Janusz Zawiła-Niedźwiecki

Kompleksowa koncepcja bezpieczeństwa systemu informatycznego Giełdy Papierów Wartościowych (I)

Zabezpieczenia techniczno-organizacyjne

We współczesnej informatyce fizyczne zabezpieczenia infrastruktury technicznej są zdominowane przez zabezpieczenia oparte na narzędziach dostarczanych w ramach systemów operacyjnych komputerów oraz w elementach sterujących pozostałych urządzeń, a towarzyszą temu rozwiązania organizacyjne praktyki korzystania z tego sprzętu oraz kontroli i optymizacji tej praktyki. W odniesieniu do systemu informatycznego giełdy stosowane są wszystkie z tych rodzajów zabezpieczeń.

System operacyjny komputerów AS/400 Giełdy Papierów Wartościowych w Warszawie jest eksploatowany z poziomem dostępności 30, co implikuje: zastosowanie haseł i profili użytkowników, zastosowanie ochrony obiektowej, rejestrację w dzienniku systemowym wydarzeń typu „naruszenie autoryzacji". Nie stosuje się wyższego poziomu dostępności, gdyż wówczas tego typu wydarzenia, poza zapisem w dzienniku systemowym, powodowałyby natychmiastowe zakończenie zadania.

Zarządzanie bezpieczeństwem systemu odbywa się przez stosowne ustawianie: zmiennych zarządzających ogólnymi aspektami bezpieczeństwa systemu, zmiennych zarządzających zapisem kroniki zdarzeń, zmiennych ochrony dostępu do obiektów w systemie OS/400, zmiennych charakteryzujących hasła użytkowników.

W ochronie danych produkcyjnych i oprogramowania aplikacyjnego systemu informatycznego giełdy została zastosowana także ochrona dostępu do obiektów. Przyjęto zasadę odebrania wszystkich publicznych uprawnień do zbiorów danych oraz publicznego udostępnienia oprogramowania. Jednak wobec restrykcyjnego limitowania dostępu do linii komend, oznacza to analogiczne limitowanie możliwości bezpośredniego dostępu do tego oprogramowania. Jedyną możliwością jego wykorzystywania jest dostęp przez menu danego użytkownika i jedynie w zakresie wynikającym z definicji środowiska pracy danego użytkownika. Rozwiązanie to szerzej omówiono w części drugiej artykułu.

W celu umożliwienia kontroli dostępu i ochrony zasobów, dla wszystkich obiektów istniejących w systemie operacyjnym komputera AS/400 są określane prawa dostępu do tego obiektu (zasobu) dla ogółu użytkowników, dla grup użytkowników (wskazanie profilu grupowego) oraz dla użytkowników indywidualnych (wskazanie indywidualnego profilu użytkownika). Domyślnie, po utworzeniu obiektu, wszystkie prawa dostępu do danego obiektu posiada jego właściciel, czyli ten użytkownik, który utworzył dany obiekt. Prawa te mogą być mu odebrane, jak również dopuszczalna jest zmiana właściciela obiektu. W systemie operacyjnym komputera AS/400 prawa dostępu mogą dotyczyć bądź to samego obiektu, bądź to danych należących do danego obiektu. Przykładowo, w celu usunięcia zbioru fizycznego należy mieć prawo do „zarządzania istnieniem obiektu", a aby usunąć dane z tego zbioru, należy posiadać prawo do korzystania z danego obiektu oraz prawo do usuwania rekordów. Grupa praw dostępu tworzy uprawnienie.

W celu ułatwienia zarządzania prawami dostępu do obiektów, w systemie operacyjnym komputera AS/400 zostały predefiniowane uprawnienia zawierające określone zbiory praw dostępu. Są to klasy uprawnień:

- wszystkie prawa dostępu do danego obiektu,
- uprawnienia do dokonywania zmian w obiekcie,
- uprawnienia do korzystania z danego obiektu bez prawa dokonywania zmian,
- uprawnienie negatywne, całkowity zakaz korzystania z obiektu.

Dodatkowo, użytkownik posiada prawo indywidualnego definiowania uprawnienia do danego obiektu poprzez wskazanie wymaganych praw dostępu. Określenie uprawnień polega na przypisaniu potrzebnej autoryzacji użytkownikowi (nazwa profilu) lub grupie użytkowników (nazwa profilu grupowego lub wskazanie grupy użytkowników, do której należy właściciel obiektu) lub wszystkim innym, nie wymienionym użytkownikom. W przypadku określania tej ostatniej autoryzacji może być ona dokonana poprzez odniesienie do listy autoryzacyjnej danego obiektu.

Lista autoryzacyjna jest to specyficzny obiekt systemu operacyjnego komputera AS/400, stosowany zazwyczaj dla uproszczenia zarządzania uprawnieniami. Lista, identyfikowana przez unikalną nazwę, składa się z listy nazw profili wraz z przyznanymi tym profilom uprawnieniami. Ochrona obiektu przez wykorzystanie listy polega na przypisaniu uprawnień do danego obiektu wszystkim

użytkownikom występującym na tej liście i tylko w zakresie wskazanym przez listę. Jedna lista może chronić wiele obiektów, dany obiekt jednak może być chroniony tylko przez jedną listę autoryzacyjną. Zmiana w liście autoryzacji może być dokonana jedynie przez administratora systemu lub programowo przez dziedziczenie uprawnień od użytkownika klasy administratora.

Profil grupowy jest to specjalny typ profilu użytkownika, który nie jest przypisany jakiemukolwiek indywidualnemu użytkownikowi, ale definiuje uprawnienia, warunki pracy oraz parametry domyślne dla prac interakcyjnych i wsadowych wspólne dla grupy użytkowników. Użycie profilu grupowego odbywa się poprzez podanie jego nazwy (odwołanie się) w profilu użytkownika indywidualnego. Ze względu na specyfikę profili grupowych, przyjęte wartości parametrów uniemożliwiają ewentualne wykorzystanie profili grupowych w zadaniach interakcyjnych.

Określenie „profil użytkownika" jest używane w dwu różnych znaczeniach:

- identyfikatora danego użytkownika w systemie operacyjnym (do określania właścicieli obiektów i do zarządzania zadaniami),
- zbioru parametrów definiujących uprawnienia danego użytkownika, warunki jego pracy oraz parametry domyślne dla jego prac interakcyjnych i wsadowych danego użytkownika.

Każdorazowe użycie profilu indywidualnego wymaga poprzedniego uwierzytelnienia (podania hasła znanego tylko właścicielowi profilu). Procedura uwierzytelnienia jest realizowana w trakcie operacji włączania się danego użytkownika do systemu. Wszystkie opisy profili użytkowników są tworzone w sposób ściśle kontrolowany za pomocą narzędzi programowych powiązanych z systemem informatycznym giełdy. Użytkownicy mogą korzystać jedynie z udostępnionych im imiennie narzędzi programowych, umożliwiających limitowany dostęp do systemu informatycznego giełdy, ściśle w zakresie wynikającym z pełnionej funkcji (makler giełdowy, makler specjalista, prowadzący lub nadzorujący sesję giełdową). Każde odwołanie do udostępnionych im funkcji systemu informatycznego giełdy odbywa się tylko za pośrednictwem menu.

Profile są tworzone za pomocą narzędzi programowych. Pracownik tworzący je nie ma uprawnień do dokonywania jakichkolwiek zmian w parametrach tworzonego profilu i oprogramowanie automatycznie przypisuje tworzonemu profilowi podstawowe parametry.

Wszystkie obiekty produkcyjne (dane, programy, obiekty specjalne) należą odpowiednio do czterech utworzonych tylko w tym celu specjalnych profili grupowych: właścicieli wszystkich obiektów w środowisku dla integracji oprogramowania, w środowisku dla testów oprogramowania, w środowisku dla rozwoju oprogramowania oraz w środowisku produkcyjnym. Profile te nie mogą być wykorzystywane jako profile indywidualne.

Dziennik systemowy jest sekwencją zbiorów bazodanowych o narzuconej za pomocą zmiennej systemowej maksymalnej liczbie rekordów. W przypadku przepełnienia się bieżącego zbioru, jest on automatycznie zamykany, a jego rolę przejmuje inny automatycznie utworzony zbiór z automatycznie generowaną nazwą. Konwencja nazewnictwa narzuca wspólny rdzeń nazwy, za którym następuje generowana końcówka – na podstawie daty i sekwencji generacji zbioru w ciągu dnia. W dzienniku systemowym zapisywane są najważniejsze informacje dotyczące zarówno przetwarzania aplikacyjnego, jak i zmian w systemie operacyjnym. Ze względu na dużą liczbę tych informacji, zbiory dziennika przechowuje się na dyskach przez stosunkowo ograniczony czas, natomiast archiwizuje się je na kasetach magnetycznych.

Z kolei dziennik zmian jest obiektem klasy „kronika", do którego podłączany jest obiekt tworzony na bieżąco, a w nim zapisywane są dane dotyczące wystąpienia zapisywanych w kronice zdarzeń. Obiekty bieżące służą do podziału kroniki na rozłączne odcinki, zwykle odpowiadające kolejnym dniom przetwarzania na komputerze. Przedmiotem zapisu w kronice jest: aktywność wskazanych profili, zmiany obiektów i odwołania do obiektów.

W systemie AS/400 mamy następujące kolejki komunikatów:

- związane z operatorem terminala (w szczególności kolejka operatora systemowego, do której automatycznie system operacyjny przesyła komunikaty informujące o statusie zadań i urządzeń, oraz komunikaty wymagające odpowiedzi operatora, często wymagające też podjęcia przez niego ściśle określonej akcji);
- związane ze stacją roboczą;
- związane z programem (mechanizm zwykle służący do synchronizacji procesów).

Najważniejsza jest kolejka operatora systemowego. Zawarte w niej komunikaty muszą być bieżąco obsłużone. Kolejka ta nie podlega archiwizacji, ale jest przechowywana w systemie pomiędzy każdymi sąsiednimi procesami raz na tydzień uruchamianej przez administratora reorganizacji systemu operacyjnego, a w przypadku wątpliwości jest drukowana.

Wraz z rozwojem systemu informatycznego giełdy i pojawieniem się nowych rozwiązań (baza danych ORACLE na komputerze Hewlett Packard, kilkadziesiąt przyłączeń domów maklerskich poprzez WAN, do czego zastosowano routery, czy udostępnienie sieci Internet) wykorzystywane są kolejne zbiory kronik, zawierających ważne informacje o stanie bezpieczeństwa systemu informatycznego giełdy.

Korzystanie z dzienników opiera się na dwóch założeniach:

- błędy o charakterze technicznym bądź wynikające z niedoskonałości oprogramowania aplikacyjnego lub systemowego interpretowane są na bieżąco głównie na podstawie zapisów w: kolejce operatora systemowego, kronice zadania, zbiorach dziennika systemowego, logach błędów sprzętu, logach systemowych dostarczanych przez pakiet technicznego oprogramowania diagnostycznego,

- błędy związane z brakiem autoryzacji do obiektu lub operacji czy też tylko fakty mówiące o wykonaniu pewnych wyspecyfikowanych operacji jako istotnych dla bezpieczeństwa przetwarzania analizowane są w cyklu miesięcznym na podstawie zapisów w dzienniku zmian.

Zabezpieczenia bibliotek produkcyjnych systemu informatycznego giełdy wykonywane są bieżąco poprzez ich przesyłanie z użyciem specjalnego pakietu MIMIX na komputery zapasowe oraz codzienne kopiowanie na taśmy magnetyczne. Taśmy są przechowywane w depozycie bankowym i rotacyjnie wymieniane z następnymi. Zabezpieczenia kwartalne są wykonywane pod koniec ostatniego miesiąca danego kwartału. Jest to kopia wszystkich zbiorów. Ona też jest przechowywana w depozycie bankowym. Po dokonaniu zmian w systemie operacyjnym (poprawki producenta, zmiana konfiguracji) wykonywana jest specjalna kopia całości systemu operacyjnego, która też jest przechowywana długoterminowo w sejfie bankowym.

System Mimix jest specyficznym pakietem bieżącego zachowywania kopii stanu systemu informatycznego komputera AS/400. Podczas jego normalnej pracy, w trybie asynchronicznym, odbywa się proces zachowywania stanu na drugi komputer AS/400. Mimix nanosi zmiany zbiorów fizycznych maszyny produkcyjnej na odpowiadające im zbiory oraz inne wskazane obiekty (np. kolejki, profile użytkowników itd.) na maszynie zapasowej. Zasada korzystania z pakietu Mimix sprowadza się do: kronikowania w specjalnym zbiorze systemowym zmian dokonanych w synchronizowanych między komputerami zbiorach danych, wybierania zapisów z tego zbioru na maszynę odbiorczą w celu utworzenia dynamicznej kopii, automatycznego przełączenia terminali użytkowników z maszyny produkcyjnej na zapasową w przypadku takiej potrzeby. Pakiet Mimix został tak zaprojektowany, że można nim operować zarówno z maszyny nadawczej, jak i odbiorczej. Przewiduje także zmianę kierunku przesyłania, czyli istnieje możliwość zamiany rolami maszyny produkcyjnej i zapasowej. W praktyce obecnej Mimix łączy trzy maszyny – maszynę produkcyjną i dwie maszyny rezerwowe. Mimix ma także wewnętrzny mechanizm bezpieczeństwa opierający się istnieniu specjalnych profili dla kilku klas użytkowników tego systemu. Z punktu widzenia bezpieczeństwa systemu, Mimix umożliwia szybki restart systemu użytkowego w chwili awarii maszyny produkcyjnej. Wadą obiektywną tego rozwiązania jest konieczność utrzymania w stałej gotowości linii komunikacyjnych o odpowiednim poziomie niezawodności.

Wszystkie pamięci dyskowe komputera produkcyjnego AS/400 GPW są wykorzystywane w sposób zabezpieczający przed utratą danych w wypadku awarii pakietu dyskowego. W tym celu wykorzystano przede wszystkim technikę zapisu lustrzanego oraz technikę zapisu *device parity*. Oddzielną sprawą jest podzielenie całej dostępnej pamięci dyskowej na trzy niezależne pule pamięci, cała pamięć dyskowa w ramach jednej puli jest zarządzana jako jeden dysk wirtualny, w następstwie czego kolejne zapisy są rozrzucane po różnych pakietach dyskowych danej puli.

Zdalne kontrolery giełdowej sieci terminalowej umożliwiają, w trybie awaryjnym, przełączenie lokalnej sieci terminalowej typu Twinax, za pośrednictwem połączenia światłowodowego sieci Token Ring w ośrodku głównym i zapasowym, do komputera AS/400 zlokalizowanego w ośrodku zapasowym. Połączenie to czynne byłoby jedynie w przypadku jednoczesnej awarii obu komputerów AS/400 w ośrodku podstawowym. Ponieważ kontrolery korzystają jednocześnie z sieci typu Twinax i Token Ring, wnioski dotyczące bezpieczeństwa są analogiczne jak w przypadku obu sieci traktowanych rozłącznie. Są one włączane jedynie w wyjątkowych sytuacjach, takich jak np. jednoczesna awaria obu komputerów AS/400 w ośrodku głównym giełdy i wyłączane po przywróceniu funkcjonowania przynajmniej jednego z wymienionych komputerów.

Poza działaniami technicznymi, bezpieczeństwu systemu informatycznego giełdy służą działania analityczno-weryfikacyjne. Sprzyja im regularne podnoszenie kwalifikacji zawodowych pracowników. Wyższe kwalifikacje implikują wyższą świadomość i, co za tym idzie, większą szansę eliminacji zagrożeń wynikających z nieświadomości, ataku typu *social engeenering* oraz błędów wynikających z powodu nieprawidłowej obsługi systemu informatycznego.

Wyznaczeni pracownicy kontroli wewnętrznej giełdy otrzymują dostęp do systemu informatycznego giełdy na zasadzie profilu audytorskiego. Umożliwia im on:

- przeglądanie i drukowanie dziennika systemowego (*audit journal*),
- przeglądanie i drukowanie kronik,
- wykonywanie różnych przeglądów logów lub plików uzyskanych z dziennika.

Przeglądy takie mogą być robione *ad hoc* w zależności od potrzeb. Dostępne są też predefiniowane *query* pozwalające wykryć zdarzenia, które mogą być próbą włamania do systemu lub mogą uniemożliwić jego działanie. Oto niektóre z nich:

- podanie błędnego hasła,
- próby zgłoszeń nie istniejących użytkowników lub użytkowników nie posiadających hasła, a więc bez możliwości logowania,
- próby nieuprawnionego dostępu do komend, programów lub danych systemowych,
- użycie profilu administratora,
- usuwanie obiektów systemowych,
- odtwarzanie danych (innych niż wynika to z normalnego funkcjonowania).

Pracownicy kontroli wewnętrznej współpracują też z audytorem zewnętrznym oraz nadzorem rynku giełdowego dotyczącego zakresu poufności danych oraz interpretacji zjawisk na rynku giełdowym. Audyt ten ma charakter systematyczny.

Z kolei audyt prowadzony przez służby informatyczne obejmuje następujące dziedziny:

- sprawdzanie listy profili ze stanem prawnym autoryzowanych użytkowników (na wszystkich komputerach),
- analizę uprawnień użytkowników i ocenę skuteczności ochrony,
- analizę bezpieczeństwa przekazu i aplikacji klientów,
- analizę sprawności technicznej komputerów i sieci transmisyjnej,
- analizę i optymalizację efektywności, a w tym pomiary czasu odpowiedzi, liczby zadań w systemie, wykrywanie zagrożeń w harmonogramie sesji z powodów efektywności,
- obserwację wykonywanych zadań i usuwanie zadań drugoplanowych, które mogłyby zagrozić sprawności przetwarzania,
- analizę błędów wykrywanych przez system operacyjny lub użytkowników i przekazywanie problemów producentom,
- szczegółową analizę zdarzeń, które doprowadziły lub mogły doprowadzić do naruszenia harmonogramu sesji,
- obserwacje i korektę składowania i odtwarzania na komputerach zapasowych (w tym nadzór nad pakietem Mimix),
- analizę przyczyn utraty przez użytkownika prawa do korzystania z systemu,
- analizy zlecane przez zarząd giełdy i inne działy giełdy w różnych sprawach dotyczących bezpieczeństwa i badanie potencjalnych naruszeń zasad.

Pracownicy służb informatycznych współpracują także z audytorem zewnętrznym i komórkami giełdy.

Audyt zewnętrzny jest prowadzony w cyklach miesięcznych przez specjalistyczną firmę zewnętrzną. Zleceniodawcą takiej oceny oraz jej odbiorcą jest kontrola wewnętrzna giełdy. On też w porozumieniu z działem notowań ustala zakres badań comiesięcznych, jak również badań specjalnych. Audyt rutynowy obejmuje analizy zapisu Audit Journala pod kątem stwierdzenia nieprawidłowości w przestrzeganiu zasad bezpieczeństwa systemowego AS/400, w tym zwłaszcza prób nieuprawnionego dostępu, oraz wyjaśnienie przypadków realizowania nietypowego dostępu do danych przez osoby uprawnione, z racji opieki nad systemem, do korzystania z profili o dużym zakresie uprawnień w systemie.

Do zadań wydzielonego stanowiska specjalisty ds. bezpieczeństwa informatycznego należy:

- poszukiwanie zagrożeń i proponowanie zabezpieczeń w zakresie sprzętu i oprogramowania,
- przygotowywanie rozwiązań zabezpieczających,
- przygotowywanie własnych i weryfikacja pozostałych procedur działania,
- wdrażanie narzędzi analizowania pracy systemów giełdowych,
- śledzenie postępu zewnętrznych doświadczeń i wiedzy teoretycznej w zakresie zagrożeń i sposobów im zapobiegania,
- projektowanie zakresu oraz regularne przeprowadzanie okresowych analiz i ocen stanu zabezpieczeń systemu giełdowego,
- podejmowanie współpracy z uznanymi podmiotami specjalizującymi się w tworzeniu standardów i dobrej praktyki w dziedzinie bezpieczeństwa informatycznego.

Janusz Zawiła-Niedźwiecki

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