Informatyka bankowa

informatyka bankowa

NR 9 2006 (9) ISSN 1895-5371

Wrzesień 2006

Miesięcznik specjalistów IT

Nie było nieprawidłowości w komputeryzacji PKO BP

Audyt przeprowadzony przez PKO BP wykazał, że zarzuty niegospodarnego przeprowadzenia informatyzacji banku mijają się z prawdą. Wybrana przez bank technologia Sun okazała się korzystniejsza zarówno pod względem cenowym, jak i technologicznym.

Bezpieczeństwo systemu bankowego

Visa Cashback już wystartowała; w pierwszym etapie gotówkę można wypłacać podczas zakupów za pomocą kart Visa wydanych przez PKO BP, MultiBank i mBank w sklepach obsługiwanych przez Polcard i eService.

Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych

Informatyka bankowa

Dr Zygmunt Ryznar

Bezpieczeństwo systemów bankowych

Bezpieczeństwo systemu bankowego to „delikatny" i złożony technicznie temat.. Nie da się na kilku czy nawet kilkunastu stronach omówić wszystkich kwestii, a ponadto zrozumienie niektórych z nich wymaga specjalistycznego przeszkolenia. Publikacji tej nie można więc traktować jako poradnik, lecz jako wprowadzenie zarówno do bankowych jak i technicznych aspektów zabezpieczania systemów.

Z wielu powodów systemy bankowe powinny być zabezpieczane w sposób wyjątkowo staranny. Zagrożenia mogą być wielorakie, a ochrona przed nimi jest często wyjątkowo trudna. Niebezpieczeństwo tkwi nie tylko w oprogramowaniu i urządzeniach zainstalowanych w systemie oraz sieciach komputerowych, lecz również w zachowaniach pracowników i klientów.

Należy pamiętać, że oszuści okradający klientów w rzeczy samej okradają bank (co najmniej z dobrego imienia i zaufania, a często i kapitału). Dotychczas szanowane powiedzenie „masz jak w banku" zaczyna przybierać rozmaite znaczenia. Dlatego bezpieczeństwo systemu bankowego powinno być jednym z głównych zadań regulacyjnych w skali całego banku i na wszystkich szczeblach obsługi klientów. Nie może ono podlegać bezwarunkowo regułom programu redukcji kosztów obsługi.

Wśród zagrożeń etyczno-organizacyjnych wymienić można :

- niestaranna - umyślna lub nieumyślna – identyfikacja klientów (sprawdzanie dokumentów, podpisów, poziomu zdolności kredytowej itp.)
- niewłaściwie określony zakres dostępu dla użytkowników systemu (każda klasa użytkowników bankowych powinna mieć indywidualnie skonfigurowane menu, z którego jedynym wyjściem jest wylogowanie się z aplikacji (zabezpiecza to przed możliwością wykonywania innych operacji i programów oraz komend systemu operacyjnego).
- umożliwienie programistom bezpośredniego – z pominięciem warstw pośrednich - dostępu do eksploatowanej wersji systemu (oprogramowania i baz danych), gdyż mogą oni w celu dokonania oszustwa modyfikować algorytmy (np. sposób zaokrąglenia kwot z generowaniem transferu różnicy na inne rachunki bankowe) lub też zmieniać zawartość baz danych używając narzędzi edycyjnych nie pozostawiających śladów audytowych, chwilowo zmieniać daty systemowe i czas (aby ukryć moment dokonania oszustwa) itp.
- umożliwienie (np. poprzez wprowadzenie fikcyjnego statusu „off-line") blokowania przesyłki wybranych transakcji z lokalnego serwera oddziałowego do serwera centralnego, wskutek czego nadużycia na kontach klientów dokonane przez pracowników oddziału mogą pozostawać w ukryciu (dzięki temu klient otrzymuje prawidłowe wyciągi ze swojego konta podczas gdy z jego salda zostały „wyprowadzone" pokaźne środki)
- fałszywy lub niepełny wydruk potwierdzenia transakcji dla klienta poprzez użycie niewłaściwego formularza (zawierającego inne nagłówki lub papieru węższego w celu pominięcia końcowych rubryk)
- dostęp nieuprawnionych osób do pomieszczeń serwerów, dysków, taśm i wydruków itp.
- dostęp nieuprawnionych osób do ewidencyjnych plików haseł, identyfikatorów użytkowników, kluczy teleksowych itp. lub niedbalstwo pracownika polegające np. na naklejaniu na obudowę monitora lub klawiatury karteczek z hasłami dostępu, nieniszczenie dokumentów (słynny amerykański włamywacz komputerowy Mitnick wyznał, iż większość haseł dostępowych uzyskał pracując jako sprzątacz w biurach).

- umyślne "podglądanie za plecami" wprowadzanych haseł, kodów PIN itp. obejmujące nie tylko podglądanie osobiste, lecz również poprzez urządzenia optyczne (np. kamery zainstalowane w bankomacie nad klawiaturą); w przypadku używania laptopów stosować można specjalną przejrzystą folię, która naklejona na ekran laptopa uniemożliwia czytanie informacji pod innym kątem.
- przypadkowe ujawnienie informacji wskutek wadliwego działania systemu lub błędu operatorskiego (np. przesłanie danych do niewłaściwego klienta, terminala lub stacji roboczej, wyrzucenie raportu z istotnymi informacjami do kosza, itp.) albo wskutek nieostrożności pracowników (np. głośne rozmowy służbowe przez telefon komórkowy poza miejscem pracy, pozostawianie informacji typu hasło, numery kart kredytowych w komputerach hotelowych, wykorzystywanych podczas podróży służbowej - aby usunąć ślady swojej pracy należy skasować wszystkie dokumenty, które były otwierane, wyczyścić schowek przeglądarki i plik z historią, oraz opróżnić kosz)
- umyślne działanie „cyber-złodziei" (np. crookerów i carderów – od oszustw kartowych) czy też włamywaczy komputerowych (tzw. intruderów, crackerów, hakerów)
- nadużycia popełniane przez aktualnych i byłych pracowników banku oraz klientów.

Jak wynika z powyższego, sporo zagrożeń tkwi w procesie uwierzytelniania czyli autentykacji i autoryzacji, opartych w systemie głównie na posługiwaniu się jedynie identyfikatorem i hasłem. Wydaje się niezbędne stosowanie dodatkowych zabezpieczeń jak tokeny, metody biometryczne itp. Autentykacja (authentication) polega na weryfikowaniu identyfikatorów klientów oraz węzłów sieci (użytkowników i serwerów) wewnętrznych i zewnętrznych. Następnym problemem jest niezabezpieczanie informacji na stanowisku pracy oraz luki w autoryzacji dostępu do zasobów, w wyniku czego poufna informacja staje się dostępna dla nieupoważnionych osób.

Nie można pominąć zagrożeń fizycznych, a tym zniszczenia lub unieruchomienia centrum obliczeniowego (umyślne lub przez czynniki losowe) a głównym zabezpieczeniem przeciwko temu jest równolegle zasilany danymi awaryjny komputer zlokalizowany w innym miejscu. Przykładem tego typu zagrożenia jest atak na WTC (World Trade Center) w dniu 11 września 2001 roku, który spowodował straty infrastruktury informatycznej na ponad 3 mld USD.

System bankowy zabezpieczany powinien być na poziomie systemu operacyjnego komputera, zarządzania siecią komputerową, aplikacji oraz poprzez przedsięwzięcia organizacyjne.

Na poziomie systemu operacyjnego i sieci dostęp do aplikacji najczęściej kontrolowany poprzez hasła (różne dla poszczególnych grup użytkowników) oraz nadawanie praw czytania, pisania, kopiowania, usuwania plików. Hasła powinny być zmienne w czasie, co może być wymuszane automatycznie przez system.

Zabezpieczenie sieci

O słabości całej sieci decydują nasłabsze jej ogniwa (przez nie można wprowadzić konia trojańskiego), każdy węzeł sieci musi podlegać tym samym rygorom, najlepiej zabezpieczać już na poziomie terminali i stacji roboczych (czyli tam gdzie można wejść do systemu). Wśród zabezpieczeń najpopularniejsze staje się stosowanie ścian zaporowych (firewalls mających na celu

wykrycie nieuprawnionych zewnętrznych i wewnętrznych użytkowników sieci), programów typu IDS (Intrusion Detection System) uzupełniających firewall oraz generowanie przez serwer bezpieczeństwa "biletów" (tokenów) użytkownika z hasłami ważnymi tylko na przeciąg sesji. Kontrola obejmować powinna wszystkie kanały sieciowe: e-mail, webmail, http, ftp, komunikatory i użytkowanie plików danych w trybie współdzielenia (file-sharing).

Rozwój łączności radiowej, satelitarnej stwarza szerokie możliwości omijania konieczności fizycznego podłączania się do okablowania sieci. W transmisji danych obowiązuje zasada szyfrowania danych przed ich wysłaniem lub użycia kodowanego tunelu w sieci VPN (Virtual Private Network).

Oprogramowanie kontroli dostępu do sieci może być rozmaite. Użytkownik może być zmuszany do wielokrotnego logowania się w ciągu dnia (do każdej aplikacji sieciowej) lub można mu zaproponować tryb pojedyńczego logowania Single Sign-On (SSO), czyli dostęp poprzez jedno hasło stowarzyszone z listą dostepnych dla niego zasobów w sieci. Pojedyncze (ale zintegrowane w skali sieci) uwierzytelnianie jest dla użytkownika łatwiejsze i mniej pracochłonne, a w sumie administrowanie siecią jest tańsze. Usługi administratorów związane z odnawianiem zapominanych haseł stanowią kto wie czy nie najbardziej pracochłonne i kosztowne (co najmniej kilkadziesiąt dolarów za 1 hasło) zadanie służby wsparcia technicznego. W przypadku SSO użytkownik ma do zapamiętania jedno hasło i id, po wprowadzeniu których pojawia mu się dostępne menu. Nie zmniejsza to bezpieczenstwa systemu, gdyż w przypadku wielu haseł użytkownik stosuje wspomagające „ściągi" (które można np. zostawić na stanowisku pracy) aby uniknąć pomyłek i wiążących się z tym blokad dostępu. Można stosować różne poziomy SSO: generalne (dostęp do zasobów w skali banku), internetowe (dostęp do portali i witryn internetowych oraz poczty elektronicznej), klasy aplikacyjne (dostep do grupy lub poszczególnych modułów systemu przetwarzania danych).

Szczególną ostrożność powinno się zachować w stosunku do sieci bezprzewodowych (WiFi), które ostatnio zyskują na popularności. Jeśli są one wykorzystywane do dostępu bankowego, to nie powinien nigdy wydarzyć się przypadek, że sieć taka „stoi otwarta" lub „prawie otwarta" (wskutek stosowania banalnych haseł), co jest łatwe do wykrycia przez tzw. wardriverów jeżdżących w pobliżu banków autami z laptopami z zainstalowanym netstumblerem, czyli programem (często bezpłatnym) do wykrywania sieci bezprzewodowych. Program ten potrafi rozpoznawać producenta punktu dostępowego, rysuje wykresy poziomu sygnału do szumów w danej sieci, umie współpracować z odbiornikami GPS. „Badaczami" sieci niekoniecznie muszą być specjaliści sprawdzający bezpieczeństwo sieci bezprzewodowych.

Innym problem jest identyfikator sieci ESSID (Extended Service Set ID), który jest rozgłaszany np. co sekundę i jest widoczny nawet do kilku kilometrów. Dobrze byłoby, gdyby był to ciąg niewiele mówiących znaków, znaczenie którego znane jest tylko przez uprawnionych użytkowników..

Szczególnego zabezpieczenia wymagają bankowe usługi internetowe

Do standardowych metod w tym zakresie należą:

- ściany zaporowe (firewall): ich zadaniem jest monitorowanie i filtrowanie pakietów danych krążących pomiędzy sieciami (np. wewnątrzną i internetową) pod kątem adresu IP (źródłowych i docelowych), protokołu transportowego (http, ftp) oraz portów; ściana zaporowa powinna być wyposażona w szczegółowe mechanizmy raportowania każdej próby nieautoryzowanego dostępu zaś w połączeniu z technologią proxy (dodatkowe pośredniczące zabezpieczenie pomiędzy użytkownikiem sieci wewnętrznej i internetowej) pamiętać powinna historię połączeń, włączając e-maile i wykonywane strony internetowe. W celu lepszego izolowania sieci zewnętrznej w ścianach zaporowych stosowana może być dodatkowa sieć zwana „strefą zdemilitaryzowaną„.
- bezpieczne połączenie SSL (Secure Socket Layer) 3.0. pomiędzy przeglądarką internetową a serwerem banku (zabezpieczenie transmisji poprzez szyfrowanie wiadomości, handshaking)
- blokowanie przesyłania danych do banku drogą nieszyfrowaną lub słabiej chronioną (np. degradacja SSL3.0. na SSL2.0)

- stosowanie metody szyfrowania ESP (Encapsulating Security Payload) polegającej na tym, że szyfrowaniu podlega nie tylko pakiet danych lecz również adresy nadawcy i odbiorcy oraz nagłówek autentyfikacyjny. W prywatnych sieciach wirtualnych (VPN) stosuje się tzw. tunelowanie (obudowanie/umieszczanie pakietów IP w innymi datagramach) mające na celu stworzenie bezpiecznego połączenia pomiędzy dwoma punktami znajdującymi się w tej samej sieci. Ulegają wówczas utajnieniu adresy obu stacji.
- certyfikat potwierdzający połączenie autentycznego użytkownika z autentyczną witryną banku (poprzez parę publicznego i prywatnego klucza)
- hasło zabezpieczające do klucza prywatnego
- stosowanie wirtualnej klawiatury do wprowadzania haseł
- identyfikator użytkownika (nadany przez bank)
- hasło użytkownika i blokowanie dostępu po kilku probach podania niewłaściwego hasła
- autentyfikacja poprzez "powitalne uściśnięcie rąk" (handshaking) polegające na wymianie ustalonych (i przepuszczanych przez funkcje "hashowania") komunikatów pomiędzy serwerem a użytkownikiem
- klucz sesyjny lub transakcyjny (token) z hasłami ważnymi tylko na przeciąg jednej sesji
- sygnowanie transakcji podpisem elektronicznym (ze zwalczaniem ataku typu man-in-the-middle MITM, w którym pomiędzy dwie strony połączenia ingeruje strona trzecia – atakujący, który może podmienić popisywany dokument na inny)
- oprogramowanie antyspamowe i antywirusowe (m.i. do wykrywania koni trojańskich i innych programów wchodzących „tylnymi drzwiami”, które same nie zdradzają swojej obecności).

Większość z powyższych metod ma na stwierdzenie autentyczności (non-repudiation) osoby dokonującej transakcji oraz ukrycie treści transakcji przed osobami niepowołanymi.

Komunikaty powinny być kompresowane, szyfrowane rozmaitymi metodami (kluczami i "hashami") i sygnowane podpisem elektronicznym oraz/lub tokenem aby maksymalnie utrudnić dostęp osobom niepowołanym (hakerom itp). Token jest to unikatowy ciąg cyfr działający tylko podczas wykonywania transakcji (sesji) przez klienta. Nazwą tą określane jest również urządzenie kryptograficzne do generowania takiego ciągu cyfr.. Bywają one rozmaite. Uruchomienie tokena czasem wymaga znajomości cyfrowego kodu (np. 6-znakowego), który właściciel urządzenia ustala sobie sam. Po kilku nieudanych próbach token jest zwykle automatycznie blokowany.

Podstawową metodą zabezpieczania treści wiadomości pozostaje szyfrowanie (kryptografia) danych za pomocą tzw. kluczy i złożone algorytmy "routowania" (mające na celu ukrycie drogi przebiegu informacji) oraz ciągła weryfikacja wszystkich procesów pojawiających się w sieci.

Istnieje wiele algorytmów szyfrowania, klasyfikowanych jako symetryczne lub asymetryczne. W metodzie symetrycznej do kodowania i rozkodowania używa się tego samego - generowanego -klucza tajnego. W algorytmie asymetrycznym komunikat po stronie wysyłającej jest szyfrowany dwoma kluczami: prywatnym (tajnym) strony wysyłającej oraz publicznym (jawnym) kluczem strony odbierającej.

Asymetryczność polega na tym, iż strona odbierająca używa do rozszyfrowania swój klucz prywatny (jako podstawa rozszyfrowania swojego klucza publicznego) i publiczny klucz nadawcy (jako podstawa weryfikacji podpisu elektronicznego nadawcy). Para kluczy (prywatny i publiczny) znajduje się we wzajemnej zależności matematycznej - takiej, że na podstawie klucza prywatnego łatwo oblicza się odpowiadający mu klucz publiczny, natomiast odwrotna zależność ("złamanie" klucza prywatnego na podstawie klucza publicznego) jest prawie niemożliwa do wykrycia - "prawie" gdyż zdarzył się przypadek odczytania klucza prywatnego OpenPGP przez czeskich kryptologów z firmy Decros/ICZ.

W praktyce - w celu przyśpieszenia transmisji danych - stosowane jest szyfrowanie hybrydowe, używające obu powyższych metod. Polega to na kodowaniu pełnej treści komunikatu za pomocą metody symetrycznej oraz stosowaniu szyfrowanych asymetrycznie elementów: skrótu elektronicznego i podpisu elektronicznego,. Skrót elektroniczny jest obliczany w taki sposób aby zapewnić spójność informacji, czyli wykryć ewentualne zmiany jakie mogą zajść podczas transmisji (w wyniku błędów przesyłania lub umyślnego zniekształcenia przez włamywacza). Po odebraniu i rozszyfrowaniu komunikatu skrót ten jest obliczany, a następnie porównywany ze skrótem odszyfrowanym z podpisu. Podpis cyfrowy polega na szyfrowaniu skrótu

wiadomości kluczem prywatnym nadawcy, zaś do jego odczytania niezbędne jest posiadanie przez odbiorcę klucza publicznego nadawcy. Warunkiem posługiwania się metodą asynchroniczną jest więc znajomość kluczy publicznych strony drugiej. Klucze te udostępniane powinny być przez centrum autoryzacyjne (Certification Authority) dysponujące bazą kluczy jawnych. Klucze udostępniane być mogą też przez internetowe serwery kluczy publicznych np. pgp-public-keys@keys.pgp.net. Właściciel klucza publicznego może usunąć swój "złamany" klucz i wprowadzić nowy.

Klucze publiczne przechowywane w repozytorium certyfikatów składają się z części nagłówkowej (nazwy właściciela i daty utworzenia) i materiału kodowego, natomiast klucze prywatne szyfrowane są dodatkowym hasłem.

W celu zabezpieczenia transmisji danych protokół HTTP wzbogacany jest o mechanizmy szyfrujące, np. SSL (Secure Socket Layer) stosujący cyfrowe certyfikaty i podpisy, szyfrowanie symetryczne i niesymetryczne skompresowanych danych i zabezpieczenie przed zmianami poprzez kody MAC (Message Authentication Code).

W ramach aplikacji *zabezpieczenie polegać może na:*

1. bardzo szczegółowym rozpisaniu menu czynności dla klas użytkowników wraz z uprawnieniami wykonywania poszczególnych funkcji i transakcji (powinno być to włożone do infrastruktury pojedyńczego logowania SingleSign-on)
2. zablokowaniu modyfikacji przez zwykłych użytkowników lub programistów zawartości określonych pól „systemowych” (np. stóp procentowych), zastrzeżonych dla uprawnionych administratorów
3. przydziale limitów kwot dla niektórych typów transakcji (do ich wprowadzania i autoryzacji) zróżnicowanych dla grup personelu (kierowników, dysponentów, kasjerow i dilerów)
4. stosowaniu zasady w stosunku do niektórych typów operacji (np. transakcji stornujących, przerzutu rachunków pomiędzy klientami), iż akceptacja transakcji lub jej odwołanie mogą być wykonane przez inną osobę, niż osoba dokonująca transakcji.
5. zastosowaniu takich zasad integralności danych, aby zabezpieczyć się przed niezależnymi" od aplikacji (np. za pomocą systemowych procedur lub edytorów) zmianami informacji, takimi jak zmiany w bazach danych, w tablicach systemowych, "poprawianie " danych archiwalnych, itp.
6. zapewnieniu realizacji wszystkich kroków transakcji zgodnie z zasadą ACID
7. wykluczeniu w aplikacji możliwości usuwania transakcji (zamiast niej należy stosować transakcje stornujące zwane czasem rewersyjnymi)
8. rejestracji dokładnych śladów audytowych
9. wiarygodnej identyfikacji klienta (np. na podstawie dokumentów, podpisu, karty chipowej, pomiaru biometrycznego: dynamicznego podpisu, odcisków palca, wielopunktowego skanowania dłoni, geometrii i linii dłoni, kształtu twarzy, obrazu tęczówki oka, głosu itp.)
10. stosowaniu dodatkowego hasła dla wybranych transakcji.
11. przejściu na specjalny tryb obsługi w przypadku awarii sieci i braku dostępu do serwera centralnego (zwykle stosowane sa wówczas ograniczenia np. wypłat gotówkowych).

Poniżej omówimy bardziej szczegółowo niektóre z zabezpieczeń.

System bankowy powinien automatycznie rozpoznawać czy oddział znajduje się w stanie on-line (podłączony) czy off-line (odłączony), aby wywoływać odpowiednie programy obsługowe z odpowiednim poziomem bezpieczeństwa..

Przy wystąpieniu awarii linii system powinien być więc automatycznie przełączany na tryb off-line, ukazując odpowiedni komunikat na stanowiskach w oddziale, którego dotyczy awaria. W trybie off-line transakcje są przechowywane w specjalnych plikach, zaopatrzonych między innymi w sumy kontrolne. Pojemność pamięci dyskowych servera oddziałowego powinna być dostateczna do zapisu transakcji co najmniej w ciągu 24 godzin. Po zaniku awarii system powinien automatycznie uruchamiać funkcje uzgadniania centralnej i lokalnej bazy danych (ściągania danych transakcyjnych z oddziału, który znajdował się w stanie off-line, oraz niezwłoczną aktualizację centralnych baz danych). Oprogramowanie awaryjne powinno być przygotowane na wielokrotne awarie telekomunikacyjne, w tym awarię podczas uzgadniania baz danych. Wznowienie pełnej obsługi klientów poprzez przejście na tryb on-line powinno być uwarunkowane kompletnym wykonaniem czynności poawaryjnych. W przypadku wielokrotnych lub dłuższych awarii dogodną porą uzgodnień danych może być ostatecznie pora nocna.

W aplikacjach transakcyjnych każda transakcja powinna być obsługiwana zgodnie z właściwościami zwanymi ACID (atomicity-atomowośc, consistency-spójność, isolation-izolacja, durability-trwałość). Atomowość polega na tym, iż zgodnie z zasadą "wszystko albo nic" system wykonać musi *wszystkie* kroki składające się na obsługę transakcji (w każdym innym przypadku nie powinna ona pozostawić skutków)"). Zasada spójności gwarantuje poprawność powiązań w skali całej bazy danych, zaś zasada izolacji oznacza iż nie występują negatywne skutki współbieżnej obsługi wielu transakcji (każda z nich może być "izolowana"). Zasada trwałości polega na tym, iz zapewniona jest możliwość odtworzenia rezultatu transakcji w przypadku awarii.

Aplikacja powinna być wyposażona w . procedury odzyskiwania danych (np. oparte na tzw. dziennikowaniu lub backupie przyrostowym) w przypadku awarii powodującej zniszczenie części danych. System zapewnić powinien pełne ślady błędów przetwarzania, umożliwiające identyfikację przyczyny błędu oraz miejsce jego wystąpienia (w jakim programie lub funkcji oraz linii lub instrukcji).

Większość zagrożeń bezpieczeństwa systemu bankowego tkwi zapewne wewnątrz banku. W serwisie DataPro „The Worldwide IT Analyst" przed paru laty podano, iż statystyka zagrożeń wygląda następująco: 5 % wirusy i hackerzy, .15 % zagrożenie fizyczne, 20 % nieetyczni pracownicy (i klienci), 60 % błędy i przeoczenia personelu. Wg KPMG [http://searchsystemsmanagement.techtarget.com/news] z końca 2001 r. 80% włamań dokonywanych jest wewnątrz firm a nie przez zewnętrznych włamywaczy. Dotyczy to zarówno użytkowników jak i programistów. Rozwiązaniem utrudniającym dokonywanie nadużyć przez programistów banku jest podział oprogramowania i baz danych na kilka całkowicie izolowanych (w aspekcie dostępu) od siebie warstw dla poszczególnych etapów budowy i testowania systemu oraz bezwzględne niedopuszczanie programistów do warstwy eksploatacyjnej (produkcyjnej). Z ich strony istnieje zagrożenie, iż mogą zmodyfikować dane w systemie poprzez swoje narzędzia a nie poprzez aplikację, nie pozostawiając żadnych śladów w dziennikach transakcji, tylko w tzw.logach, których sprawdzenie wymaga dużo czasu i kwalifikacji niedostępnych przeważnie audytorom wewnętrznym banku. *Każda z warstw powinna być w pełni izolowana*, to znaczy posiadać swoje klasy użytkowników, swoje definicje produktów, swoje oprogramowanie aplikacyjne i swoje bazy danych. Idealną izolację zapewniają oddzielne komputery dla poszczególnych warstw. Można stosować też warstwy na wspólnym komputerze z odpowiednio wysoką klasą zabezpieczenia (np. w grupie B standardów międzynarodowych). Liczba warstw może być znaczna w zależności od zakresu prowadzonych prac modyfikacyjnych. Nadużyciom ze strony użytkowników przeciwdziała się głównie poprzez uprawnienia na poziomie funkcji i czynności menu oraz limity kwotowe nadawane klasom użytkowników. Przejście zmian od warstwy pośredniej do warstwy produkcyjnej następować powinno po jawnym (z pozostawieniem informacji, kto i kiedy zatwierdził zmiany). Ten tryb organizacji prac jest trudny do utrzymania w sytuacji, gdy w systemie występuje wiele błędów i z punktu widzenia nadzorujących „nie ma czasu na biurokrację" (przy okazji unikają oni własnej

odpowiedzialności). Szczególnie dotyczy to postępowania awaryjnego, szczególnie w przypadku konieczności ręcznej korekty danych przez większą liczbę liczba osób.

Bezpieczeństwo internetowych transakcji bankowych zależy nie tylko od systemu bankowego, lecz również od zachowania klienta i zabezpieczeń komputera z którego on korzysta.

Jeśli jest to komputer zupełnie pozbawiony ściany zaporowej i osłaniających programów antywirusowych, wówczas bank może być zupełnie „niewinny" gdy jego dane podczas logowania zostaną ukradzione przez program śledzący i odesłane do hackera i ten w naszym imieniu zrealizuje transakcję. Fiszing (phishing) jest łatwiejszy w przypadku niestosowania tokenu lub „zdrapek", ale również wtedy nie można wykluczyć oszustw, aczkolwiek trudniej jest je zrealizować. Przypadki takie zanotowano również w naszym kraju.

Popularną metodą przejmowania danych (w tym jednorazowych haseł) są wirtualne witryny bankowe do złudzenia przypominające oryginalny serwis. W fikcyjnej witrynie można przechwycić wszystkie informacje, wyświetlić klientowi potwierdzenie przelewu, a następnie wykorzystać identyfikator (id) użytkownika i „ukraść" hasło do zlecenia przelewu. Dlatego trzeba bacznie obserwować witrynę bankową np. czy działa w trybie szyfrowanym (chociaż zdarza się, że i „kłódki" potwierdzające szyfrowanie są falszywe) czy występują wszystkie szczegóły (np. w menu) jak zwykle.

Nierozważne zachowanie klienta polega też na wykonywaniu transakcji w publicznej kawiarence internetowej lub w trybie bezprzewodowym (hotspot). Korzystanie z bezprzewodowych publicznych punktów dostępowych może wiązać się z koniecznością wyłączenia szyfrowania WEP (Wired Equivalent Privacy - starsza metoda szyfrowania) lub WPA (Wi-Fi Protected Access), co oczywiście wpływa na bezpieczeństwo transmisji (możliwość przejęcia takich poufnych danych jak nazwa użytkownika, hasło itp.). Nawet w przypadku stosowania WPA i WEP jest możliwe zgadnięcie hasła, gdyż wykorzystywane przez podsłuchiwaczy automatyczne słowniki mogą zgadywać tysiące haseł na sekundę. Dlatego też dla internetu bezprzewodowego zalecany jest tryb HotSpotVPN (wtedy jeśli bezprzewodowa sieć nie szyfruje danych, to tym zajmie się osobisty komputer osoby korzystającej z publicznego punktu dostępowego) .

Klient powinien wiedzieć jak posługiwać się podpisem elektronicznym. Użytkownik ma klucze dwóch rodzajów: prywatny oraz publiczny. Klucz publiczny daje się tym, którzy będą mieli prawo odczytu twoich informacji, podpisanych kluczem prywatnym. Klucz prywatny pozostaje jedynie w twojej dyspozycji i nie należy go udostępniać osobom postronnym. Dla serwera SSH (Secure Shell) to jest identyfikator użytkownika- porównać go można do klucza otwierającego prywatne mieszkanie. Trzymać go można na dyskietce lub pendrivie (a nie na na dysku, do którego mają dostęp inne osoby). może dać okazję do jego nieautoryzowanego wykorzystania . Klucz publiczny możemy udostępnić na swojej prywatnej stronie internetowej, serwerze (nie fałszywym) zajmującym się udostępnianiem kluczy lub wysłać znajomej osobie. Przy korzystaniu z usług szyfrowanych zabezpieczanych kluczami należy zwracać uwagę na termin ważności certyfikatu.

Wątpliwości co do zachowania klientów można mieć więcej. Przykładowo, płacąc kartą należy mieć kontrolę nad tym co się z nią dzieje (np. gdy jest zabierana z sali restauracyjnej od klienta). W zasadzie trzeba wprost powiedzieć, że w obecnym stanie stosowanych zabezpieczeń (np. karty magnetyczne zamiast chipowych, brak biometrycznych metod rozpoznawania klienta) klient musi mieć trochę szczęścia, by nie paść ofiarą oszustwa, nawet wtedy gdy bardzo się stara być ostrożnym.

Wiedza o zagrożeniach może pomóc użytkownikom korzystającym z internetowego dostępu do systemów bankowych

Sądzimy, że użytkownicy internetu powinni być świadomi następujących zagrożeń jakie mogą napotkać:

- „cracking" (zgadywanie/łamanie/rozszyfrowywanie haseł dostępowych, algorytmów szyfrujących, kluczy publicznych i prywatnych itp.),
- „sniffing" (podglądanie, podsłuchiwanie - z użyciem urządzenia lub programu) np. za pomocą programu typu "packet sniffer", umożliwiającego wgląd do treści pakietu danych, a więc również id uzytkownika i hasła (szczególnie jest to proste gdy nie są szyfrowane); sniffing jest nie wykrywany przez firewall gdyż nie wytwarza ruchu w sieci i może być uzywany szczególnie łatwo przez użytkowników wewnątrz sieci (czyli pracowników banku).
- „snooping" (pasywne wejście do sieci: podpięcie do kabla i oczekiwanie na dane przekazywane np. analizatorom sieci),
- „spoofing" (badanie sieci np. poprzez aktywne podpięcie do kabla tj. wpuszczanie do sieci danych i poleceń - np. symulowanego protokołu komunikacyjnego, podszywanie się pod kogoś - poprzez fałszywy adres nadawczy IP - i uzyskanie dzięki temu nielegalnego dostępu do danych); spoofing jest wykorzystywany szczególnie do ataku typu „DoS"
- automatyczne skanowanie portów (metoda ta została użyta w przypadku wirusów Nimda i Code Red, co pozwoliło szybko je rozpowszechnić)
- "back door" ("tylne drzwi") - wejście do komputera w inny sposób niż poprzez logowanie użytkownika do systemu, a np. poprzez pocztę elektroniczną lub dzięki zainstalowaniu odpowiedniego oprogramowania, np. keyloggerów , w celu rejestrowania wprowadzanych na klawiaturze znaków (co pozwala uzyskać hasło jeszcze przed jego zaszyfrowaniem), zapisania odwiedzanych stron internetowych a nawet rozmów prowadzonych za pomocą komunikatora.
- wprowadzenie wirusów i trojanów ("koni trojańskich"), tj. programów udających "pożyteczne lub niewinne rzeczy" a tak naprawdę przeznaczonych do uruchomienia działań destrukcyjnych (niszczenie danych na komputerze, na którym się znajdują) i „szpiegowskich" (kopiowanie plików na inne komputery w sieci). Trojany i wirusy zaszywane są w załącznikach poczty elektronicznej, w plikach bat, autorun.inf, com, exe, pseudotekstowych (.hta) zawierających wykonywalne skrypty, obiektowych (.shs) , plikach rozpoznawanych na pierwszy rzut oka jako "screen savery", w grach, makrach VBA w plikach DOC, XLS, PPT i MDB itp.
- "moles" (krety) - wiadomości pocztowe, których celem jest uzyskanie danych adresata, np. adresu IP przekazywanego zwrotnie do serwera nadawcy przy ściąganiu obrazka
- „session hijacking" (przechwycenie sesji legalnego użytkownika)
- DoS ("denial of service attack" lub "zombie attack") - blokowanie użytkownikom usług internetowych poprzez stwarzanie sztucznego tłoku w sieci i przeciążanie ("zatapianie" -flooding) serwera komunikami typu "adresy zwrotne' (return address spoofing), sprawdzaniem połączenia komendą "ping" (ping of death), replikującymi się wirusami, dużymi pakietami danych podlegającymi ciągłej fragmentacji od początku (tear drop attack), uruchamianie na serwerze zapętlających się programów (wykonywanych bez końca), wysyłanie tak znacznej liczby symulowanych żądań połączeń (SYN attack) że pozostają one bez odpowiedzi uniemożliwiając obsługę "prawowitych" żądań, itp. Rozproszony DoS (distributed DDoS) jest inicjowany przez wiele komputerów, skoncentrowanych na „bombardowaniu" np. serwera bankowego, przy czym nie musi być to ich własny zamierzony atak lecz wymuszony z zewnątrz na skutek wykorzystaniu luki bezpieczeństwa w systemie operacyjnym, serwerze internetowym lub serwerze bazy danych.

- przepełnianie wejściowego buforu serwera (BO-buffer overflow), w celu uzyskania uprawnień do instalacji własnych programów przeznaczonych np. do analizy zrzutów pamięci znajdujących się na dysku w celu odnalezienia haseł dostępowych
- analiza informacji identyfikujących użytkownika znajdujących się na komputerze klienta w postaci "ciasteczek" (tzw.cookies - jeśli nie są one przechowywane w postac zaszyfrowanej) i następnie modyfikacja ("zatruwanie") tych cookies w celu osiągnięcia dostępu do aplikacji klienta w jego imieniu
- podgląd kodu źródłowego strony internetowej i zmiana wartości w polach ukrytych (nie pojawiających się na ekranie)
- zmiana parametrów łącza CGI (czasem aplikacje nie kontrolują tych parametrów)
- wykorzystanie informacji zapisywanych na komputerze podczas testowania (debugging), o kasowaniu których zapomnieli programiści po ukończeniu testowania
- wykorzystanie luk systemowego oprogramowania w celu uzyskania hasła administratora i przejęcia kontroli
- wykorzystywanie luk w systemach operacyjnych, przeglądarkach internetowych i w oprogramowaniu antywirusowym
- phishing jest rodzajem oszustwa internetowego, polegającego na wyłudzeniu od klientów (po podszyciu się pod instytucję finansową – poprzez fikcyjną witrynę lub email) danych uwierzytelniających. Na przykład internauta otrzymuje e-mail pochodzący rzekomo od banku, w którym prosi się go o podanie hasła, numeru karty kredytowej i „koniecznie o zweryfikowanie danych osobowych". W emailu może być też link do „nowej" lub „eksperymentalnej" strony banku (oczywiście fałszywej), do której klient może się próbnie „zalogować", używając swoich zwykłych danych uwierzytelniających.
- zainstalowanie na komputerze trojana lub wirusa, który automatycznie (bez potrzeby otwierania załącznika do emaila) - dzięki podmianie kontrolowanej listy witryn - przy wpisaniu prawidłowego adresu internetowego przekierowywuje na fałszywą stronę banku.

Poza powyższymi zagrożeniami występują też inne o mniejszej szkodliwości, np. rozpoznawanie sieci (network reconnaissance) poprzez uchwycenie dopuszczalnych adresów IP, nazw domen (DNS) i portów IP. Nawet tzw. pingowanie (pinging) adresu serwera może być wykorzystane przez hakera do poważnego ataku. Próby skanowania sieci z zewnatrz zwykle są wykrywalne jako tzw. intruzje (włamania) przez firewalle lub routery brzegowe (routery są to urządzenia sterujące ruchem pakietów w sieci).

W wyniku wyżej opisanych działań mamy więc w praktyce do czynienia z takimi produktami jak „sniffery" (analizatory sieci i „szperacze", czyli programy szpiegowskie ukryte w sieci, których celem jest przechwytywanie haseł („password sniffer") i kodów komunikacyjnych, zwykle stanowiących początkową sekwencję bajtów sesji) oraz „IP spoofing"/"packet forge spoofing" (fałszowanie danych w pakietach komunikacyjnych, w szczególności „podrabianie" adresów tak aby były rozpoznawane jako „wewnątrzsieciowe" a nie pochodzące od kogoś kto usiłuje dopiero dostać się do sieci).

Przykładem trojana bankowego jest Bankhook.A, który instaluje się w komputerze wykorzystując lukę MhtRedir w Internet Explorerze. Wirus ten śledzi ruch internetowy na szyfrowanych protokołach (https) dotyczących witryn bankowych. Jeśli natrafi na nie, wówczas zbiera informacje typu: nazwa użytkownika, hasło, nr konta bankowego, numer karty kredytowej itp., poczym za pomocą skryptu odsyła je do określonego zdalnego komputera. Odmiana NL trojana Bancos Trojan kontroluje dostęp do ponad 2500 portali bankowych z ponad 120 krajów (w tym niemieckich i szwajcarskich).

Phishing jest metodą popularną zarówno w Polsce jak i zagranicą. Najnowsze doniesienia z września br. informują o ataku BarcPhish określonego jako „spoofmail" skierowanego do klientów on-line banku Barclays. W ataku tym wystepuje az 70 różnego typu komunikatów mailowych: np. „oficjalny" update systemu, „security update" , weryfikacja danych osobowych. Postać komunikatow niczym nie różni się od prawdziwej poczty bankowej.. Naciśnięcie na link w komunikacie wprowadza na imitację strony banku, na którą klient wprowadza takie dane jak nr konta, nr karty płatniczej-kredytowej, PIN .

Dla lepszego zrozumienia niektórych technicznych szczegółów tej publikacji warto zdefiniować takie pojęcia jak „wirus, robak, trojan", które aczkolwiek zbliżone do siebie, posiadają różne mechanizmy działania.

Wirus jest to program (zwykle szkodliwy), który ma zdolność reprodukowania siebie poprzez infekcję plików danych i programów. Istnieją też pseudowirusy (hoax) reprodukujące fałszywe informacje typu „masz zainfekowany komputer" (łącznie z opisem nieistniejącego wirusa), „komunikat FBI..." itp. i równie skutecznie obciążające sieć i serwery. Czasem prawdziwy wirus startuje jako hoax i dopiero następnie uruchamia swoje działanie.

Robak jest bardzo podobny do wirusa, z tym, że rozmnaża się samodzielnie bez zagnieżdżania w plikach, ale też może je uszkadzać. Ponadto może być zdolny do szybkiej reprodukcji i zatykania sieci gdyż rozsyła się zwykle poprzez emaile i IRC (Internet Relay Chat – konwersacje internetowe). Przykładowe robaki to: I Love You, Navidad, Pretty Park, Happy99 i ExploreZip. Aby nie być gołosłownym, robak „I love You" uszkadza pliki VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, JPG, JPEG, MP3 i MP2 oraz kradnie poufne informacje odsyłając je do autora robaka.

Trojany ani nie rozmnażają się poprzez zarażanie plikow (jak wirusy), ani nie reprodukują siebie (jak robaki). Pozornie wyglądają na nieszkodliwe przypadkowo ściągnięte programy o nazwach zachęcających do uruchomienia (np. Donald Dick, Extacis) lecz jeśli je uaktywnimy instalują szkodliwe programy, które mogą usuwać pliki z dysku (np.te dbające o bezpieczeństwo) i umożliwić penetrację komputera przez zewnętrznych użytkowników w celu ściągnięcia poufnych informacji (otwierając sobie porty potrzebne do ich wysłania na zewnętrzne adresy).

Po omówieniu powyzszych terminów poświęcimy parę zdań profesjonalistom. W terminologii ogólnej „haker" jest raczej zaawansowanym programistą zdolnym do wyłapania słabych punktów zabezpieczenia (a nie włamywaczem), nie mniej jednak „hacking" oznacza zwykle uzyskanie nieuprawnionego dostępu do systemu komputerowego. W środowisku kart płatniczych pojawił się - poza używanym często określeniem "crook(er)" - termin „carder" do oznaczenia osoby, która w nieuczciwy sposób zdobywa numery i piny kart.

Oprogramowanie i proceder, dzięki któremu nielegalnie osiąga się korzyści finansowe (kosztem klientów lub stron trzecich) zostało ochrzczone nazwą „crimeware".

Co dalej

Narastająca liczba bankowych oszustw finansowych w trybie „online" musi doprowadzić do zwiększenia nakładów na technologie zapewniające bezpieczeństwo. Chodzi między innymi o lepsze metody identyfikacji klientów i odejście od stosowania haseł. Dane z USA mówią, iż jeden na pięciu klientów pada ofiarą złodziejstwa identyfikacyjnego (identity theft) a w skali roku liczba takich osób sięga 10 milionów. Wypowiadane są poglądy, że w najblizszej przyszłości większość banków amerykańskich i o zasięgu międzynarodowym odejdzie od zabezpieczania za pomocą haseł.dostępu online do kont klientów. Co więc w zamian?

Wysoką pewność identyfikacji posiadają biometryczne metody rozpoznawania klientów (kształt dłoni, linie papilarne palców, tęczówka oka, pomiar nacisku na podpis itp.). Szersze stosowanie tych metod to sprawa akceptowania wyższych kosztów oraz jakby zmniejszenia „prywatności" klientów lub też naruszenia prawa ochrony danych osobowych (pojawia się kwestia poufności nie tylko informacji biznesowych czy transakcyjnych lecz również osobistych).

Kształt dłoni – odczytywany przez ekran, na którym klient kładzie rękę - wyrażany jest przede wszystkim przez jej szerokość, długość palców i niektóre punkty. Już ponad 350 banków stosuje ten system rozpoznawania przy obsłudze skrzynek seifowych.

Metoda rozpoznawania odcisków palców wydaje się być pewna, jednakże zawodzi czasem w przypadku spracowanych dłoni, a szczególnie dotyczy to robotników budowlanych. Metoda ta jest ulepszana i procent błędów maleje (ok. aktualnie 8 procent odcisków nie może być odczytanych, a kiedyś było to 30%).

Do niedawna urządzenia do rozpoznawania tęczówki oka były bardzo drogie, a obecnie cena niektórych z nich spadła prawie do 1000 dolarów.

Jedną z metod biometrycznego rozpoznawania użytkowników systemu, będących pracownikami banku, może być automatyczny odczyt odcisku linii papilarnych odciskanych na myszy komputerowej.

Straty finansowe z tytułu zewnętrznych i wewnętrznych "włamań" do systemów banków i instytucji finansowych stanowią pilnie strzeżoną tajemnicę, lecz mogą być znaczne i według szacunków dla niektórych banków wynoszą nawet parę procent kapitału własnego albo obrotu.

W celu przeciwdziałania zjawisku ponoszenia strat wskutek włamań, należy realizować co najmniej następujące czynności organizacyjne: staranna weryfikacja oprogramowania na odporność włamaniową i nieobliczalne zachowanie użytkownika (tzw.idiot-test) przed jego zainstalowaniem, regularna analiza śladów audytowych z ukierunkowaniem na operacje nietypowe dla danego klienta lub uzytkownika, opracowywanie klas użytkowników również pod katem widzenia potencjalnych nadużyć, wprowadzenie dla programistów bankowych ograniczeń kontaktu z rzeczywistymi bazami danych (tzn. z wersją produkcyjną) systemu bankowego oraz określona polityka kadrowa wykluczająca pracowników popełniających oszustwa lub podatnych na nie.

Podsumowanie

Zabezpieczyć doskonale systemów bankowych zapewne się nie da, ale należy dokładać wszelkich starań by były jak najlepsze. Najsłabszymi ogniwami bezpieczeństwa obecnie wydają się być: uwierzytelnianie klientów i oszustwa dokonywane przez personel banków.

Nie wszystko sprowadza się do kosztu nowych urządzeń i lepszego oprogramowania. Zawodzi tez sprawność organizacyjna. Na przykład w Polsce jeszcze nie uruchomiliśmy na szeroką skalę wszystkich dostepnych środków, chociażby mechanizmu podpisu elektronicznego. Mimo, iż uchwalona 27 lipca 2001 roku przez Sejm ustawa o podpisie elektronicznym stworzyła nowe możliwości wzmocnienia bezpieczeństwa, dalej trwają prace nad standardem zasad bezpiecznej wymiany danych pomiędzy bankami i ich klientami we wspólnej sieci bankowości elektronicznej w oparciu o infrastrukturę klucza publicznego. Standaryzacja ma na celu zachęcenie do stosowania e-podpisu w Polsce, bo do tej pory klienci byli zniechęceni mnogością niekompatybilnych jego formatów. Polskie centra certyfikacji powołały nieformalny zespół roboczy, którego zadaniem będzie zaadaptowanie międzynarodowej normy XAdES do potrzeb polskich standardów podpisu elektronicznego. Szyfrowanie danych i technologia podpisów elektronicznych są podstawowymi metodami zabezpieczania transakcji elektronicznych. W zabezpieczaniu dostępu zapewne najskuteczne i najszybsze (ale chyba i najdroższe) będą biometryczne metody rozpoznawiania klientów.

Skutecznym środkiem przeciwko oszustwom popełnianych przez pracowników banku jest metoda śladów audytowych (system notuje “ślady pobytu w aplikacji” w kilku miejscach: w oddziałowym transakcyjnym pliku audytowym, centralnym pliku audytowym, historii rachunków, historii zmian w kartotece klientów, historii zmian definicji produktów, w dziennikach -journals - systemu zarządzania bazą danych służących m.i. do zapewniania integralności transakcji poprzez tzw. rollback oraz w dziennikach logowania tworzonych przez system operacyjny komputera i system operacyjny sieci komputerowej. Zatarcie wszystkich śladów w przypadku nadużyć jest wtedy praktycznie niemożliwe, a dodatkową

zaletą tej nadmiarowości jest to. że istnieje kilka żródeł odzyskiwania danych. Jedyny problem zapewne w tym, że te ślady musza być starannie analizowane przez wewnętrznych audytorów, gdyż inaczej sa „sztuką dla sztuki".

Dodatkowym środkiem kontrolnym, przeciwdziałającym nadużyciom jest rozsyłanie listów do klientów, posiadających wysokie salda na rachunkach, z prośbą o niezależne potwierdzenie sald. Przydatny może być również „inteligentny" program komputerowy sygnalizujący „gwałtowne" ruchy na kontach lub inne nietypowe dla danego klienta zachowanie.

Bezpieczeństwo systemu bankowego jest równie ważne jak prawidłowe naliczanie odsetek depozytowych czy kredytowych. Wymaga znacznych nakładów, lecz jest warunkiem zaufania ze strony klienta, a w ostatecznym rozrachunku zabezpiecza zarówno klienta jak i bank.