Jerzy Marek Bednarczyk, Janusz Zawiła-Niedźwiecki

Zarządzanie bezpieczeństwem systemu teleinformatycznego (I)

Znaczenie omawianego problemu dobrze odzwierciedla maksyma, że największym kapitałem instytucji publicznej jest zaufanie jej klientów. Zaufanie to budowane jest między innymi na podstawie przekonujących zasad bezpieczeństwa obsługi. Te zaś coraz częściej są realizowane dzięki systemom teleinformatycznym.

Istotnym elementem podejścia do problemu bezpieczeństwa jest uzyskanie równowagi pomiędzy wprowadzonym poziomem zabezpieczeń a związaną z tym utratą swobody i elastyczności bieżących prac rozwojowych nad systemem oraz kosztami takich zabezpieczeń. Szczególna odpowiedzialność w tym zakresie wiąże się z ewentualnością przenoszenia na klientów ciężaru związanych z tym wydatków.

Zagrożenia dla systemu działania (instytucji)

Potencjalne zagrożenia oraz zasady radzenia sobie z nimi przedstawiono w „Przeglądzie Organizacji" nr 6/97 i 10/97. Przypomnimy tylko, że przed wybraniem właściwych sposobów postępowania należy określić potencjalne skutki zaistnienia danego zagrożenia oraz prawdopodobieństwo jego wystąpienia. Na podstawie takiej oceny można wybrać właściwe z czterech podejść do współistnienia z zagrożeniem: akceptację, nadzorowanie, aktywne jego zmniejszanie lub planowanie ciągłości działania.

W rzeczywistości nie jest łatwo dokonać takiego jednoznacznego przyporządkowania. Inne bowiem będą na przykład koszty nagłego i niespodziewanego zagrożenia, a inne tego zagrożenia, o którym byliśmy wcześniej uprzedzeni. Ważne znaczenie ma też czas trwania szkody lub zagrożenia. Inna jest sytuacja, jeśli awaria trwa kilka godzin, inna, gdy kilka dni lub w najgorszym przypadku nie jest możliwa do usunięcia. Każda z tych trzech sytuacji wymaga odmiennego działania zmierzającego do przywrócenia ciągłości działania. Także używane często określenia: krótkotrwały, znaczący czy długotrwały są pojęciami względnymi, a rzeczywiste znaczenie niesprawności zależy od specyfiki konkretnej firmy i rodzaju zakłócenia. Kilkugodzinna awaria w nocy w instytucji, która pracuje tylko w dzień, jest w tym sensie znacznie „krótsza" od minutowej awarii w trakcie obsługi klienta.

Naturalnym sposobem na zwalczenie krótkotrwałego zakłócenia jest je przeczekać pilnie bacząc końca zagrożenia. Takie postępowanie jest jednak możliwe tylko wtedy, gdy straty finansowe i prestiżowe wynikłe z zatrzymania pracy są wyraźnie mniejsze od kosztów jej utrzymywania. Znaczące zakłócenie wymaga więcej aktywności i wcześniejszych przygotowań. W tej sytuacji firma zazwyczaj ogranicza swoją działalność, udostępniając klientom ograniczony pakiet najważniejszych ze swoich usług. Długotrwałe (rozległe) zakłócenie może oznaczać konieczność organizacji firmy od podstaw, w nowym miejscu, z nowymi ludźmi i z wykorzystaniem nowego sprzętu. Trzeba przy tym pamiętać o konieczności równoczesnego zapewnienia obsługi stałych klientów w czasie rekonstrukcji firmy. Dlatego opracowuje się „Plany Ciągłości Działania", wynikające z nich działania organizacyjne i prawne, uzupełniające zakupy sprzętu itp.

Zagrożenia dla systemu teleinformatycznego

Problematyka bezpieczeństwa odnoszona dawniej do tradycyjnego systemu informatycznego zasadniczo ograniczała się do ochrony komputera i specjalnej sali komputerowej oraz ochrony danych zawartych w pamięci masowej tego komputera, a także skopiowanych na zewnętrzne nośniki. Systemy współczesne są już przeważnie systemami teleinformatycznymi poprzez udział nowego elementu, tj. komunikacji zdalnej, wnoszonego bądź przez samą konstrukcję systemu, bądź przez korzystanie z usług sieci publicznych, takich jak np. Internet czy Reuters. W takich systemach obok dotychczasowych pojawiają się nowe problemy z zakresu bezpieczeństwa. Wynikają one tak z samej technologii, jak i faktu, że zakres funkcjonowania systemu teleinformatycznego może znacznie przekraczać granice samej instytucji, której funkcje realizuje (np. tzw. *home banking* w usługach banków). Przyjrzymy się tym wszystkim problemom, wymieniając tylko tradycyjne.

Zagrożenie bezpieczeństwa informacji w systemie teleinformatycznym ma miejsce, gdy istnieje możliwość nieuprawnionego dostępu do przechowywanych, przetwarzanych lub przesyłanych informacji niejawnych, albo gdy istnieje możliwość nieuprawnionego oddziaływania na sieć w celu zdobycia informacji lub dezorganizacji pracy sieci. Znaczenie poszczególnych zagrożeń zależy od konkretnej sytuacji. Należy realistycznie patrzeć na te zagrożenia oraz na prawdopodobieństwo ich realizacji, wybierając kompromisy między dostępnością systemu

a stopniem bezpieczeństwa (im system bardziej zabezpieczony, tym korzystanie z niego bardziej utrudnione) oraz między kosztem zabezpieczeń a potencjalnymi stratami. Istotne przy tym jest, aby nie szukać tylko bezpośrednich zabezpieczeń informatycznych, lecz przeanalizować wszystkie aspekty problemu. Na przykład architekturę systemu i jego topografię (rozłożenie przestrzenne), która może pozwolić na rezygnację z drogich rozwiązań sprzętowych lub programowych na rzecz tańszej fizycznej ochrony pomieszczeń, budynków czy traktów telekomunikacyjnych. Nie bez znaczenia jest również sama treść przekazu danych. Jeśli są to np. dane przygotowane do publikowania, nie ma konieczności ich ochrony przed odczytem, a wystarczy chronić je przed zafałszowaniem lub zanikiem. Duże znaczenie ma też dobór załogi bezpośrednio obsługującej system informatyczny firmy, jej lojalność wobec firmy, świadomość występujących zagrożeń oraz profesjonalizm w działaniu, co dodatkowo podnieść mogą systematyczne specjalistyczne szkolenia dotyczące bezpieczeństwa systemów informatycznych.

W Polsce nie ma jeszcze wystarczających standardów i norm dotyczących wszechstronnej ochrony przekazu danych komputerowych. Z konieczności instytucje chcące zabezpieczyć swoje systemy informatyczne muszą opierać się na doświadczeniu własnym lub bazują na oprogramowaniu i sprzęcie firm zachodnich, głównie amerykańskich, szwajcarskich i izraelskich. W takich okolicznościach, wobec rozmiaru i wyrafinowania współczesnych zagrożeń, warto rozważyć zorganizowanie odpowiedniej komórki zajmującej się stałym prowadzeniem polityki bezpieczeństwa firmy. Określa ona, co i jak powinno być chronione, ustanawia odpowiedzialność za ochronę poszczególnych elementów systemu, definiuje poziomy zabezpieczeń, nieustannie sprawdza, czy nie ma luk w ochronie, analizuje doświadczenia z przypadków zaistniałych w swojej i innych firmach. Dzięki temu można modelowo oddzielić kwestie wyznaczania i kontroli przestrzegania wewnętrznych standardów bezpieczeństwa od ich implementacji.

Zagrożenia dla materialnych składników systemu

Materialne składniki systemu informatycznego można podzielić na: komputery wraz z wyposażeniem, sieć logiczną, instalacje wspomagające (np. sieć energetyczna, klimatyzacja). Podstawowymi zagrożeniami dla tych składników systemu są: błąd obsługi, niesprawność techniczna urządzeń, awaria zasilania, awaria klimatyzacji, kataklizm (pożar, zalanie, uszkodzenie budynku), sabotaż lub atak terrorystyczny.

Zagrożenia dla niematerialnych składników systemu

Niematerialne składniki systemu teleinformatycznego można podzielić na: systemy operacyjne komputerów, oprogramowanie systemu użytkowego oraz jego dane. Podstawowymi zagrożeniami dla tych składników systemu są: błąd obsługi, utrata, zniekształcenie lub ujawnienie danych albo oprogramowania, oszustwo, włamanie do systemu, sprzeniewierzenie lub ujawnienie informacji, porzucenie pracy lub niespodziewana nieobecność pracownika, niedostępność nośników danych (uszkodzenie, utrata), brak dokumentacji.

Zagrożenia dla komunikacyjnych składników systemu

Wymiana wiadomości pomiędzy użytkownikami sieci teleinformatycznej podlega typowym zagrożeniom. Mogą one pojawić się z przyczyn losowych (np. zmiana zawartości wiadomości w wyniku błędu transmisji) lub mogą być związane z celową akcją ze strony intruza. Może to być podsłuch pasywny, kiedy intruz ma możliwość jedynie poznania treści przesyłanych wiadomości czy też stwierdzenia faktu ich przepływu, lub podsłuch aktywny, kiedy ma on również możliwość ingerencji w przesyłane wiadomości, w ich zawartość lub kolejność. Współczesne techniki przechwytywania informacji stwarzają niestety rozliczne możliwości takiej ingerencji. Dane komputerowe można bowiem przejmować zarówno w ramach transmisji teleinformatycznych, jak i w wyniku analizy fal elektromagnetycznych emitowanych przez sprzęt komputerowy (emisję z mikrokomputera PC można zarejestrować z odległości kilku kilometrów). Przy tym ingerencja może nastąpić z zewnątrz (ze strony osób nie będących użytkownikami systemu) lub (w praktyce częściej) ze strony legalnych użytkowników systemu. Zagrożenia komunikacyjne można więc podzielić na: zagrożenia bierne, tj. nieuprawnione ujawnienie informacji bez aktywnego oddziaływania na sieć (bez zmiany stanu systemu, np.: podsłuch przesyłanej informacji, obserwacja ruchu w sieci, odbiór emisji ujawniającej) oraz zagrożenia czynne, tj. aktywne oddziaływanie na sieć lub jej elementy (preparowanie nie autoryzowanych zmian systemu, np. modyfikacje, powtórzenia lub wstawki fałszywych wiadomości, nieuprawnione zwiększanie możliwości stacji sieciowych, zmiana lub wykasowanie programów sterujących pracą sieci). Najpoważniejszymi z nich są:

Maskarada – stacja (użytkownik) udaje inną stację (użytkownika), a celem jest zdobycie chronionej informacji, tworzenie fałszywych ujść informacji, symulowanie pokwitowań wiadomości, wprowadzanie do systemu fałszywych wiadomości lub przeniesienie kosztów swojej działalności w sieci na innego użytkownika.

Powtórzenia – ponowne nadanie przesłanej już informacji (lub jej części) w celu wytworzenia nieuprawnionego efektu, np. zwiększenia uprawnień.

Modyfikacja – niewykrywalna zmiana treści danych podczas transmisji, zwłaszcza jeśli używane są publicznie znane kody nadmiarowe, gdyż ten sam kod może być wykorzystany do „zabezpieczenia" zmodyfikowanych danych.

Wjazd na barana – wprowadzenie do kanału transmisyjnego własnych danych w czasie trwania seansu łączności między uprawnionymi stacjami,

np. w czasie oczekiwania stacji na pokwitowanie lub podczas rozmowy telefonicznej.

Odmowa usługi – ma miejsce, gdy stacja nie spełnia swoich funkcji lub uniemożliwia właściwą pracę innych stacji, np. likwidując komunikaty kierowane do adresata.

Koń trojański – wprowadzony do systemu powoduje, że stacja realizuje funkcje nieuprawnione, np. kopiuje dane do nieuprawnionego kanału czy umożliwia dostęp do danych nieuprawnionemu użytkownikowi.

Potrzask – występuje, gdy stacja ma zainstalowany ukryty mechanizm umożliwiający: wytworzenie nieuprawnionego efektu na rozkaz np. uaktywnienie zainstalowanego wirusa komputerowego czy wykasowanie programów sterujących.

Analiza ruchu – uzyskiwanie informacji na podstawie obserwacji ruchu w sieci, np. o rozmieszczeniu ważnych użytkowników lub centrów kierowania.

Emisja ujawniająca – elektromagnetyczne przenikanie sygnałów do otaczającej przestrzeni, przewodów i konstrukcji metalowych umożliwiających detekcję informacji.

Usługi zabezpieczeń[1)]

Są to usługi dostarczane przez warstwę komunikujących się systemów, zapewniające odpowiednie zabezpieczenie tych systemów lub przesyłanych danych. Mają one charakter elementarny. Praktyczne realizacje zabezpieczeń zawierają ich kombinacje.

Legalizacja – wymaga poświadczonej informacji składającej się z danych przesyłanych (listy uwierzytelniające) i przechowywanych lokalnie. Obejmuje ona: zalegalizowanie stacji, tj. potwierdzenie, że stacja jest żądaną stacją partnerską oraz legalizację źródła (użytkownika), tj. potwierdzenie, że dane odebrane pochodzą z wiarygodnego źródła.

Wypełnianie zobowiązania (nieodrzucanie) – umożliwia uwiarygodnienie źródła i ujścia danych, zabezpiecza odbiorcę przed próbą wysyłania przez nadawcę fałszywej odmowy przesłania danych, a nadawcę przed fałszywą odmową ich odbierania przez adresata (odbiorcę).

Sterowanie dostępem (kontrola dostępu) – zapewnia ochronę przed nielegalnym wykorzystaniem zasobów dostępnych przez sieć (osiąganych poprzez protokoły sieci). Jest stosowane dla różnych typów dostępu do zasobów, np. czytania, zapisywania, usuwania, przetwarzania informacji. Funkcje sterowania dostępem odrzucają próby nieuprawnionego dostępu, tworzą raporty o takich przypadkach, generują alarmy i zapisują tzw. ślad kontroli zabezpieczeń. Mechanizmy sterowania dostępem mogą być stosowane na końcu połączenia komunikacyjnego lub w każdym punkcie przejściowym.

Integralność danych – ochrona informacji przed zakłóceniem kolejności, zgubieniem, powtarzaniem, wstawianiem lub modyfikowaniem danych przez nieuprawnione działania. Może ona dotyczyć pojedynczej jednostki danych, której długość może być dowolna, lub strumienia jednostek danych.

Poufność danych – ochrona informacji przed nieuprawnionym ujawnianiem. Rozróżnia się: poufność połączenia (zapewniającą poufność wszystkich danych w każdym połączeniu), poufność wybranego pola (konkretnych pól wewnątrz danych) i poufność strumienia ruchu (zapewniającą ochronę informacji, która mogłaby być uzyskana w wyniku obserwacji ruchu).

Jerzy Marek Bednarczyk,
Janusz Zawiła-Niedźwiecki

[1)] W dalszej części tekstu opieramy się na normie PN-92/T-20001/02 (będącej tłumaczeniem normy ISO 7498-2:1989) „Systemy przetwarzania informacji – Współdziałanie systemów otwartych (OSI) – Podstawowy Model Odniesienia – Architektura zabezpieczeń".

Autorzy – Jerzy Marek Bednarczyk jest kierownikiem Zespołu Techniki Dystrybucji w Dziale Informatyki Giełdy Papierów Wartościowych, dr Janusz Zawiła-Niedźwiecki jest pracownikiem Instytutu Organizacji Systemów Produkcyjnych Politechniki Warszawskiej i dyrektorem Działu Informatyki Giełdy Papierów Wartościowych w Warszawie.

Tabela. Niektóre zagrożenia komunikacji oraz usługi, które przed tymi zagrożeniami chronią

USŁUGA / ZAGROŻENIE	Integralność zawartości	Integralność sekwencji	Legalizacja uwierzytelnienie nadawcy	Niezaprzeczalność nadania	Poufność zawartości
Nieuprawniony odczyt wiadomości					X
Wprowadzenie fałszywych wiadomości			X		
Modyfikacja zawartości wiadomości	X				
Powielanie lub przejęcie i opóźniona transmisja		X			
Skasowanie wiadomości		X			
Zaprzeczenie wysłania				X	