji gotówkowych przechodzi do urządzeń samoobsługowych. Ponad to oddziały powoli stają się reliktami i w niedalekiej przyszłości zaczną znikać. Kredyty, lokaty, ubezpieczenia i inne usługi bankowe staną się domeną Internetu. Razem z rozwojem techniki i zabezpieczeń rozwijają się metody kradzieży. Jest to nieustanny wyścig zbrojeń. Gdy tylko zostanie wykryta nowa metoda nielegalnego pozyskania środków pieniężnych z banku zostają uruchomione wszystkie niezbędne zasoby by takie zjawisko wyeliminować. Dzisiaj banki zaczynają działać wyprzedzająco, starają się przewidzieć działania niepożądane i przeciwdziałać im zanim jeszcze wystąpią.

Skimming – kopiowanie kart płatniczych

Na świecie w latach 80, a w Polsce później, bo w latach 90 pojawił się nowy sposób kradzieży pieniędzy z banków. Już nie napady, a **skimming** najbardziej zagraża zdeponowanym środkom w bankach. Według definicji skimming jest przestępstwem, polegającym na nielegalnym skopiowaniu zawartości paska magnetycznego, chip'a elektronicznego karty płatniczej, bankomatowej bez wiedzy jego posiadacza w celu wytworzenia kopii i wykorzystania do nieuprawnionych płatności za towary, usługi oraz wypłat z bankomatów. Możemy wyróżnić dwa rodzaje skimingu: skimming w placówce handlowej oraz skimming bankomatowy. Prób dokonania skimmingu w Polsce jak i na całym świecie jest wykrywanych kilkadziesiąt miesięcznie. Skala tego zjawiska obecnie jest bardzo duża. **Skimming w placówce handlowej**, polega na wykonaniu kopii karty przez sprzedawcę lub inną osobę, która weszła w jej chwilowe posiadanie. Najczęściej osoba dokonująca klonowania nie jest w takiej chwili w stanie poznać kodu PIN. Dlatego wykorzystanie takiej sklonowanej karty odbywa się w punktach gdzie nie jest wymagana autoryzacja transakcji kodem PIN. **Skimming bankomatowy**, polega na tym, że przestępcy instalują na bankomatach lub w ich wnętrzu specyficzne urządzenia, które służą do pozyskiwania danych z paska magnetycznego lub chipa oraz PIN-u takie jak kamery, nakładki czytników, fałszywa klawiatura lub płaska płytka obwodu umieszczona w czytniku na kartę, dzięki której można podsłuchać i zmanipulować komunikację między terminalem a chipem i uzyskać numer PIN. Zarejestrowane w ten sposób informacje są najczęściej transmitowane drogą radiową i służą do produkcji fałszywych kart, za pomocą, których możliwe jest pobieranie gotówki z kont klientów banków za pośrednictwem bankomatów.

Przykładowy sposób na instalację kamery za pomocą, której przestępcy próbują poznać nasz kod PIN przedstawia rys. 3. Istnieje wiele innych sposobów instalacji takich kamer. Jednym z bardziej popularnych jest instalowanie listew reklamowych u góry bankomatu z małą kamerką. Na urządzeniach samoobsługowych nie mają prawa znaleźć się takie elementy jak na rys. 3. Nie są one instalowane przez banki! Na rys. 4. przedstawiony został inny przykład próby zdobycia naszego kodu PIN.

[9] http://ssl.certum.pl/certyfikaty/certy,informacje_co_to_jest_certyfikat_ssl.xml (17.03.2013).

Źródło: http://www.kartyonline.net/arty.php?id=104 (17.03.2013)

Rys. 3. Nielegalna kamera na obudowie bankomatu

Źródło: Opracowanie własne na podstawie [http://www.kartyonline.net/arty.php?id=104, (17.03.2013)

Rys. 4. Klawiatury w urządzeniach samoobsługowych.

Jak widać na zdjęciach ciężko jest dostrzec różnice między oryginalną klawiaturą bankomatową, a nakładką zainstalowaną w celu poznania naszego kodu. Teraz zaprezentuje przykładowy wygląd bankomatu z nakładką szczytującą zawartość karty np. pasek magnetyczny. Ilustruje to rys. 5.

Źródło: Opracowanie własne na podstawie http://www.kartyonline.net/arty.php?id=104(7.03.2013)

Rysunek. 5. Czytniki kart w urządzeniach samoobsługowych

Na przedstawionych zdjęciach trudno jest dostrzec różnice między oryginalnym czytnikiem, a nakładką zainstalowaną przez przestępców. Osoby zajmujące się tym procederem wyspecjalizowały się w tworzeniu nakładek, montażu kamer w taki sposób by maksymalnie utrudnić ich wykrycie przez zwykłych klientów korzystających z urządzeń. Wiele z banków chcąc zminimalizować zagrożenie skimmingiem zaczęło instalować w urządzeniach własne nakładki tzw. anty skimmery. Na rys. 6. przedstawiono przykładowy wygląd takich anty skimmerów.

Źródło: http://kryzysowo.wordpress.com/2011/01/28/gdy-pieniadze-same-znikaja-nam-z-konta skimming-czym-jest-i-jak-sie-chronic/atm_anti_skimmer/ (17.03.2013).

Rysunek 6. Anty skimmer

W przypadku uszkodzenia takiego anty skimmera lub instalacji innego urządzenia na nim wypłaty są niemożliwe. To pozornie nieskomplikowane urządzenie posiada szereg zabezpieczeń. Jednak nie instalują ich wszystkie banki, a ich wygląd może znacznie różnić się od siebie, ponieważ na rynku występuje wiele różnych modeli i dostawców urządzeń samoobsługowych. W przypadku wątpliwości najlepiej udać się do

najbliższej placówki, do której należy urządzenie i zapytać, a nawet poprosić o sprawdzenie urządzenia. Pracownicy placówek mają obowiązek kilka razy dziennie sprawdzać podległe im urządzenia samoobsługowe, na pewno nie odmówią, gdy zwrócimy się do nich z taka prośbą. Obowiązek ten należy również do grup konwojowych. Ale do nich lepiej nie podchodzić, ponieważ podczas przenoszenia wartości pieniężnych czy obsługi urządzenia są bardzo wyczuleni na wszystkie osoby znajdujące się w pobliżu – stanowią dla konwojenta realne zagrożenie. Konwojenci zareagują błyskawicznie zgodnie z tym jak zostali wyszkoleni i przygotowani. Nadmienić należy, że są wyposażeni w broń palną z ostrą amunicją. Czy możemy sami uchronić się przed skimmingiem? Jest to możliwe, ale należy korzystać z kart płatniczych i bankomatowych, stosując zasady zwiększające bezpieczeństwo w tym:

- **nie przekazujmy karty innej osobie, jeśli nie jest to konieczne;**
- **nie zdradzajmy swojego kodu PIN;**
- **najlepiej zasłonić klawiaturę podczas wpisywania kodu;**
- **najlepszym rozwiązaniem jest korzystanie ze znanych nam urządzeń;**
- **nie zaszkodzi również rozejrzeć się i sprawdzić czy ktoś nas obserwuje;**
- **nigdy nie wyrzucajmy paragonu z urządzenia do najbliższego kosza!** Złodzieje tylko na to czekają. Na paragonie poza informacją o wypłaconej kwocie są dane o stanie naszego konta. Złodziej nie zaryzykuje aresztowania próbując okraść konto, na którym nic nie ma. Zdajmy sobie sprawę, że dokonanie przez złodziei operacji skimmingu jest dla nich bardzo ryzykowne. Dlatego potrafią wysypać zawartość kosza i sprawdzić go w poszukiwaniu paragonów z bankomatów. Wielu z nas zostawia je przy urządzeniu, co z punktu widzenia bezpieczeństwa jest niedopuszczalnym błędem. Jeśli już przeszkadzają nam paragony i nie chcemy ich zbierać to najlepiej potargać je na drobne kawałki lub wyrzucić dopiero w domu. Pamiętajmy, że w przypadku chęci złożenia reklamacji w banku paragon jest postawą takiej reklamacji.

W przypadku jakichkolwiek podejrzeń posiadacze kont Online sami mogą sprawdzić, jakie transakcje były wykonywane na rachunku. Warto od czasu do czasu skorzystać z tej funkcji, którą banki oddały mam klientom do dyspozycji[10].

Technologia zbliżeniowa, jako narzędzie walki z nieuprawnionym kopiowaniem kart

Dzisiaj sektor bankowy znajduje nowe sposoby na walkę ze skimmingiem. Na rynku polskim w roku 2007 pojawiły się karty z technologią zbliżeniową. Karty te umożliwiają dokonywanie transakcji bezstykowych w punktach handlowo-usługowych wyposażonych w specjalny terminal, który za pośrednictwem łącza radiowego odczytuje dane zapisane na mikroprocesorze zatopionym w karcie. Przy zakupach, których wartość nie przekracza aktualnie w Polsce 50 zł, transakcja nie wymaga potwierdzenia PIN-em. W przypadku, gdy wartość zakupów jest większa, transakcja nadal przebiega zbliżeniowo, ale użytkownik karty musi ją potwierdzić w sposób standardowy, wpisując PIN. Technologia zbliżeniowa to nie tylko karty, może zostać zaimplementowana np. w naszych telefonach, zegarkach i różnych innych nośnikach za pomocą, których dokonamy zapłaty za towary i usługi. Sprawdźmy czy nasz bank oferuję takie usługi, warto z nich korzystać. Celem tej technologii było nie tylko przyspieszenie dokonywania płatności, ale przede wszystkim sprawienie by klient już nigdy nie musiał wypuszczać swojej karty z ręki. Chroni to posiadacza takiej karty przed jej nieuprawnionym skopiowaniem, czyli tak zwanym skimmingiem w czasie dokonywania płatności w sklepie[11].

Kolejną nowością są urządzenia samoobsługowe wyposażone w technologię zbliżeniową. W 2012 roku Bank Śląski uruchomił pierwsze maszyny tego typu w Polsce. Jedna została zlokalizowana w Katowicach na ulicy Sokolskiej, druga w Warszawie na Placu Trzech Krzyży. Na obudowie urządzenia znajduje się specjalny czytnik, do którego przykładamy kartę, a następnie wstukujemy PIN-kod. W przeciwieństwie do płatności zbliżeniowych, każda transakcja, niezależnie od wartości musi być autoryzowana, żeby złodziej nie mógł skradzioną kartą wyczyścić nam konta. Dzięki tej technologii bankomaty staną się bezpieczniejsze, a zjawisko skimmingu przestanie istnieć. Warto zaznaczyć, że jest to jeden z pierwszych tego typu projektów na świecie. Podobne urządzenia można spotkać tylko w Hiszpanii. Obecnie jest to faza testowa, ale miejmy nadzieję, że sprawdzi się szybko znajdując uznanie po czym zostanie rozpowszechniona. Jednak, gdy banki eliminują jedno zagrożenie to złodzieje wyszukują inne metody by dobrać się do naszych pieniędzy[12].

[10] http://www.kartyonline.net/arty.php?id=104 (17.03.2013).
[11] http://encyklopedia.servis.pl/wiki/Terminal_POS (18.03.2013).
[12] http://thebanksquare.com/2012/11/14/pierwsze-bankomaty-z-technologia-nfc-juz-w-polsce/ (18.03.2013).

Phishing – nielegalne wyłudzanie poufnych danych

Kolejną nielegalną metodą jest zjawisko Phishingu. Według definicji Phishing, jest to wyłudzanie poufnych informacji osobistych takich jak hasła, loginy lub szczegóły karty kredytowej przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Instytucja taka jak bank nigdy nie poprosi klienta o podanie takich danych! Informacje te są poufne i należą tylko i wyłącznie do klienta, jeszcze raz zaznaczam, że banki ich nie potrzebują! Czy możemy się ustrzec przed tego typu zagrożeniem? Wydaje się, że tak jak i w wielu innych podobnych przypadkach zawsze wiele zależy od naszej czujności i odpowiedniej reakcji. Nie należy odpowiadać na maile, w których proszą nas o podanie takich poufnych informacji. Jeśli otrzymamy takiego maila najlepiej poinformować bank np. dzwoniąc na numer infolinii podanej na oficjalnej stronie naszego banku. Maile tego typu zazwyczaj są rozsyłane do wielu osób. Nasza właściwa postawa, czyli przekazanie informacji do banku może pomóc innym klientom. Bank szybko ostrzeże swoich klientów zamieszczając odpowiednie informacje na stronie internetowej oraz rozgłaszając ją w mediach. Nie bądźmy obojętni na takie zdarzenia[13].

W materiale, potwierdzono, że zmienił się poziom zabezpieczeń od czasów przytoczonej na początku artykułu historii. Już nie tylko uzbrojony strażnik jest gwarantem bezpieczeństwa klientów, pracowników i wartości pieniężnych, ale przede wszystkim dzisiaj stawia się na nowoczesne systemy elektroniczne i mechaniczne oraz wykonane przez wykwalifikowanych ludzi specjalistyczne plany ochronne. Opisane przykłady to zaledwie wierzchołek góry lodowej pokazujących zagrożenia, przed którymi stoją ówczesne banki. Podjęto także próbę przybliżenia metod stosowanych przez te instytucje do przeciwdziałania kradzieżom. Wiele ze szczegółów dotyczących metod i systemów z oczywistych względów jest objętych tajemnicą dlatego nie zostały w tym opracowaniu omówione. W dzisiejszych czasach banki chociażby chcąc przyciągnąć klientów będą stawiać na najwyższe standardy bezpieczeństwa. Potencjalny napad, utrata deponowanych środków swoich klientów zagraża reputacji takiej instytucji jaką jest bank i może wiązać się z utratą zaufania swoich klientów i odpływem ich do innego banku, który zapewnia większe bezpieczeństwo. Cegiełkę do całego systemu dokłada również Państwo wyznaczając podstawowe zasady funkcjonowania sektora oraz dając gwarancje ulokowanym przez nas środkom w postaci Bankowego Funduszu Gwarancyjnego opisanego na samym początku. Pamiętajmy również, że sami jesteśmy ważnym elementem w całym systemie dotyczącym bezpieczeństwa środków pieniężnych. **Bank dba o Twoje pieniądze, zadbaj o nie i Ty!**

Bibliografia

Akty prawne:

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne. (Dz. U. 2010, nr 166, poz. 1128).

Literatura:

Podręcznik e-marketingu. *Twój biznes w Internecie.* Komputer ekspert 04/2009.
Feldy M., *Sklepy internetowe.* Oficyna a Wolters Kluwer business Warszawa 2012.
Kuck J. *Nowoczesne technologie w logistyce,* AON, Warszawa 2013.
Tyrała P., *Refleksja nad teorią i praktyką bezpieczeństwa,* w: Lisiecki M., *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, Wyd. Wyższej Szkoły Zarządzania i Prawa, Warszawa 2008, wydanie II rozszerzone.
Tyrała P., *Sekuritologia. Bezpieczeństwo kompleksowe.* Wyd. Max – Druk Rzeszów 2010.

Strony internetowe:

http://www.makbet.pl/artykul/302/skok-po-polsku, (17.03.2013).
http://pl.wikipedia.org/wiki/Bankowy_Fundusz_Gwarancyjny (17.03.2013).
http://www.zabezpieczenia.com.pl/monitoring/nowe-zabezpieczenia-bankowe-lx20-1ev-i-ex20-1pv (17.03.2013).
http://pl.wikipedia.org/wiki/System_alarmowy (17.03.2013).
http://www.zab-el.pl/?kontrola-dostepu,23&PHPSESSID=44d25f13acc5ef51052cedf55a3b4f1f (18.03.2013).

[13] http://pl.wikipedia.org/wiki/Phishing (18.03.2013).

http://ssl.certum.pl/certyfikaty/certy,informacje_co_to_jest_certyfikat_ssl.xml (17.03.2013).
http://www.kartyonline.net/arty.php?id=104 (17.03.2013).
http://encyklopedia.servis.pl/wiki/Terminal_POS (18.03.2013).
http://thebanksquare.com/2012/11/14/pierwsze-bankomaty-z-technologia-nfc-juz-w-polsce/ (18.03.2013).
http://pl.wikipedia.org/wiki/Phishing (18.03.2013).

Recenzent: prof. zw. dr hab. Paweł TYRAŁA