Janusz Zawiła-Niedźwiecki

Kompleksowa koncepcja bezpieczeństwa systemu informatycznego Giełdy Papierów Wartościowych (II)

Zabezpieczenia programowe

Oprogramowanie systemu Giełda zostało opracowane przez francuski oddział (GFI – Groupe Française d'Informatique) jednej z największych firm programistycznych na świecie – EDS. System ten jest adaptacją oprogramowania funkcjonującego przez kilka lat na giełdzie w Lyonie. W części tłumaczy to zastosowaną metodykę zabezpieczania dostępu. W toku eksploatacji od 1992 roku oprogramowanie to zostało gruntownie przebudowane i rozbudowane. Pojawiły się nowe cechy funkcjonalne systemu. Zachowana została jednak podstawowa struktura i mechanizmy zabezpieczeń.

Oprogramowanie systemu informatycznego Giełdy składa się z ponad 1200 obiektów programowych oraz ponad 800 plików baz danych. Zorganizowane jest w trzy podstawowe systemy notujące:

- rynek jednolitego kursu, zbudowany z modułów: obsługi parametrów notowania, obsługi karnetu zleceń, realizacji dodatkowego obrotu na sesji (tzw. dogrywka), operacji maklera specjalisty,
- rynek ciągły,
- rynek pakietowy oraz w szereg modułów wspólnych i systemów „okołogiełdowych": obsługi indeksów giełdowych, rozliczania sesji, fakturowania obrotu giełdowego, bazy słownikowej notowań, archiwum notowań, dystrybucji informacji giełdowych.

Wszystkie funkcje systemu informatycznego giełdy uruchamiane są przez wywołanie danej opcji. Opcja systemu jest budowana na zasadzie „menu". Konstrukcją opcji zajmuje się administrator aplikacji. W niewielkim uproszczeniu można przyjąć, że cały system informatyczny giełdy reprezentowany jest przez ciąg zdefiniowanych opcji (menu). Istnieje też specjalne oprogramowanie służące do przedzielania opcji uczestnikom (przez uczestnika rozumiemy instytucję korzystającą z obsługi przez system informatyczny Giełdy: biuro maklerskie, samą giełdę, KPWiG, KDPW) i użytkownikom (pracownik danej instytucji posiadający swój indywidualny kod dostępu do systemu informatycznego – profil dostępu, realizujący określone dla niego funkcje). W przypadku biura maklerskiego można wyróżnić następujące klasy użytkowników: makler specjalista, makler oraz obserwator – posiadający wyłącznie pasywne funkcje systemu służące do obserwacji rynku. Hierarchiczna zależność tych klas jest taka, że makler specjalista (osoba fizyczna) może posiadać trzy ww. kody dostępu do systemu, a więc jest postrzegany jako trzej użytkownicy z różnymi uprawnieniami. Przydzielanie opcji polega na:

- przydzieleniu tych funkcji (opcji) systemu danej instytucji (uczestnikowi), które są przez nią realizowane (np. biuro maklerskie, nie pełniące funkcji specjalisty dla danego papieru wartościowego, nie otrzyma opcji pozwalających na ich realizację),
- przydzieleniu danemu użytkownikowi (fizycznemu pracownikowi danej instytucji) spośród opcji przyznanych uczestnikowi (instytucji) tych opcji, które określone są w ramach danej klasy użytkownika.

Wszystkie wersje wynikowe programów tworzone są na zasadzie tzw. adopcji uprawnień. Każdy wywołany program, bez względu na uprawnienia użytkownika, przyjmuje (adoptuje) wszystkie uprawnienia właściciela programu. Zastosowano przy tym zasadę odebrania wszystkich publicznych uprawnień do zbiorów danych, natomiast publicznego udostępniania oprogramowania. Jednak wobec restrykcyjnego limitowania dostępu do funkcji wydawania komend dla systemu operacyjnego komputera oznacza to analogiczne limitowanie bezpośredniego dostępu do oprogramowania. Jedyną możliwością jego wykorzystania jest wywoływanie funkcji (opcji) poprzez menu danego użytkownika i jedynie w zakresie wynikającym z definicji środowiska pracy tego użytkownika.

Zastosowana przez EDS-GFI metoda zabezpieczania danych polega na ustaleniu uprawnień użytkownika do danych poprzez budowanie ciągu menu umożliwiających dostęp do pewnych klas użytkowników oraz przydzielaniu użytkownikowi prawa

uczestnictwa w jednej lub kilku ściśle określonych klasach operacji (funkcjach systemu informatycznego giełdy). Nie skorzystano tu z możliwości oferowanych przez system operacyjny OS/400 ustalenia bezpośrednich relacji pomiędzy użytkownikami i zbiorami danych. Głównym powodem był fakt, że szereg plików zawiera dane bardzo wielu uczestników. Domy maklerskie powinny mieć dostęp do danych własnych, ale oczywiście nie możliwości dostępu do danych innych domów maklerskich. Ograniczając się do metody bezpośredniej ochrony plików danych, należałoby utworzyć pliki logiczne dla każdego domu maklerskiego oddzielnie, co jednak osłabia bariery stawiane osobom nieuprawnionym, a liczba plików logicznych powiązanych z podstawowymi plikami byłaby równa iloczynowi obecnej liczby plików logicznych i liczby domów maklerskich, a to spowodowałoby spadek wydajności całego systemu.

Główną zaletą ochrony danych poprzez adopcję jest fakt, że użytkownicy nie mają bezpośrednich uprawnień do plików danych. Zatem żadną inną metodą niż poprzez dostarczone oprogramowanie użytkowe nie mogą się dostać do tychże plików. Taka metoda ochrony nie jest jednak pozbawiona wad. Podstawowe z nich to: utrudniony audyt informatyczny, potrzeba rygorystycznej organizacji procesu tworzenia oprogramowania oraz wymóg skutecznej ochrony programów i danych użytych w ochronie systemowej. Wobec dwu pierwszych wad stosuje się rozwiązania organizacyjne, np. wprowadzaniem programów do produkcji zajmuje się tylko bardzo ograniczone grono upoważnionych osób, a przed wprowadzeniem ma miejsce kilkustopniowa ocena programów. Wada ostatnia została rozwiązana przez ograniczenie prawa użytkowników do wydawania systemowi operacyjnemu komend. System informatyczny giełdy chroni także ustawienie listy dozwolonych bibliotek oraz przypisanie funkcji w specjalnych plikach w bibliotece systemowej, indywidualnych dla każdego z użytkowników. Tak więc np. wywołanie przez osobę upoważnioną, do funkcji innych niż maklerskie, programów obsługujących maklerów zakończy się komunikatem o niewłaściwej liście bibliotek lub braku dostępnych funkcji.

W programach umożliwiających dostęp do zbiorów danych zawierających informacje zastrzeżone wyłącznie dla danego uczestnika przeprowadza się weryfikację przez specjalny program sprawdzający, na podstawie danych zawartych w profilu użytkownika, do jakiego uczestnika (instytucji) on należy oraz udostępnia się wyłącznie te dane, których właścicielem jest zidentyfikowany uczestnik. Pozwala to w sposób programowy na jednoznaczną ochronę tych informacji, które są dedykowane wyłącznie danemu uczestnikowi, a więc zwłaszcza na ograniczenie dostępu użytkownika tylko do zleceń danego biura maklerskiego, a obsługę przez maklera specjalistę tylko tych papierów wartościowych, których specjalistą jest dane biuro.

Użytkownicy, którzy nie mają prawa do wydawania systemowi komend, nie mają także prawa do wydawania zdalnych komend, co w ramach systemu operacyjnego jest osobną klasą możliwych uprawnień. Uzyskiwane jest to poprzez specjalny program zdefiniowany jako jeden z atrybutów sieciowych. Podobną techniką system chroniony jest przed niewłaściwymi transferami czy dostępem do folderów i plików. Ponieważ jednak maklerzy potrzebują używać systemowej funkcji transferu plików do przekazu paczek zleceń i pobierania wyników notowań, transfer jest chroniony kilku metodami jednocześnie. Podstawowe z nich to: transfer plików wywoływany jest jak inne opcje poprzez menu systemu informatycznego giełdy, zakończenie sesji współpracy terminalowej kończy się usunięciem pakietu konwersji AS/400 – PC i zerwaniem połączenia, transfer odbywa się do pośrednich plików, indywidualnych dla każdego domu maklerskiego, umieszczonych w specjalnie do tego przeznaczonej bibliotece transferowej, dalsze przesłanie do plików docelowych odbywa się za pośrednictwem adopcji uprawnień, przesyłana paczka zleceń musi zawierać identyfikację domu maklerskiego w każdym rekordzie, a poufny kod domu maklerskiego w rekordzie początkowym. Podstawowa ochrona polega na tym, że specjalny program, zdefiniowany jako jeden z atrybutów sieciowych, dopuszcza tylko transfery do i z biblioteki transferowej, a wszystkie pliki mające kontakt z pakietem konwersji AS/400 – PC są chronione prawami dostępu poszczególnych domów maklerskich. W przypadku dostępu do zintegrowanego systemu plików i folderów, dopuszcza się jedynie dostęp typu „odczyt" do plików potrzebnych do aktualizacji pakietu konwersji.

Tylko upoważnieni, a nieliczni administratorzy systemu AS/400 mają specjalne uprawnienia pozwalające im na dostęp poza aplikacją. Ponadto każdorazowy planowany dostęp z tych profili do plików produkcyjnych musi być zawczasu dopuszczany na mocy decyzji przełożonych, a w momencie wykonywania jest automatycznie odnotowywany w dzienniku zdarzeń systemowych *(audit journal)*, który jest systematycznie audytowany zewnętrznie. Ograniczony dostęp do danych mają także operatorzy, ale dotyczy on tylko zadań składowania tych danych na taśmach magnetycznych. W toku tych prac operatorzy „nie widzą" danych produkcyjnych.

Zabezpieczenia przekazu danych

Opracowując zabezpieczenia przekazu danych uwzględniono następujące typy zagrożeń dla systemu informatycznego giełdy:

- Zagrożenia losowe zewnętrzne (np. zakłócenia w zasilaniu, wyładowania atmosferyczne, klęski żywiołowe). Ich wystąpienie może prowadzić do utraty integralności danych, zniszczenia danych, a w ekstremalnej sytuacji – do zniszczenia infrastruktury technicznej przekazu oraz utraty danych. Ciągłość pracy systemu zostanie zakłócona, choć z zasady nie dojdzie do naruszenia poufności informacji.

■ Zagrożenia losowe wewnętrzne (np. niezamierzone błędy i pomyłki operatorów, administratorów bądź użytkowników systemu, awarie sprzętu lub oprogramowania). Ich wystąpienie również może prowadzić do utraty integralności danych, zniszczenia danych, zakłócenia ciągłości przekazu oraz naruszenia poufności informacji.

■ Zagrożenia zamierzone, czyli świadome i celowe. Działania atakujące system podejmowane są najczęściej z niskich pobudek (chęć zysku, rewanżu, wandalizm), ale także z pobudek przestępczych (szpiegostwo gospodarcze lub terroryzm) lub swoiście pojmowanej zabawy. Jest to najpoważniejszy rodzaj zagrożeń, gdyż jest nastawiony na naruszenie poufności informacji. Sprawca najczęściej unika uszkadzania infrastruktury technicznej oraz zakłócania ciągłości przekazu. Dąży on bowiem do ukrycia faktu dokonania ingerencji w system informatyczny.

Zagrożenia pochodzące z zewnątrz są często nazywane włamaniami. Włamanie jest efektem działania intruza – *hackera*. Analizuje on słabe punkty systemu w celu zdobycia quasi-uprawnionego dostępu i dokonuje ataku, wykorzystując najczęściej istniejące połączenia zewnętrzne. Przykładowo mogą to być nie chronione przyłącza do sieci Internet, urządzenia komunikacyjne z możliwością automatycznego przyjmowania połączeń z sieci rozległych lub połączenia z sieciami LAN innych instytucji. Tego rodzaju działania są w Polsce karalne jedynie wówczas, gdy czyn jest umyślny i gdy *hacker* zostanie przyłapany na gorącym uczynku. Z tego powodu *hacker* pragnie pozostać anonimowy, co dodatkowo może zwiększyć zakres jego ingerencji, gdyż dąży on do usunięcia śladów swojej działalności, np. przez uszkodzenie kronik systemowych czy też oryginalnych wersji modyfikowanych zbiorów. Często spotykany jest szczególny sposób ataku *hackera* polegający na podszywaniu się pod istniejącego użytkownika. W takim przypadku zawodzą zwykłe techniczne metody ochrony.

Ingerencja poprzez publiczną i prywatną (wewnętrzną) sieć telefonii ma charakter głównie podsłuchu. Każdy pracownik giełdy uświadamiany więc jest, jakiego rodzaju informacji nie może przekazywać ani przez sieć naziemną, ani komórkową. Szczególną uwagę zwraca się przede wszystkim na możliwość przekazania tą właśnie drogą tajnego hasła autoryzującego korzystanie z profilu użytkownika. Istnieje przecież technika *hackerska* zdobywania informacji poprzez zabiegi socjotechniczne.

Operacja podsłuchu i przechwytywania jest zawsze bardzo kosztowna dla intruza, bo wiąże się z wniesieniem oraz zainstalowaniem unikalnego i wyrafinowanego sprzętu. Z tego powodu przedsięwzięto takie środki utrudniające podsłuch, aby dodatkowo zwiększyć jego koszty. Podsłuch jest działaniem prowadzącym do uzyskania dostępu do przekazywanej informacji bez wiedzy i zgody wszystkich biorących w tym procesie stron. Należy podkreślić, że podsłuch jest najbardziej typowym działaniem, którego można się spodziewać w warunkach eksploatacji publicznych łączy do transmitowania danych. Niebezpieczeństwo podsłuchu polega na tym, że intruz może dowolnie spożytkować uzyskane dane – np. do ich publicznego ujawnienia, wykorzystania w celu uzyskania własnej korzyści materialnej lub uszczuplenia cudzej, albo też w celu przygotowania pola do właściwej ingerencji w system poprzez, na przykład, uzyskanie dostępu do tajnych haseł. Biorąc to pod uwagę w przekazie między ośrodkami podstawowym i zapasowym giełdy oraz w przekazie między giełdą a KDPW, stosowana jest technika kryptograficzna. Urządzenia szyfrujące posiadają certyfikację Urzędu Ochrony Państwa.

Ważnym elementem polityki bezpieczeństwa giełdy staje się problematyka synchronizacji czasu w sieci giełdowej, zwłaszcza w aspekcie rozwoju sieci rozległej i perspektywie pojawienia się zagranicznych, odległych członków giełdy. Wystarczy tylko przeanalizować sytuację, w której maklerzy składają zlecenia zdalnie ze swoich biur maklerskich. Są one wprowadzane na komputerach wyposażonych we własny, wewnętrzny zegar, występują więc różnice w stosunku do czasu komputerów giełdowych, a może też zaistnieć problem interpretacji tej różnicy. Istnieją na szczęście narzędzia do synchronizacji czasu dostępne pod praktycznie każdym systemem operacyjnym. W warunkach giełdy korzystającej z sieci, w których stosowane są różne systemy operacyjne (OS/400, Novell Netware, Windows NT, UNIX) oraz różne protokoły transmisyjne (SNA, IPX/SPX, TCP/IP), takie narzędzie jest bardzo skomplikowane. Musi być ono zainstalowane na każdym komputerze, na którym czas jest istotnym parametrem. Musi być ustalony komputer, którego czas (choćby był niezgodny z czasem rzeczywistym) jest obowiązującym wzorcem dla wszystkich. Musi być ustalony protokoł transmisyjny, za pomocą którego następuje propagacja czasu w całej sieci. Muszą być opracowane procedury bezpieczeństwa wykluczające ryzyko związane z fałszywą zmianą czasu. Alternatywnym, rozważanym rozwiązaniem jest przyjęcie zewnętrznego źródła czasu wzorcowego, np. publicznego wzorca czasu krajowego emitowanego drogą radiową i opracowanie metody synchronizacji systemu giełdowego z takim wzorcem. Wskazanie użytkownikom takiego wzorca zdjęłoby z giełdy odpowiedzialność za poprawność i skuteczność dystrybucji czasu wzorcowego w sieci systemu informatycznego giełdy. Nadajnik takiego wzorca czasu ma być niebawem uruchomiony w Polsce.

Na potrzeby ochrony przed ulokowaniem się wirusów komputerowych stosuje się dwa rodzaje rozwiązania antywirusowego: do zwalczania wirusów na poszczególnych stacjach roboczych oraz do zwalczania wirusów atakujących samo środowisko sieciowe. Ponadto przygotowano specjalne stanowisko do testowania nośników danych wnoszonych z ze-

wnątrz i objęto wszystkich pracowników giełdy obowiązkiem poddawania testom antywirusowym każdego takiego nośnika.

Mając na uwadze ochronę przekazu danych, strukturę sieciową systemu informatycznego giełdy można analizować w następującym układzie:

- transmisja danych po lokalnej sieci Twinax,
- transmisja danych po lokalnych sieciach LAN Ethernet i Token Ring,
- transmisja danych między ośrodkami giełdowymi: podstawowym i zapasowym po łączach dzierżawionych,
- transmisja danych do redystrybutorów informacji giełdowych po łączach dzierżawionych przez nich,
- transmisja danych do Telewizji Polskiej po łączach dzierżawionych – serwis jawny (ogólnodostępna telegazeta) i kodowany (dla abonentów),
- transmisja danych do tablic wyświetleniowych po sieci LAN i wewnętrznych liniach specjalnych,
- transmisja danych poprzez sieć Frame-Relay między terminalami zdalnymi domów maklerskich a ośrodkami giełdowymi.

Większa część przekazu dokonywana jest w protokole SNA, właściwym dla systemów opartych na komputerach IBM. W łączności zdalnej protokoł SNA jest umieszczany w pakietach protokołu TCP/IP. Ochrona przekazu SNA polega przede wszystkim na zabezpieczeniu przed podszyciem się pod stację roboczą. Potencjalny intruz może bowiem liczyć na wadliwe zabezpieczenia w oprogramowaniu systemowym, uzależniającym przywileje między innymi od konkretnego adresu sprzętowego interfejsów w terminalach maklerskich.

Transmisja Twinax dotyczy lokalnych terminali systemu informatycznego giełdy. Odbywa się od kontrolera w komputerze AS/400 przez porty, zespoły gniazd i pętle twinaxowe do dołączonych do nich terminali. Do wszystkich terminali podłączonych do danej pętli twinaxowej dochodzi ten sam sygnał. Wybór, które informacje są właściwe dla danego terminala, odbywa się według adresu ustawianego za pomocą mikroprzełączników w urządzeniu lub w odpowiednim układzie jego pamięci. Generalnie uważa się, że połączenia Twinax są bardzo pewnym elementem sieci.

W skład sieci LAN na giełdzie wchodzą:

- sieć LAN GPW w ośrodku zapasowym (wyłącznie Token Ring), a w tej sieci między innymi router do komunikacji zdalnej,
- sieć LAN w ośrodku podstawowym (Ethernet i Token Ring), a w tej sieci między innymi routery do obsługi segmentów LAN samej giełdy, segmentów LAN ekspozytur domów maklerskich w siedzibie giełdy i router do komunikacji zdalnej,
- serwery LAN giełdy oraz wyniesiony serwer LAN KPWiG.

Wszystkie połączenia między węzłami komunikacji komputerowej LAN są prowadzone światłowodami. Wykorzystuje się opcję *security* na portach koncentratorów LAN. Oznacza to, że na danym porcie nie jest możliwe podsłuchiwanie ramek przekazywanych po sieci, które nie są przeznaczone do komputera przypisanego do tego portu. Ramki nie przeznaczone do zabezpieczonego portu są przekazywane do niego z losowo wyznaczoną zawartością części informacyjnej ramki. Wszystkie wykorzystywane urządzenia aktywne sieci LAN (koncentratory, routery) są administrowane z wykorzystaniem niejawnych kodów dostępu. Kodami dostępu, pozwalającymi na zmianę funkcjonalności urządzeń aktywnych, dysponują tylko upoważnieni administratorzy sieci. W routerach, które służą do obsługi maklerów, zastosowano mechanizmy ograniczające możliwość komunikacji z ekspozytur domów maklerskich w siedzibie giełdy do komputerów giełdowych. Możliwe jest podejmowanie komunikacji jedynie do komputerów wyznaczonych filtrami przekazu założonymi w routerach. Analogiczne ograniczenia odnoszą się do protokołów komunikacyjnych, które mogą posłużyć do obsługi domów maklerskich. Zastosowane ograniczenia pozwalają na podejmowanie komunikacji tylko z wyznaczonymi komputerami giełdy.

Potencjalny atak na środowisko sieci LAN może polegać na uzyskaniu dostępu do zasobów danego serwera lub na nie kontrolowanym przedostaniu się poprzez serwer skonfigurowany jako router. Stosowane mechanizmy ochrony przed dostaniem się do serwera polegają na utrzymaniu tajności haseł użytkowników i na regularnym systemowym wymuszaniu zmiany hasła przez użytkownika. W serwerze Novell, skonfigurowanym jako router, została uruchomiona opcja blokady przenoszenia pakietów IPX z jednej sieci do drugiej. Protokoł IPX, z racji swojej budowy, jest w chwili obecnej niemożliwy do obejścia poprzez sieć Internet. Zatem jedynym miejscem, w którym mogłoby nastąpić włamanie, jest komputer podłączony do LAN. Dlatego też uwaga administratorów sieci i odpowiednie narzędzia monitoringu są ukierunkowane na ten problem.

Zgodnie z ostatnimi tendencjami w technice zabezpieczeń informatycznych stosowane są do ochrony systemu informatycznego giełdy separatory logiczne tzw. *firewalle*, które dopuszczają ściśle zdefiniowany ruch między siecią wewnętrzną giełdy a sieciami zewnętrznymi. Zadaniem *firewalla* jest ochrona lokalnej sieci przed atakiem z zewnątrz. Ochrona ta dotyczy łączy wychodzących poza teren giełdy na nie kontrolowany przez nią obszar domów maklerskich, KDPW oraz sieć usług publicznych. *Firewalle* pracują z pakietami protokołu TCP/IP. Zadaniem *firewalla* jest przede wszystkim kontrolowanie transmisji TCP/IP w obu kierunkach (na zewnątrz i do wewnątrz). Filtruje on pakiety wychodzące i przychodzące wykorzystując wbudowane w niego reguły separacji.

Janusz Zawiła-Niedźwiecki

Autor jest pracownikiem Instytutu Organizacji Systemów Produkcyjnych Politechniki Warszawskiej (stopień doktora) i dyrektorem Działu Informacji Giełdy Papierów Wartościowych w Warszawie.