Zeszyty
Naukowe nr 764 2007
Uniwersytetu Ekonomicznego w Krakowie

Jan Madej
Katedra Informatyki

Wykorzystanie analizy zachowania u˝ytkownika do wykrywania ataków na bezpiecze*ƒ*stwo systemu informatycznego

1. Wst´p

Technologia informatyczna (TI) ma współcześnie bardzo duże znaczenie. Dzięki swoim zaletom, do których zalicza się szybkość i łatwość przetwarzania, gromadzenia i przesyłania danych, jest wykorzystywana w rożnych dziedzinach życia gospodarczego, społecznego i kulturalnego. Systemy informatyczne[1] (SI) funkcjonują w niemal wszystkich przedsiębiorstwach, instytucjach i organizacjach, pełniąc istotną rolę. Niestety, poza niekwestionowanymi zaletami, technologia ta ma także swoje wady, wśród których za najważniejszą uznaje się podatność na zagrożenia. Dlatego tak duża waga przywiązywana jest do zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informatycznych. Pod tym pojęciem rozumiane są wszystkie czynności związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu[2] [PN-I-13335-1].

[1] Według [*Słownictwo…* 1999] system informatyczny (*Information System*) to system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje.

[2] Wymienione tutaj pojęcia tzw. atrybuty bezpieczeństwa zostały zdefiniowane w [PN-I--13335-1].

Jednak pomimo tego, że problem bezpieczeństwa SI znany jest od lat, dotychczas nie opracowano jednego, skutecznego sposobu, który uchroniłby system przed wszystkimi zagrożeniami. Niniejsze opracowanie[3] poświęcone jest właśnie jednemu z zagrożeń bezpieczeństwa SI – zagrożeniu ze strony użytkownika oraz metodzie jego wykrywania.

2. èródła zagro˝eƒ bezpieczeƒstwa systemu informatycznego

Źródłami zagrożeń bezpieczeństwa SI mogą być jego poszczególne elementy, tzn. sprzęt, oprogramowanie, ludzie oraz przyczyny niezależne czyli zdarzenia losowe.

Zagrożenia związane ze sprzętem są efektem złego funkcjonowania albo awarii fizycznych elementów systemu informatycznego, tj. części komputerowych (np. twardego dysku, płyty głównej) lub urządzeń zapewniających właściwą pracę systemu (np. zasilania, klimatyzacji). Sprzyja temu, przede wszystkim, niska jakość elementów, złe projekty techniczne systemu, nieodpowiedni dobór komponentów oraz brak umiejętności osób konserwujących i obsługujących sprzęt.

Zagrożenia, których źródłem jest oprogramowanie są efektem błędów popełnianych w różnych fazach jego projektowania, tworzenia lub modyfikowania[4]. Poza błędami wynikającymi z samego oprogramowania, niektóre błędy mogą być spowodowane niezgodnością z innymi działającymi programami lub z systemem operacyjnym.

Zdarzenia losowe dzieli się na zewnętrzne – pochodzące od sił przyrody (powódź, wyładowania atmosferyczne, wichura itp.) oraz wewnętrzne – pochodzące z otoczenia systemu informatycznego (pożar, zalanie, zmiany napięcia prądu elektrycznego, pole elektromagnetyczne itp.). Zdarzeniom pochodzącym od sił przyrody nie można zapobiec. Jedynym wyjściem jest zastosowanie mechanizmów, które mogą zminimalizować skutki ich wystąpienia. W przypadku zdarzeń, których źródłem są przyczyny wewnętrzne, możliwości ochrony są dużo większe.

Jednak za główne źródło zagrożeń należy uznać ludzi, którzy w sposób pośredni lub bezpośredni, przypadkowo bądź umyślnie mają wpływ na system.

[3] Artykuł powstał w ramach tematu badawczego nr 43/KI/4/2002/S *Metody i narzędzia analizy danych w systemach informacyjnych*.

[4] Klasycznym już przykładem błędu w oprogramowaniu, który objawił się z wielką siłą dopiero po latach, jest tzw. problem roku dwutysięcznego. Chęć zaoszczędzenia przez twórców programów dwóch bajtów w zapisie daty, kosztowała miliony dolarów, które wydały przedsiębiorstwa, organizacje i rządy wielu krajów na jego usunięcie.

Mogą oni spowodować zarówno złe funkcjonowanie sprzętu i oprogramowania, jak również dokonać ingerencji w inne zasoby systemu.

Rodzaj i wielkość ewentualnego zagrożenia, którego bezpośrednią przyczyną jest człowiek zależy od funkcji, jaką pełni on w systemie, jego umiejętności oraz od tego, czy działa przypadkowo czy celowo. Dlatego też zagrożenia pochodzące od ludzi można podzielić ogólnie na umyślne i nieumyślne.

W tym opracowaniu zagrożenia pochodzące od ludzi określane będą mianem ataków na bezpieczeństwo systemu. Jednak w literaturze przedmiotu można spotkać ten termin wyłącznie w kontekście zagrożeń umyślnych, dlatego, aby podkreślić element woli człowieka, będzie mowa o atakach umyślnych i nieumyślnych. W rzeczywistości, z punktu widzenia skutków wystąpienia zagrożeń oraz metod ochrony i wykrywania ataków, często nie jest istotne, czy są one umyślne czy nie.

W literaturze występuje kilka klasyfikacji ataków. Większość z nich opiera się na założeniu, że funkcjonowanie SI polega na przepływie informacji od źródła do miejsca przeznaczenia (por. np. [Stallings 1997]), co pozwala wyróżnić następujące ataki:

– przerwanie (*interruption*) – zniszczenie systemu lub jego części albo spowodowanie jego niedostępności lub niemożności użycia. Jest to atak na dostępność systemu (np. fizyczne uszkodzenie komputera, przecięcie kabli sieciowych, uszkodzenie struktury katalogów);

– przechwycenie (*interception*) – polega na dostępie osoby niepowołanej do zasobów systemu. Jest to atak na poufność (np. podsłuch w sieci, nielegalne kopiowanie plików);

– modyfikacja (*modification*) – przejawia się tym, że niepowołana osoba uzyskuje dostęp do zasobów i wprowadza w nich zmiany. Jest to atak na integralność (np. zmiana zawartości plików, modyfikacja komunikatów przesyłanych w sieci);

– podrobienie (*fabrication*) – polega na wprowadzaniu do systemu fałszywych obiektów. Jest to atak na autentyczność (np. wysłanie fałszywych komunikatów, wygenerowanie fikcyjnych sprawozdań).

Każdy z ww. rodzajów ataku jest, w mniejszym lub większym stopniu, naruszeniem niezawodności i rozliczalności systemu.

Z punktu widzenia metod wykrywania ataków na bezpieczeństwo systemu istotne jest rozpoznanie kto go dokonał i jakie były jego przesłanki. Ataki mogą pochodzić zarówno od osób projektujących i użytkujących system, jak i od osób z zewnątrz.

Znaczna część ataków nieumyślnych ma charakter przypadkowy i jest efektem nieuwagi, bezmyślności, zaniedbań czy niekompetencji osób uczestniczących w projektowaniu, tworzeniu lub eksploatacji systemu. Rodzajów takich ataków jest wiele, z nich niektóre trudno jest nawet przewidzieć. Ryzyko ich wystąpienia można zmniejszyć poprzez odpowiedni dobór kadry, rozsądne przydzielanie

uprawnień, szkolenia oraz zabezpieczenia programowe i sprzętowe. Inaczej wygląda sytuacja w przypadku ataków umyślnych.

Oczywistym powodem ataków umyślnych są bezpośrednie lub pośrednie, wymierne korzyści pochodzące z ich przeprowadzenia. Dlatego często obiektem ataków są systemy, w których występuje zależność pomiędzy dostępem do informacji a korzyściami finansowymi (np. banki, towarzystwa ubezpieczeniowe). Nigdy jednak nie można wykluczyć takich powodów, jak pragnienie zemsty, zazdrość, ciekawość czy po prostu satysfakcja z włamania do systemu. Niestety występują także ataki, których przyczyn nie można wytłumaczyć w żaden inny sposób jak tylko chęcią wątpliwej rozrywki czy złośliwością. W ostatnich latach liczba takich właśnie ataków nasiliła się dzięki dostępności w Internecie programów do ich przeprowadzania. Zachęca to różne osoby, które nie muszą nawet mieć odpowiednich umiejętności do podejmowania takich prób (zob. np. [Machnacz 2000a; 2000b; Patkowski 2001]). Dlatego w praktyce każdy system informatyczny, choć w różnym stopniu, narażony jest na ataki. Przeciwdziałanie im i ich wykrywanie jest bardzo ważne, gdyż niezauważone mogą wywołać duże i trudne do zidentyfikowania szkody.

Jednym z ataków na bezpieczeństwo systemu jest atak użytkownika (ze strony użytkownika). Jest to oczywiście jedno z zagrożeń pochodzących od ludzi, ale ponieważ stanowi ono obiekt zainteresowania tego opracowania, omówione zostanie dokładniej.

Cechą charakterystyczną tych ataków jest to, że przeprowadzane zostają z wnętrza systemu przez osoby będące jego legalnymi użytkownikami. Wyróżnić można następujące rodzaje ataków użytkownika:

– legalny użytkownik nieumyślnie doprowadza do naruszenia bezpieczeństwa (np. przypadkowo kasuje pliki, wynosi dane poza przedsiębiorstwo, zaraża system wirusem),

– legalny użytkownik umyślnie narusza bezpieczeństwo systemu lub nadużywa swoich uprawnień (np. dokonuje aktu sabotażu, kopiuje dane w celu odsprzedania ich konkurencji, modyfikuje pliki dla osiągnięcia własnych korzyści),

– osoba (intruz) wchodzi w posiadanie uprawnień legalnego użytkownika (np. podpatruje hasło współpracownika) i dokonuje nadużyć „w jego imieniu”[5].

W tej sytuacji rodzi się pytanie, który z ataków stanowi największe zagrożenie dla systemu? Nie ma na nie jednoznacznej odpowiedzi, wszystko zależy od

[5] Jest to sytuacja szczególna i można byłoby przyjąć, że ponieważ ataku nie dokonał osobiście legalny użytkownik systemu nie jest to atak użytkownika. Jednak ze względu na fakt, że intruz działa w imieniu użytkownika (a przez system postrzegany jest jako legalny użytkownik) ten przypadek należy tutaj uwzględnić. Tym bardziej, że można wyobrazić sobie sytuacje, w której legalny użytkownik systemu dopuszcza się ataku, kiedy: po pierwsze pod nieobecność współpracownika korzysta bezprawnie z jego komputera; po drugie otrzymuje niezbędne uprawnienia (np. hasło) od innego użytkownika z prośbą, aby w jego zastępstwie wykonać jakąś pracę.

szeregu innych czynników (np. uprawnień użytkownika, jego umiejętności czy intencji). Z pewnością jednak na uwagę zasługuje przypadek kiedy legalny użytkownik (np. pracownik przedsiębiorstwa) dokonuje umyślnego naruszenia bezpieczeństwa. Ponieważ decydując się już na taki krok, na ogół, posiada odpowiednią wiedzę, umiejętności, znajomość mechanizmów ochrony, zdaje sobie sprawę ze znaczenia i wartości zasobów systemu. Ponadto, dysponując wystarczającą ilością czasu i informacjami o słabych punktach ochrony, może przeprowadzić atak w sposób niezauważony lub zatrzeć po nim wszystkie ślady. Z tych właśnie powodów wynikają trudności z wykrywaniem takich ataków i czasami nawet długotrwała, nielegalna działalność może pozostać niezauważona. Dodatkowym, przykrym aspektem tej sytuacji, jest fakt, że to właśnie legalny użytkownik (pracownik przedsiębiorstwa) celowo dopuścił się przestępstwa lub nadużycia. Niestety sytuacje takie nie należą do rzadkości, według IDC (*International Data Corporation*) statystycznie ponad 70% zarejestrowanych ataków na system miało miejsce z wnętrza przedsiębiorstwa i dokonane było przez osoby pracujące w sieci lokalnej (cyt. za [Stawowski 1998]).

3. Systemy wykrywania włamań

Ponieważ zapotrzebowanie na narzędzia wykrywające zagrożenia systemów informatycznych jest duże, na rynku dostępne są gotowe produkty służące do tego celu[6]. Programy takie określa się mianem systemów IDS (*Intrusion Detection Systems*), co dosłownie oznacza systemy wykrywania wtargnięć. W polskiej terminologii informatycznej przyjęła się nazwa systemy wykrywania włamań i jest ona powszechnie stosowana[7]. Należy jednak pamiętać, że systemy te zajmują się wykrywaniem rożnych rodzajów naruszeń bezpieczeństwa SI, takich jak [Stawowski 1999]:

– włamania (*break-in*) – przejęcie i wykorzystywanie konta i zasobów użytkownika systemu,

– odmowa usługi (*denial of service*) – obniżenie lub zablokowanie dostępności zasobów i usług systemu,

[6] Np. program Stalker firmy Haystack Laboratories, program IDES/NIDES firmy SRI International, program Real Secure firmy Internet Security Systems.

[7] Znaczącym momentem w rozwoju systemów IDS było wystąpienie Dorothy Denning pt. *An Intrusion-Detection Model* na sympozjum *IEEE Symposium on Security and Privacy* w 1986 r. Przedstawiła ona model wykrywania włamań do systemu komputerowego. Od tego czasu terminem *intrusion detection* zaczęto określać tego typu programy. Obecnie systemy IDS pełnią coraz to nowe funkcje, a sam termin stał się bardzo „pojemny". Przykładowo, według E. Amoroso [1999] wykrywanie włamania jest to proces identyfikowania i reagowania na szkodliwą działalność skierowaną przeciw zasobom informatycznym i sieciowym.

– złośliwe użytkowanie (*maliciouse use*) – wykorzystywanie zasobów (usług systemu) niezgodnie z jego przeznaczeniem (np. w celu naruszenia integralności i autentyczności danych),

– przeciek (*leakage*) – niekontrolowane wydobycie informacji z systemu,

– maskarada (*masquerade*) – podszywanie się pod innego użytkownika systemu,

– penetracja (*penetration*) – nieupoważnione rozpoznawanie zabezpieczeń systemu (np. celem znalezienia jego słabych punktów).

Aby zapobiegać zagrożeniom systemy wykrywania włamań korzystają z różnych metod, czasami bardzo skomplikowanych (zob. np. [Amoroso 1999]). Ponadto pełnią one coraz więcej funkcji, a wykrywanie ataków użytkownika stało się tylko jednym z ich zastosowań, które w zależności od systemu realizowane jest z różnym efektem.

4. System wykrywania ataków u˝ytkownika

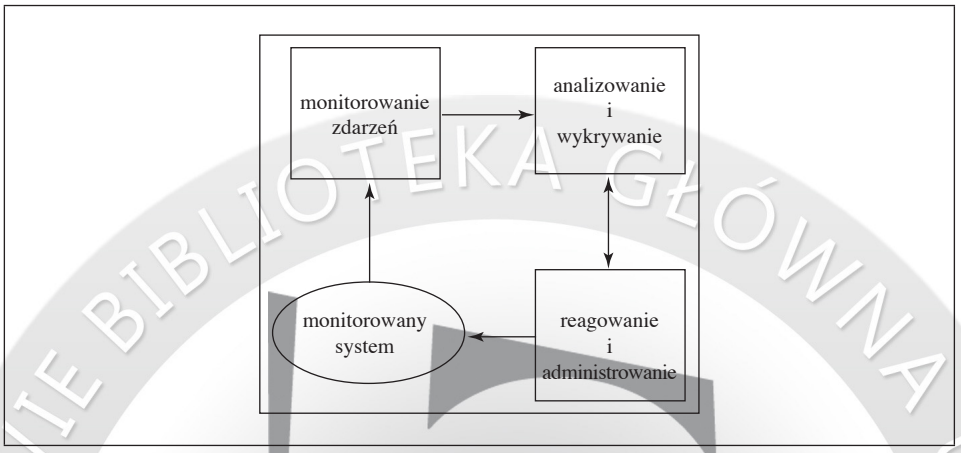
Stosowane w SI metody i środki ochrony ukierunkowane są często tylko na blokowanie dostępu do systemu intruzom z zewnątrz. Tymczasem, jak już wspomniano, duży odsetek ataków ma miejsce z wnętrza systemu i dokonywany jest przez jego legalnych użytkowników. W takiej sytuacji nieodzowne staje się korzystanie z systemów wykrywania ataków użytkownika. Jednak skonstruowanie takiego systemu, choć koncepcyjnie proste, w praktyce napotyka na szereg trudności. Dotychczas nie znaleziono jednego skutecznego i zarazem uniwersalnego sposobu. Wiadomo, że system taki powinien składać się z kilku modułów (rys. 1), które pełniłyby następujące funkcje: monitorowały zdarzenia spowodowane zachowaniem użytkownika, analizowały je, wykrywały ataki na podstawie analizy, a następnie reagowały na nie w odpowiedni sposób. Analiza, wykrywanie i reagowanie powinny opierać się na ustalonych regułach i podlegać administrowaniu.

Najważniejszym i zarazem najtrudniejszym do rozwiązania problemem jest analiza zachowania użytkownika i uzyskanie na jej podstawie odpowiedzi na pytanie, czy nastąpił atak. Idea wydaje się prosta – system zna i kontroluje zachowanie użytkownika, a kiedy ten próbuje zrobić coś niedozwolonego lub zachowuje się podejrzanie – stosownie reaguje. Jednak w rzeczywistości, aby w ogóle było możliwe wykrycie anormalnego zachowania, system musi wiedzieć, jak takie zachowanie wygląda albo jak wygląda normalne zachowanie użytkownika.

Dlatego można wyróżnić dwie metody wykrywania ataków:

– metodę sygnatur anormalnego zachowania (występują tu tzw. sygnatury ataków oraz sygnatury ciągów tekstowych),

– metodę profilu normalnego zachowania.

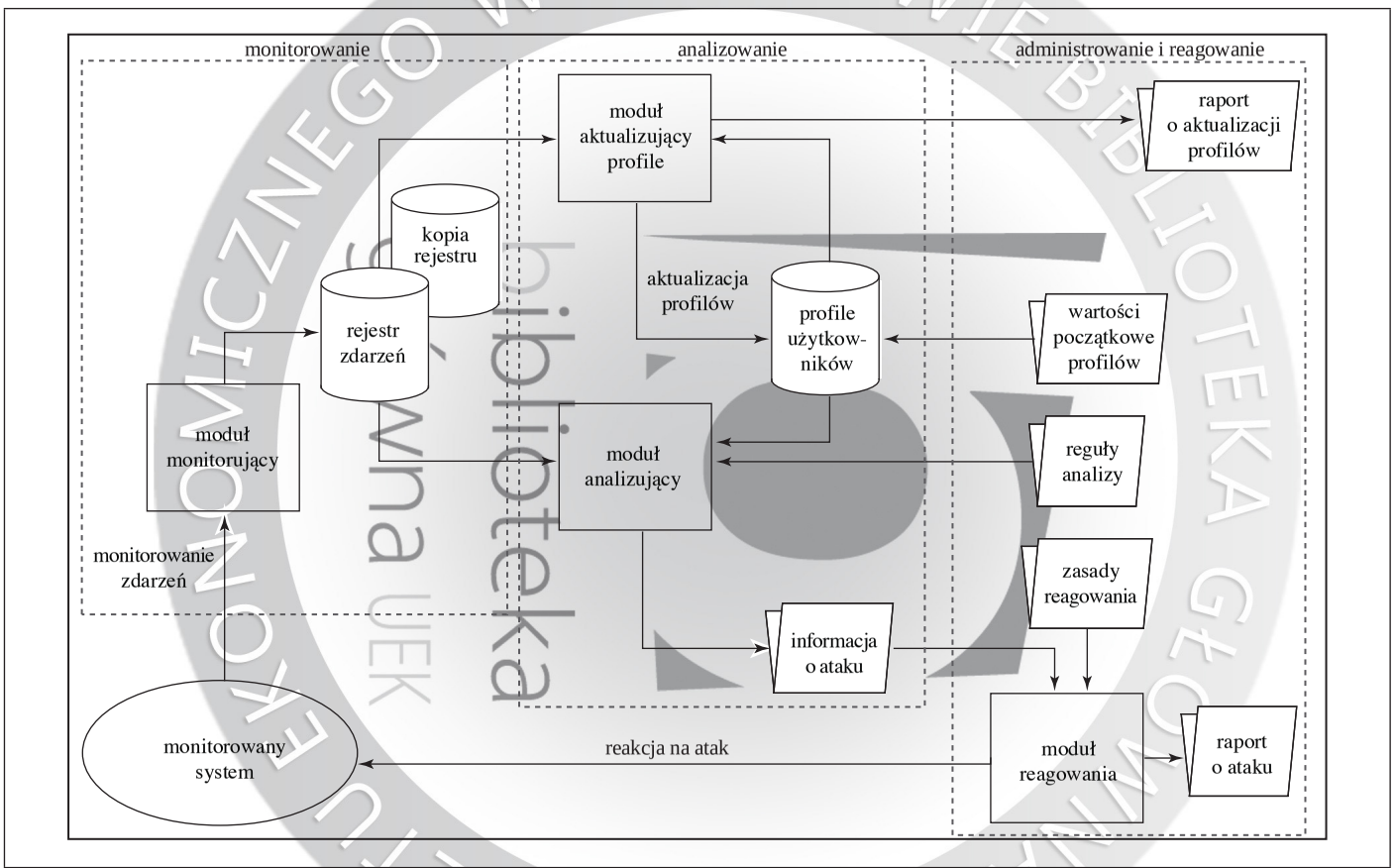


Rys. 1. Schemat wykrywania ataków użytkownika
Źródło: opracowanie własne.

Metoda sygnatur anormalnego zachowania porównuje wykonywane przez użytkownika czynności lub przesyłane i generowane przez niego ciągi znaków z sygnaturami znanych technik i sposobów ataków. Rozwój tej metody zmierza w kierunku systemów ekspertowych analizujących w czasie rzeczywistym zachowanie użytkownika i dopasowujących je do znanych wzorców zachowań podczas prób naruszenia bezpieczeństwa (sygnatur anormalnego zachowania). Informacje na temat wzorców zachowań pochodzą przede wszystkim od specjalistów, a największą trudnością jest zebranie aktualnych danych i odpowiedni sposób ich opisu. Jednak po uporaniu się z tym problemem, wykrywalność ataków, które posiadają swój wzorzec jest bardzo wysoka. Systemy te są poza obszarem zainteresowania niniejszego opracowania.

Metoda profilu normalnego zachowania opiera się na monitorowaniu zdarzeń generowanych przez użytkownika, analizowaniu ich i wykrywaniu tych, które odbiegają od przyjętej dla niego normy. Jednak zachowania użytkownika nie da się przewidzieć ani opisać w sposób jednoznaczny, a występujące odstępstwa od normy nie zawsze świadczą o ataku. Dlatego podczas konstruowania tego typu systemów pojawia się szereg trudnych do rozwiązania problemów. Schemat funkcjonowania systemu wykrywania ataków użytkownika przedstawia rys. 2. Jego opis zamieszczony został w kolejnych podrozdziałach.

Monitorowanie zdarzeń. Monitorowanie przebiegu zdarzeń to punkt wyjścia dla funkcjonowania systemu wykrywania ataków użytkownika. Dostarczane podczas monitorowania dane są wykorzystywane zarówno na potrzeby przeprowadzanej w czasie rzeczywistym analizy, jak i w sytuacji kiedy dojdzie już do ataku i konieczne staje się znalezienie jego przyczyn. Monitorowaniu powinno



Rys. 2. Schemat funkcjonowania systemu wykrywania ataków użytkownika

Źródło: opracowanie własne.

podlegać nie tylko zachowanie zwykłych użytkowników, ale przede wszystkim użytkowników uprzywilejowanych z administratorami włącznie. Dane uzyskane podczas monitorowania muszą mieć odpowiednią postać, która pozwoli na zapisanie ich w bazie danych – tzw. rejestrze zdarzeń. Taki sposób przechowywania umożliwia łatwe wyszukiwanie informacji potrzebnych do analizy. Konieczne jest także odpowiednie zabezpieczenie i sporządzanie kopii rejestru, gdyż podczas ataku jest on szczególnie narażony na zniszczenie w celu zatarcia śladów.

Zdarzenia podlegające rejestracji. Podstawową rzeczą, jaką należy zrobić konstruując moduł monitorowania jest ustalenie listy zdarzeń, które powinny być rejestrowane. Ponieważ sposobów ataków jest wiele, dlatego lista rejestrowanych zdarzeń może być długa. Jednak o tym, które ze zdarzeń będą wykorzystywane podczas analizy decyduje budowa modelu opisującego profil normalnego zachowania użytkownika. Ogólna zasada monitorowania mówi, że „należy śledzić i zapisywać wszystko, co się tylko da". W praktyce oznacza to, że rejestracji powinna podlegać każda operacja wykonana przez użytkownika, a w szczególności:

– częstotliwość otwierania sesji usług sieciowych (ftp, telnet, ssh). Usługi sieciowe mogą służyć różnym celom, np. ftp przekazywaniu danych na zewnątrz przedsiębiorstwa;

– czas trwania otwartych sesji i czas, jaki upłynął od ostatniego korzystania z usług sieciowych;

– próby połączenia się z innymi komputerami lub logowanie się na konta innych użytkowników systemu;

– praca z systemem w godzinach pozasłużbowych. Nietypowe godziny pracy (np. późne godziny nocne) mogą świadczyć o tym, że ktoś korzysta z systemu pod nieobecność użytkownika;

– miejsca skąd następuje połączenie z systemem. Nietypowe miejsca, z których użytkownik dokonuje połączenia (np. spoza granic kraju) mogą świadczyć o próbie włamania;

– częstotliwość dokonywania zmian katalogu (przeglądanie zasobów systemu). Podczas ataku system często jest przeszukiwany w celu znalezienia interesujących dla atakującego plików;

– modyfikowanie i próby usunięcia plików systemowych, logów, plików z historią wydawanych poleceń. Zmiana zawartości ww. plików podczas ataku to często praktyka, której celem jest ukrycie śladów lub modyfikacja systemu na potrzeby kolejnych ataków;

– częstotliwość nieudanych operacji w systemie (np. próby uruchamiania programów, wykonywania poleceń, odczytywania plików, do których użytkownik nie ma uprawnień). Nieudane próby wykonania operacji mogą świadczyć o tym, że ktoś usiłuje dokonać nadużycia lub sprawdza, jakie ma uprawnienia i możliwości;

– operacje na plikach i katalogach, a w szczególności próby ich modyfikacji, kasowania, kopiowania oraz zmiany praw dostępu;

– uruchamianie programów wywołujących błędy systemu operacyjnego lub błędy innych działających programów. Takie sytuacje mogą być umyślnie wywoływane w celu naruszenia stabilności systemu lub uzyskania przez atakującego większych uprawnień;

– próby wykonania poleceń systemowych, które mają wpływ na bezpieczeństwo systemu i jego zasobów (np. polecenia *chmod*, *chown* z systemu Unix);

– uruchamianie programów spoza listy akceptowanego oprogramowania.

W systemie powinien funkcjonować mechanizm nadzorujący programy wykorzystywane przez użytkowników i pozwalający na uruchamianie tylko tych, które zostały zaakceptowane i dopuszczone do użytkowania.

Analiza zachowania użytkownika. Zarejestrowane zdarzenia dostarczają informacji modułowi analizującemu zachowanie użytkownika i wykrywającemu naruszenia. Zasada działania takiego modułu opiera się na założeniu, że zachowanie osoby atakującej lub nadużywającej swoich uprawnień różni się od normalnego zachowania użytkownika. Ponadto zakłada się także, że „odstępstwo od normy" da się zmierzyć i na podstawie uzyskanej różnicy (między zachowaniem normalnym a aktualnym) wyciągnąć wniosek o naruszeniu bezpieczeństwa. Jednak aby takie wnioskowanie było możliwe do przeprowadzenia, należy najpierw skonstruować tzw. profil normalnego zachowania użytkownika.

Profil normalnego zachowania użytkownika to wzorzec, na podstawie którego podejmowana jest decyzja, czy zarejestrowane zdarzenie potraktować należy jako naruszenie bezpieczeństwa czy nie. Z reguły, profil opisywany jest za pomocą modelu matematycznego posiadającego zestaw parametrów, odpowiadających rejestrowanym zdarzeniom. Przy czym to budowa modelu i przyjęte w nim reguły wnioskowania decydują, jakie zdarzenia zostaną w nim uwzględnione.

Zbudowanie profilu nie jest zadaniem łatwym, gdyż wymaga uwzględnienia także charakteru i potrzeb systemu. Ponadto duży problem stanowi uzyskanie danych niezbędnych do ustalenia wartości początkowych profilu. Profil ze źle ustalonymi wartościami początkowymi nie spełnia swojej funkcji, a zanim nastąpi jego aktualizacja na podstawie nowych danych, może już dojść do niezauważonych ataków. Dlatego w takiej sytuacji należy uwzględnić wszelkie dostępne informacje o użytkowniku i ustalić wartości początkowe profilu na podstawie:

– danych uzyskanych z analizy logów systemowych, dzienników zapór *firewall* lub innych programów, które zapisują operacje użytkowników. Trzeba jednak pamiętać, że takie pozyskiwanie danych jest bardzo pracochłonne, a na dodatek nie gwarantuje oczekiwanego efektu;

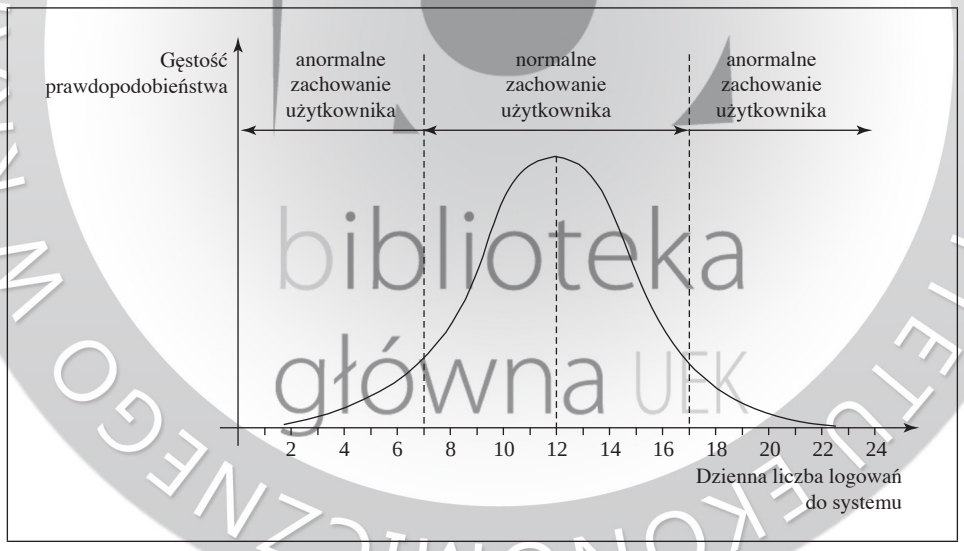
– odgórnie przyjętych założeń. Wadą tego rozwiązania jest konieczność posiadania szczegółowej wiedzy na temat zachowania poszczególnych użytkowników lub ich grup.

Do budowy profilu normalnego zachowania użytkownika, analizy i podejmowania decyzji o naruszeniu bezpieczeństwa najczęściej wykorzystywane są następujące metody:

– modelowanie zachowania użytkownika za pomocą narzędzi statystyki matematycznej,

– modelowanie zachowania użytkownika za pomocą modelu Markowa.

Podczas modelowania zachowania użytkownika za pomocą narzędzi statystyki matematycznej poszczególne parametry profilu traktowane są jako zmienne, a obliczane miary (wartość oczekiwana, wariancja, odchylenie standardowe) pozwalają podjąć decyzję na temat jego zachowania. W najprostszym przypadku wykrycie ataku następuje poprzez porównanie wartości zarejestrowanych zdarzeń z odpowiadającymi im wartościami oczekiwanymi profilu użytkownika. Jeżeli wykraczają one poza przyjęte granice, wtedy uznaje się, że doszło do naruszenia bezpieczeństwa (rys. 3).



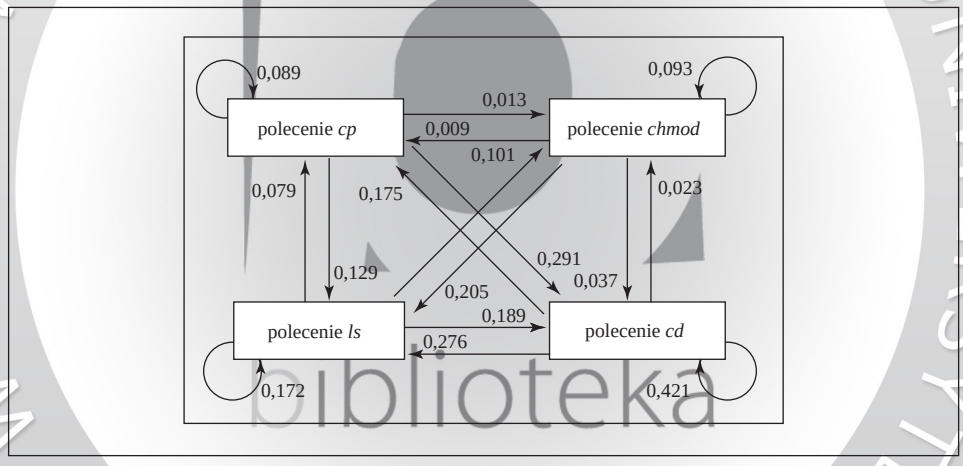
Rys. 3. Przykładowy rozkład zachowania użytkownika

Źródło: opracowanie własne.

W bardziej złożonych modelach brane są pod uwagę także korelacje i wzajemne zależności przyczynowo-skutkowe pomiędzy poszczególnymi zmiennymi, zdarzeniom przypisywane są odpowiednie wagi i uwzględniany jest czynnik

czasu[8]. Wszystko to pozwala na lepsze modelowanie zachowania użytkownika i trafniejsze podejmowanie decyzji o charakterze jego działań.

Modelowanie zachowania użytkownika za pomocą procesu Markowa polega na ustaleniu prawdopodobieństwa przejść pomiędzy kolejno wykonywanymi przez niego operacjami (rys. 4). Wykorzystywane jest ono najczęściej do określania kolejności uruchamianych programów i wydawanych poleceń. Modelowanie to zakłada, że pracę użytkownika charakteryzuje pewna określona kolejność operacji. Okazuje się, że w praktyce przynosi to dobre rezultaty podczas wykrywania sytuacji anormalnych. Użytkownicy bardzo często mają indywidualny sposób postępowania w czasie pracy z systemem. Wynika to z ich przyzwyczajeń, upodobań czy charakteru wykonywanej pracy. Zmiana kolejności lub uruchamianie programów, z których użytkownik wcześniej nie korzystał (bo ich np. nie znał) może być łatwo wychwycona i świadczyć o zaistnieniu sytuacji anormalnej.



Rys. 4. Przykładowe prawdopodobieństwa przejść przy wykonywaniu poleceń użytkownika

Źródło: opracowanie własne.

[8] Wzajemne zależności pomiędzy zdarzeniami i ich przyczynowo-skutkowy charakter pełnią istotną rolę w opisie zachowania użytkownika. Przykładowo, zmiana hasła przez użytkownika powoduje modyfikację pliku z hasłami i jest to zjawisko normalne, gdy tymczasem sama modyfikacja tego pliku (bez polecenia zmiany hasła) może świadczyć o próbie ataku. Przypisywanie wag zdarzeniom ma za zadanie ustalić ich faktyczne znaczenie. Przykładowo, skasowanie przez użytkownika pliku ze swojego katalogu nie jest tak istotne jak usunięcie pliku systemowego. Uwzględnienie czynnika czasu przy analizowaniu zdarzeń pozwala na lepsze odwzorowanie zachowań użytkownika. Przykładowo, może okazać się, że użytkownik inaczej zachowuje się np. w poniedziałek (kiedy rozpoczyna tydzień pracy), a inaczej w piątek (pod koniec tygodnia pracy).

Nieodzownym elementem, który umożliwia w dłuższym czasie korzystanie z opisu zachowania użytkownika za pomocą profilu, jest moduł aktualizacji. To dzięki niemu możliwe jest poprawne funkcjonowanie systemu wykrywania ataków. System musi uwzględniać zmiany, jakie pojawiają się w zachowaniu użytkownika i wynikają z nowo zdobytych umiejętności, innego sposobu pracy, nowych obowiązków czy utrwalania się pewnych przyzwyczajeń. Aktualizacja taka powinna odbywać się automatycznie, jednak osoba nadzorująca funkcjonowanie systemu musi otrzymywać raporty informujące o zmianie profilu normalnego zachowania użytkownika. Celem raportów jest dodatkowa weryfikacja słuszności wprowadzonych zmian.

Reagowanie na atak. Sytuacja, w której moduł analizowania uznał, że nastąpiła próba ataku lub nadużycia uprawnień, wymaga podjęcia odpowiedniej akcji celem uniknięcia zagrożenia lub zminimalizowania strat. Ustalenie, jakie działania należy podjąć, nie jest łatwe. Możliwe do przyjęcia są następujące akcje (mogą być one przeprowadzone łącznie):

– wysłanie komunikatu (ostrzeżenia) do użytkownika,
– zablokowanie konta i działań użytkownika,
– wysłanie komunikatu lub złożenie raportu administratorowi.

Każda z powyższych możliwości posiada swoje ograniczenia[9], dlatego jej wybór powinien być uzależniony od charakteru, wagi i sposobu naruszenia bezpieczeństwa. Generalnie, podjęte środki powinny być proporcjonalne do wykonanych przez użytkownika czynności[10]. W praktyce można często spotkać się z opinią, że lepiej jest stosować ostrzejsze środki i natychmiast blokować dalsze operacje użytkownika niż dopuścić do naruszenia bezpieczeństwa systemu. Ponadto, takie postępowanie „dyscyplinuje" użytkowników i sprawia, że czują się kontrolowani, co z kolei zniechęca do nadużyć. Z przyczyn oczywistych podejście to ma również swoich przeciwników.

Pomimo prac stymulowanych dużym zapotrzebowaniem na systemy tego typu, ściśle sprecyzowanych celów oraz możliwości przeprowadzania doświadczeń, systemy te w dalszym ciągu nie są doskonałe. Charakteryzują się dużymi wahaniami skuteczności, a ich budowa, wdrażanie i funkcjonowanie napotyka na szereg problemów. Podstawowym powodem tego stanu rzeczy jest duża nieprzewidywalność i zmienność zachowania użytkownika oraz pojawiające się, coraz to nowe, metody ataku.

[9] Przykładowo, wysłanie komunikatu może tylko ostrzec atakującego i sprawi, że przyśpieszy on atak, zaś zablokowanie konta użytkownikowi, który przez pomyłkę wykonał niedozwoloną operację spowoduje, że nie będzie mógł on dalej pracować.

[10] Przykładowo, na przeglądanie przez użytkownika katalogów systemowych można zareagować tylko ostrzeżeniem, ale skasowanie np. pliku z hasłami powinno doprowadzić do zablokowania jego dalszych działań.

Podczas funkcjonowania systemy mogą generować dwa rodzaje błędów:

– fałszywy alarm – sygnalizowanie ataku, kiedy w rzeczywistości użytkownik nie robi niczego złego (np. po powrocie ze szkolenia sprawdza nowo zdobyte umiejętności);

– niska wykrywalność ataków – związana np. ze zbyt dużą tolerancją systemu, monitorowaniem niewłaściwych zdarzeń lub postępowaniem atakującego nie odbiegającym od normalnego zachowania użytkownika.

W tym zakresie wysiłki twórców skierowane są na minimalizację obu rodzajów błędu oraz na zaprojektowanie mechanizmu łatwego sterowania „czułością" systemu.

Poza wymienionymi błędami systemy te napotykają także na inne trudności:

– trudności z wykrywaniem ataków użytkowników, którzy w momencie tworzenia profilów normalnego zachowania dopuszczali się już nadużyć i profil został skonstruowany z ich uwzględnieniem,

– trudności z wykrywaniem ataków użytkowników, którzy stopniowo dopuszczają się nadużyć i profil jest aktualizowany z ich uwzględnieniem,

– trudności z ustaleniem wartości progowych. W przypadku wielu zdarzeń trudno jest ustalić, gdzie dokładnie przebiega granica, po przekroczeniu której sytuację należy uznać za anormalną[11],

– znaczne obciążenie systemu informatycznego (sieci komputerowej) przez rozbudowany system wykrywania ataków lub podczas pracy dużej liczby użytkowników,

– możliwość zablokowania lub obniżenia sprawności systemu poprzez umyślne generowanie zachowań anormalnych,

– wykrywanie ataku po jego wystąpieniu, tzn. kiedy szkoda została już wyrządzona (np. system wykrył atak po skasowaniu plików).

5. Praktyczne rozwiązania w zakresie wykrywania ataków na bezpieczeństwo systemu informatycznego

Pomimo szeregu wspomnianych wyżej trudności, systemy wykrywania ataków użytkownika są konstruowane i funkcjonują, przede wszystkim, jako jeden z elementów systemów IDS. Poniżej zostały przedstawione i krótko scharakteryzowane najpopularniejsze na rynku tego rodzaju systemy (por. np. [Muszyński 2001]):

– *RealSecure* firmy *Internet Security Systems* (zob. http://www.iss.net) jest jednym z najpopularniejszych systemów IDS. Jego funkcjonowanie opiera się na technikach wykrywania nadużyć, uzupełnionych o mechanizmy wykrywania

[11] Przykładowo, ustalenie na maksymalnie 10 liczby dziennych logowań do systemu może okazać się niewystarczające w sytuacji kiedy np. serwer jest przeciążony i często zrywa połączenia.

anomalii. *RealSecure* jest zaprojektowany w formie modułów inspekcyjnych, analizujących ruch sieciowy oraz działania użytkowników w systemie operacyjnym. System umożliwia wykrywanie, alarmowanie i blokowanie ataków z sieci oraz nieautoryzowanych działań użytkowników lokalnych. System cechuje architektura rozproszona, na którą składają się trzy podstawowe komponenty: *Network Sensor* (moduł analizujący ruch sieciowy, wykrywający znane wzorce ataków, działania podejrzane oraz inne zdefiniowane zdarzenia), *OS Sensor* (moduł dokonujący analizy zdarzeń rejestrowanych w systemie operacyjnym komputera, wykrywający m.in. znane wzorce ataków i działania podejrzane) oraz *Workgroup Manager* (konsola umożliwiająca scentralizowane zarządzanie modułami inspekcyjnymi);

– *ICEpac* to zestawem produktów (zob. http://blackice.iss.net) zawierający zarówno sieciowe system IDS, jak i IDS działający w węzłach sieci. Posiada on zdalnie instalowane i zarządzane oprogramowanie klienckie (*BlackICE Agents*, *Sentry* i *Guard*), które monitoruje w czasie rzeczywistym ruch pakietów w sieci we wszystkich jej warstwach i wykonuje pełną analizę protokołów. Oprogramowanie to, w razie wykrycia podejrzanych działań, blokuje dostęp do chronionego komputera i wysyła zawiadomienie o ataku do modułu *ICEcap Manager*, który zbiera wszystkie dane, alarmuje i blokuje pozostałe komputery w sieci;

– *Cisco Secure IDS* firmy *Cisco Systems* (zob. http://www.cisco.com) jest typem sieciowego sytemu IDS, co oznacza, że opiera się na ciągłym monitorowaniu całego ruchu w przydzielonej mu podsieci, porównując pakiety oraz konteksty pakietów z wzorcami ataków. Cechą wyróżniającą ten produkt jest fakt, że jest on dostarczany jako dedykowane urządzenie sieciowe wyposażone w odpowiednie oprogramowanie;

– *eTrust Intrusion Detection* firmy *Computer Associates* (zob. http://www.cov.com) oferuje funkcje inwigilacji, wykrywania intruzów i ataków, wykrywania i blokowania nieodpowiednich adresów URL, generowanie alarmów i logów oraz reagowania w czasie rzeczywistym;

– *NetProwler* firmy *Symantec* (zob. http://www.symantec.com) implementuje trzywarstwową architekturę zapewniającą odpowiednią skalowalność w dużych sieciach. Te trzy warstwy to: Agent (komponent instalowany na dedykowanych komputerach, przeznaczony do monitorowania ruchu w podsieci, do której jest przyłączony), *Manager* (repozytorium oparte na bazie danych SQL i zawierające informacje konfiguracyjne oraz informacje alarmowe o atakach), *Console* (konsola wyświetlająca ataki wykryte przez wszystkich agentów znajdujących się pod jej kontrolą. Pozwala także na konfigurowanie i zarządzanie wszystkimi agentami).

6. Zakończenie

Na zakończenie należy przedstawić zostanie kilka zaleceń i postulatów, które mogą być pomocne przy dalszym rozwoju i wdrażaniu systemów wykrywania ataków. Zaliczyć do nich można:

– tworzenie systemów operacyjnych z wbudowanymi mechanizmami szczegółowego rejestrowania zachowania użytkownika;

– opracowanie odpowiednich mechanizmów systemu operacyjnego połączonych z systemem wykrywania ataków, które umożliwią usunięcie szkód spowodowanych działaniem użytkownika;

– określenie standardowych poziomów bezpieczeństwa operacji wykonywanych przez użytkownika w obrębie systemu informatycznego. Pozwoli to lepiej kontrolować zagrożenia spowodowane operacjami użytkownika;

– utworzenie standardowej metody opisu zachowania użytkownika, niezależnej od platformy systemowej i sprzętowej. Pozwoli to na szerszą kontrolę użytkowników oraz na łatwą wymianę informacji o ich zachowaniu;

– utworzenie ogólnoświatowego, standaryzowanego systemu przekazywania danych o metodach ataków na bezpieczeństwo systemu.

– realizowanie w systemach informatycznych odpowiedniej polityki bezpieczeństwa w zakresie nadawania uprawnień i nakładania ograniczeń. Tam, gdzie jest to możliwe, należy korzystać z zasady wszystko co nie jest dozwolone jest zabronione;

– dbałość o odpowiedni dobór personelu oraz przeprowadzanie szkoleń dla pracowników z zakresu bezpieczeństwa systemów informatycznych;

– stosowanie w systemach informatycznych odpowiednich procedur podczas zwalniania pracowników – tzn. automatyczne blokowanie kont i odbieranie uprawnień już w momencie przekazania wypowiedzenia;

– bieżące usuwanie z systemu informatycznego martwych i tymczasowych kont użytkowników;

– stosowanie mechanizmów pozwalających uruchamiać tylko zaakceptowane programy.

Niektóre z przedstawionych zaleceń można zrealizować bardzo łatwo, inne wymagają czasu i pewnych nakładów finansowych, a jeszcze inne dalszych badań, doskonalenia technik i skoordynowania prac przedstawicieli różnych dziedzin. Jednak warto je rozważyć, gdyż zapotrzebowanie na tak ważne narzędzie jak system wykrywania ataków będzie rosnąć w miarę rozwoju i znaczenia TI.

Literatura

Amoroso E. [1999], *Wykrywanie intruzów. Wprowadzenie do monitorowania, korelacji, tropienia, pułapek i reagowania w Internecie*, Wydawnictwo RM, Warszawa.
Dudek A. [1998], *Nie tyko wirusy*, Wydawnictwo Helion, Gliwice.
Klander L. [1998], *Hacker Proof czyli Jak się bronić przed intruzami*, Zakład Nauczania Informatyki Mikom, Warszawa.
Machnacz A. [2000], *Inżynieria społeczna*, dodatek specjalny do PCKurier 21/2000, *Bezpieczne sieci*, Wydawnictwo Lupus, Warszawa.
Machnacz A. [2000a], *Przestępcy i ich motywy*, NETforum 10, Wydawnictwo Lupus, Warszawa.
Machnacz A. [2000b], *Profil przestępcy*, NETforum 11, Wydawnictwo Lupus, Warszawa.
Muszyński J. [2001], *Systemy wykrywania włamań do sieci* [w:] [NetWorld www].
Patkowski A.E. [2001], *Z perspektywy napastnika*, NetWorld 6, Wydawnictwo IDG Poland SA, Warszawa.
Słownictwo znormalizowane. Technika informatyczna [1999], Polski Komitet Normalizacyjny, Warszawa.
PN-I-13335-1 [1999], *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa.
Robling Denning D.E. [1993], *Kryptografia i ochrona danych*, Wydawnictwo Naukowo-Techniczne, Warszawa.
Stallings W. [1997], *Ochrona danych w sieci i intersieci*, Wydawnictwo Naukowo-Techniczne, Warszawa.
Stawowski M. [1998], *Ochrona informacji w sieciach komputerowych*, Wydawnictwo ArsKom, Warszawa.
Stawowski M. [1999], *Badanie zabezpieczeń sieci komputerowych – Testy penetracyjne, Symulacja włamań, Analiza zabezpieczeń*, Wydawnictwo ArsKom, Warszawa.
Zarządzanie bezpieczeństwem [2000], red. P. Tyrała, międzynarodowa konferencja naukowa, Kraków 11–13 maja, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków.

Utilization of User Behaviour Analysis for the Detection of Attacks on Computer System Safety

The article is devoted to the detection of attacks on a computer system safety with application of analysis of its users activities. As a result of user behaviour analysis, the construction of so called Intrusion Detection System (IDS) is possible. The IDS system monitors, registers and analyses user behaviour and on this basis tries to detect potential attacks on a computer system safety. The paper presents a general model of IDS systems operation and discusses particular stages of their activity. The difficulties and limitations connected with the creation and performance of such systems have also been considered. At the end, the existing IDS solutions, available in the market, have been briefly characterized.