A C T A U N I V E R S I T A T I S L O D Z I E N S I S
FOLIA OECONOMICA 119, 1992

Gabriela Idzikowska*, Zofia Owczarek**

ZAGROŻENIA DANYCH W SYSTEMACH INFORMATYCZNYCH

Przedmiotem zagrożeń w informatyce są dane. Zagrożenie danych jest wynikiem niewłaściwych działań ludzkich lub zdarzeń losowych dotyczących danych [3]. W tradycyjnych (manualnych) systemach przetwarzania liczba elementów wywołujących zagrożenia była znacznie mniejsza niż obecnie, ponieważ systemy te były mniej skomplikowane. Były one łatwiejsze do przewidzenia i do wykrycia, w porównaniu z bardziej skomplikowanymi technologicznie systemami informatycznymi. Na system informatyczny składa się bowiem wiele elementów (sprzęt, oprogramowanie systemowe i użytkowe, różne grupy osób współpracujących z systemem), a liczebność poszczególnych z nich jest także bardzo duża.

1. Klasyfikacja zagrożeń

Nie istnieje doskonała klasyfikacja zagrożeń. Różni autorzy w różny sposób podchodzą do ich specyfikowania. Niektórzy z nich szczegółowo wymieniają możliwe zagrożenia [3], co nie jest najlepszym rozwiązaniem ze względu na to, że nie sposób przewidzieć ich wszystkich, a więc lista zagrożeń nigdy nie będzie zamknięta. Inni autorzy próbują grupować zagrożenia według rodzajów bądź przyczyn. M a r t i n [5] wyróżnia następujące grupy zagrożeń:

- działanie sił przyrody,
- błędy sprzętu i oprogramowania,
- ludzka niedokładność,
- złośliwe zniszczenie,

* Dr, adiunkt w Katedrze Informatyki.
** Dr, adiunkt w Katedrze Informatyki.

- przestępstwo,
- naruszenie poufności.

M a i r, W o o d, D a v i s wymieniają [3]:
- błędy ludzkie,
- błędy sprzętu i oprogramowania,
- nadużycie komputera,
- katastrofy.

R. P. F i s h e r rozważa zagrożenia z punktu widzenia ochrony danych [3]. Wyróżnia on sześć podstawowych zagrożeń, jakimi są: przypadkowe ujawnienie, przypadkowa modyfikacja, przypadkowe zniszczenie, umyślne ujawnienie, umyślna modyfikacja, umyślne zniszczenie.

Na podstawie różnych klasyfikacji (także nie wymienionych w niniejszym opracowaniu) można wysnuć wniosek, że zagrożenia mogą być przypadkowe lub umyślne. Takie dwie grupy zagrożeń można wyróżnić na podstawie wywołujących je przyczyn.

2. Zagrożenia przypadkowe

Do typowych zagrożeń przypadkowych zalicza się [2]:
- wypadki losowe,
- błędy sprzętu,
- błędy oprogramowania,
- błędy użytkowników.

Wypadkami losowymi mogą być przykładowo: pożar, zalanie, wysoka lub niska temperatura, silne pole magnetyczne. Projektanci i organizatorzy ośrodków obliczeniowych zwykle uświadamiają sobie możliwość zaistnienia tego typu zagrożeń i uwzględniają je w swych pracach. Ponadto istnieją normy budowlane, obowiązujące przy budowie ośrodków lub adaptacji pomieszczeń.

W odniesieniu do sprzętu mogą wystąpić następujące błędy:
- błędy systemu ochrony pamięci,
- uszkodzenia urządzeń pamięci zewnętrznej,
- błędy w logice działania systemu - dopuszczanie zbyt wielu programów do działania w stanie uprzywilejowanym,
- błędy systemu kanałów wejścia i wyjścia,
- uszkodzenia urządzeń transmisji danych,
- błędy w pracy urządzeń szyfrujących.

W przypadku oprogramowania przyczynami zagrożeń mogą być:

- błędy w projektach programów związane z nieprawidłowymi założeniami, niepoprawnymi algorytmami, niewłaściwą strukturą programu,
- błędy w kodowaniu, a więc źle użyte instrukcje, niepoprawnie zbudowane pętle itd.,
- błędy w testowaniu i poprawianiu programów, zwłaszcza gdy poprawki nie są bieżąco dokumentowane,
- błędy w łączeniu niezależnych programów w system programów,
- błędy w oprogramowaniu systemowym, nie wykryte przez producenta,
- błędy w oprogramowaniu systemowym wynikające z wprowadzania zmian na własną rękę,
- błędy związane z brakiem aktualnej i zupełnej dokumentacji programów.

Błędy występujące w tej grupie są szczególnie istotne dla systemu informatycznego, gdyż mogą one prowadzić do zniekształcenia danych. Również niezwykle istotne znaczenie mają błędy danych wejściowych wynikające z nieprzestrzegania standardów dokumentacji.

Potencjalne zagrożenia ze strony użytkowników można podzielić na 4 grupy:

- błędy operatora systemu,
- błędy operatorów urządzeń,
- błędy użytkowników zastosowań,
- błędy dystrybutorów nośników informacji.

Operator systemu i projektanci mogą popełnić błędy w zakresie definiowania, projektowania, organizowania i utrzymania systemu ochrony dostępu do danych. Może to dotyczyć zwłaszcza:

- błędnego definiowania praw dostępu i wykonywania zastrzeżonych operacji (aktualizacji, modyfikacji),
- przeoczenia typów danych wymagających szczególnego zabezpieczenia,
- testowania i uruchamiania mechanizmów ochrony,
- nieprawidłowości w operowaniu hasłami lub przypadkowego ich ujawnienia.

Dużym zagrożeniem dla systemu informatycznego jest również nieprawidłowe postępowanie operatorów urządzeń. Przykładowo może ono polegać na:

- umożliwieniu kopiowania lub modyfikacji nośników magnetycznych niepowołanym osobom w wyniku zbyt małej dbałości o te nośniki,
- przypadkowym skasowaniu zawartości wolumenu magnetycznego,
- popełnianiu błędów w czasie interwencji operatorskich w pracę systemu,
- przypadkowym udostępnieniu chronionych nośników magnetycznych, wydruków, dokumentacji lub czasu maszyny osobom nieupoważnionym.

Ostatnia kategoria błędnego postępowania operatora urządzenia jest charakterystyczna również dla wszystkich dystrybutorów nośników (operator systemu, bibliotekarz zbiorów, pracownicy sekcji kontroli wejścia-wyjścia, użytkownicy zastosowań).

Poza pierwszą grupą zagrożeń przypadkowych (wypadki losowe), pozostałe kategorie nie zawsze są uwzględniane przez osoby projektujące i organizujące eksploatację systemu informatycznego, mimo iż są źródłem większości błędów w danych.

3. Zagrożenia umyślne

Zagrożenia umyślne mają na celu [2]:

- uzyskanie w danym momencie lub zapewnienie stałego dostępu do danych,
- dokonanie zmian zawartości lub zniszczenie części albo całości zbioru danych lub programów,
- zapoznanie się z potrzebami i zainteresowaniami poszczególnych użytkowników w zakresie informacji,
- poznanie struktury i sposobu działania mechanizmów tworzących system ochrony dostępu do danych.

Zagrożenia umyślne prowadzą zwykle do przestępstw komputerowych, rozumianych jako takie działania, które angażują system informatyczny jako środek lub jako obiekt popełniania przestępstwa [1]. Przewiduje się, że w najbliższych latach może nastąpić znaczny wzrost przestępstw komputerowych spowodowany łatwiejszym dostępem do sprzętu (mikrokomputery, sieci, przetwarzanie rozproszone).

W literaturze opisano szereg możliwości popełniania przestępstw komputerowych [1, 2, 4, 5].

Najgroźniejszym typem przestępstwa jest użycie programu, który umożliwi ominięcie wszystkich kontroli w celu modyfikacji lub uja-

wnienia zasobów komputerowych (superzapping). Tę możliwość wykorzystują zwykle programiści systemowi do poprawiania oprogramowania systemowego. W przypadku dużych komputerów lub sieci każde użycie takiego programu jest rejestrowane w dzienniku. Niebezpieczeństwo pojawia się w warunkach przetwarzania rozproszonego, ponieważ autonomiczne mikrokomputery mają bardzo ograniczone możliwości ewidencjonowania historii zdarzeń.

Jedną z groźniejszych metod atakowania systemów informatycznych przez intruzów jest oddziaływanie na oprogramowanie, zwłaszcza systemowe. Polega ono na czasowym lub stałym umieszczeniu w systemie takiego ciągu instrukcji, który zezwala na nieupoważniony dostęp, lub wykonując poprawnie żądaną funkcję wywołuje nielegalne efekty uboczne. Taki przypadek jest określany mianem "konia trojańskiego" (Trojan Horse).

Prostszą metodą oddziaływania na system operacyjny czy też system zarządzania bazą danych jest wykrywanie i wykorzystywanie luk w tym oprogramowaniu (Trapdoors). Przykładowo, w systemie operacyjnym OS/360 można odczytać zawartość zbioru zapisanego w pamięci dyskowej po jego logicznym usunięciu z katalogu poprzez skopiowanie fizycznej pozostałości na dysku.

Oprogramowanie systemowe może być także zagrożone przez jego producenta, który umieszcza moduł aktywizujący się okresowo i w określonych warunkach. Działanie tego modułu może mieć dewastujący wpływ na wszystkie eksploatowane pod jego kontrolą systemy zastosowań (bomba logiczna - logic bomb).

Dość znaną techniką przestępczego oddziaływania na system informatyczny jest kradzież małych ilości zasobów bez jawnego wpływu na całość. Nosi ona nazwę "Salami" i polega na kumulowaniu na rzecz przestępcy kwot wynikających z zaokrągleń.

Kolejna grupa przestępstw dotyczy nieautoryzowanego wykorzystania urządzeń. Można tu wymienić:

- "jazdę na barana" (piggybacking), polegającą na selektywnym przechwytywaniu komunikacji między użytkownikiem a procesorem, tj. podjęciu sesji w momencie, kiedy autoryzowany użytkownik nie kończy swojej współpracy z komputerem po zakończeniu operacji i pozostawia końcówkę bez opieki;

- personifikację (impersonation), oznaczającą udawanie uprawnionego użytkownika lub urządzenia dzięki znajomości sposobu dostępu;

- wejście między liniami (wire tapping), polegające na użyciu specjalnego terminala podłączonego do kanałów komunikacyjnych w celu uzyskania wejścia do systemu w czasie, gdy upoważniony użytkownik nie jest aktywny, ale ma połączenie z kanałem komunikacyjnym;
- atak asynchroniczny (asynchronous attack) realizowany w ten sposób, że przy nakładających się czasach przetwarzania jeden proces próbuje zmienić parametry, które inny proces ogólnie zbadał, ale nie zdążył ich wykorzystać;
- podsłuch (eavesdropping), czyli włączenie się do kanałów komunikacyjnych w celu przechwycenia komunikatu.

Przestępstwa mogą polegać ponadto na łamaniu haseł, kradzieży zbiorów lub sprzętu, szperaniu w koszach z makulaturą w celu ujawnienia danych, haseł lub programów. Trudno obecnie przewidzieć, jakie możliwości popełniania przestępstw komputerowych pojawią się w przyszłości.

4. Zabezpieczenia w systemach informatycznych

W celu przeciwdziałania różnym zagrożeniom można stosować szereg metod zabezpieczenia (ochrony) danych przed nieprawidłowym działaniem na zbiory, zniszczeniem, ujawnieniem, uszkodzeniem itd. Nabiera to szczególnego znaczenia w sytuacji stosowania nowych technologii informatycznych, zwłaszcza baz danych i sieci mikrokomputerowych.

Wszystkie środki ochrony systemów informatycznych można podzielić na środki administracyjne i informatyczne.

Środki administracyjne odnoszą się w szczególności do dużych ośrodków obliczeniowych, ale niektóre z nich mogą być zastosowane w każdych warunkach. Środki te mogą być techniczne bądź zarządcze. Środki techniczne dotyczą właściwej konstrukcji budynku, sali maszyny, instalacji klimatyzacyjnej i elektrycznej, środków ochrony przeciwpożarowej, urządzeń alarmowych, instalacji odgromowej, fizycznej kontroli dostępu do pomieszczeń szczególnie ważnych (np. sali maszyny, biblioteki nośników magnetycznych, magazynu materiałów eksploatacyjnych itd.). Zabezpieczenie zarządcze obejmuje wszelkie problemy związane z właściwą organizacją ośrodków obliczeniowych i pracy poszczególnych komórek. Wiąże się to z:

- kontrolą przyjęć pracowników (wykształcenie, dotychczasowe zatrudnienie, karalność itd.),
- przestrzeganiem tajemnicy służbowej,
- właściwym postępowaniem przy zwalnianiu pracownika (zdanie wszelkich własności ośrodka, zmiana haseł, uprawnień, zezwoleń itd.),
- rozdzieleniem obowiązków i kompetencji między różne grupy uczestniczące w eksploatacji systemu,
- zabezpieczeniem biblioteki dokumentacji, programów i zbiorów danych,
- opracowaniem toku kontroli, a także środków działania na wypadek zdarzeń losowych,
- ustaleniem trybu opracowywania i modyfikacji programów (i systemów),
- szkoleniem pracowników i kontrolą ich działań.

Zabezpieczenie informatyczne może być realizowane przez metody związane z;
- technicznymi środkami weryfikacji,
- kontrolami wbudowanymi w system operacyjny,
- kontrolami wbudowanymi w programy użytkowe.

Urządzenia informatyki mają wbudowane techniczne środki weryfikacji swojej pracy. Mogą one wykryć niesprawność urządzenia, po czym software obsługuje błąd i przekazuje sygnał o diagnozie układowi wykonawczemu (tymi urządzeniami mogą być dodatkowe procesory diagnostyczne, systemy mikroprocesorowe lub specjalizowane układy). Zabezpieczeniem fizycznym może być również zamek blokujący klawiaturę urządzenia.

Od systemu operacyjnego wymaga się:
- zapewnienia prawidłowości zapisu i odczytu na zewnętrznych nośnikach informacji,
- możliwości kontroli kolejności wykonywania obliczeń,
- możliwości kontroli kolejności przetwarzania zbiorów,
- mechanizmów ochrony danych,
- zabezpieczenia przed przypadkową zmianą zawartości zbiorów,
- zabezpieczenia systemu użytkowego.

Wymienione wymagania mogą dotyczyć w ogóle oprogramowania systemowego, a więc również systemu zarządzania bazą danych. W grupie metod zabezpieczenia realizowanych przez oprogramowanie systemowe występują: hasła, klucze ochrony, tablice upoważnień, szyfrowanie, a w szczególności prowadzenie dziennika konsoli. Dziennik

konsoli (kontrolny, systemu, ślad kontrolny) jest jedną z najważniejszych metod podnoszenia bezpieczeństwa w systemach komputerowych. Bez dokładnego dziennika nie jest możliwe zbadanie tego, co zdarzyło się w przeszłości. Może on być wyświetlony bądź drukowany w różnych układach, a jego zawartość może służyć do badań statystycznych (może on stanowić czynnik odstraszający dla potencjalnych intruzów).

Programy użytkowe powinny realizować następujące funkcje kontrolne:

- stwierdzenie dopuszczalności użycia zasobów sprzętu i danych,
- zapewnienie raportów aktualizacji,
- tworzenie kopii bezpieczeństwa zbiorów,
- w procedurach modyfikacji - identyfikacja stanowiska, z którego zmieniono dane (dotyczy systemów wielodostępnych),
- żądanie potwierdzenia w odniesieniu do procedury usuwania rekordów ze zbioru,
- stosowanie cyfry kontrolnej dla identyfikatorów numerycznych,
- przeprowadzanie kontroli formalnej pól w rekordach wejściowych, a także kontroli kompletności dokumentów wprowadzanych do przetwarzania,
- emitowanie tabulogramów kontrolnych z wszelkimi koniecznymi statystykami,
- wyróżnianie trybu zapisu związanego ze stornem i korektą itd.

Podobnie, jak nie można przewidzieć wszelkich możliwych zagrożeń, tak nie sposób przewidzieć i wymienić wszystkich możliwych zabezpieczeń. Realna ocena sytuacji wskazuje, że 100% zabezpieczenia nie da się osiągnąć. Projektowanie zbyt dużej liczby różnorodnych zabezpieczeń informatycznych dla określonego systemu lub systemów może spowodować zmniejszenie efektywności działania. Ten rodzaj zabezpieczeń powinien być stosowany zwłaszcza w odniesieniu do zasobów szczególnie ważnych z punktu widzenia przedsiębiorstwa lub ośrodka obliczeniowego. Wszystkie zasoby natomiast mogą być chronione przy użyciu metod administracyjnych, w tym zarządczych, gdyż są one najskuteczniejsze i najmniej kosztowne.

Literatura

[1] B l a t c h f o r d C., The Automated Office and Computer Crime, A Preliminary Assessment, "Industrial Management and Data Systems", January/February 1986.

[2] D y c z k o w s k i M., Zagrożenia ochrony dostępu do danych w systemach wspomaganego komputerem zarządzania, "Prace Naukowe AE", Wrocław 1983.

[3] F i s h e r R. P., Information Systems Security, Prentice-Hall Inc., Englewood Cliffs, New Jersey 1984.

[4] H o f f m a n L., Poufność w systemach informatycznych, WNT, Warszawa 1982.

[5] M a r t i n J., Security, Accuracy and Privacy in Computer Systems, Prentice-Hall Inc., Englewood Cliffs, New Jersey 1973.

Gabriela Idzikowska, Zofia Owczarek

DATA THREATS IN INFORMATION SYSTEMS

The article discusses the problem of threats connected with introduction of informatics to data processing. There are analyzed typical deliberate and non-deliberate threats (computer offences) and ways of counteracting them.