Andrzej Szymonik

Zagrożenia systemu informatycznego

Zarządzanie logistyczne w wojskowej jednostce budżetowej wiąże się z pozyskiwaniem, gromadzeniem i przetwarzaniem olbrzymiej ilości informacji. Zaspokajanie potrzeb informacyjnych dla realizacji funkcji zarządzania wymaga stworzenia systemu informacyjnego[1], zapewniającego ciągły dostęp do aktualnych, dokładnych i prawdziwych informacji. Współczesne systemy informacyjne uległy skomputeryzowaniu i określane są jako systemy informatyczne[2]. Dzięki nim uzyskuje się:

- poprawę jakości zarządzania i kierowania
- komputerową wymianę informacji między uczestnikami ciągle wydłużającego się „łańcucha logistycznego"
- standaryzację komputerowych dokumentów zarządzania i kierowania oraz standaryzację ich obiegu
- zwiększenie wiarygodności procesów decyzyjnych i planistycznych
- obniżenie kosztów logistycznych
- zwiększenie skuteczności i niezawodności działania „łańcucha logistycznego".

Nowoczesne logistyczne systemy informatyczne, działające na olbrzymich przestrzeniach, narażone są na wszelkiego rodzaju niebezpieczeństwa. Informacje przesyłane w sieciach komputerowych mogą być przechwytywane lub modyfikowane przez osoby niepowołane. Dlatego bezpieczeństwo informacyjne jest poważnym problemem.

Zagrożenia dla systemu informacyjnego pod względem źródła pochodzenia można podzielić na[3]:

- **losowe** (np. temperatura, wilgotność, zanieczyszczenia, zakłócenia systemu zasilania, kataklizmy, wojna, błędy operatora, błędy administratora, wadliwa konfiguracja systemu, zaniedbania, defekty struktury, sprzętu)
- **intencjonalne** (świadome i zamierzone).

Zagrożenia intencjonalne mogą mieć postać:

- **pasywną** (np. podsłuch – sniffing, podgląd – obserwacja lub monitorowanie pola elektromagnetycznego, analiza ruchu – częstość transmisji, źródło, miejsce przeznaczenia informacji)
- **aktywną** (np. modyfikacja, usunięcie informacji, wprowadzenie własnego komunikatu, przekierowanie informacji, powtarzanie, podszywanie się pod osobę uprawnioną, pośrednictwo).

Prywatność danych i bezpieczeństwo sieci komputerowych przedsiębiorstw w coraz większym stopniu są zagrożone wymyślnymi atakami.

W sieciach komputerowych, techniki ataków można sklasyfikować w trzech kategoriach[4]:

- sieciowe
- na system operacyjny
- na aplikacje.

Ataki sieciowe dotyczą infrastruktury komunikacyjnej, a ich celem mogą być urządzenia sieciowe, takie jak routery i przełączniki, a także protokoły warstwy sieciowej na serwerach. Celem ataku sieciowego jest zazwyczaj uzyskanie uprawnień pozwalających na manipulowanie ustawieniami konfiguracyjnymi, mającymi wpływ na trasowanie ruchu komunikacyjnego. Są wśród nich ataki typu DoS *(denial of service attacks)* przez uniemożliwienie działania – odmowa usługi. Mamy w nich do czynienia z działaniem mającym na celu utrudnienie lub uniemożliwienie prawowitym użytkownikom korzystania z jakiejś usługi lub zasobu. W tym przypadku celem jest załamanie serwera lub co najmniej znaczne spowolnienie jego pracy.

Ataki na system operacyjny wykorzystują cały szereg błędów i luk w powszechnie stosowanych systemach operacyjnych. Najczęściej wykorzystywana jest koncepcja superużytkownika (*root* w systemach Unix lub administratora w systemach Microsoft Windows). Taki uprzywilejowany użytkownik przechodzi bez przeszkód przez wszystkie środki ochrony wbudowane w system operacyjny, może więc mieć dostęp do wszystkich plików (łącznie z systemowymi) i urządzeń, tworzyć nowych użytkowników i nadawać im uprawnienia. Większość technik uzyskiwania uprawnień superużytkownika lub administratora wykorzystuje tzw. efekt przepełnienia bufora. Technika ta pozwala włamywaczowi na wprowadzenie własnego kodu do innego programu pracującego na komputerze i wykonaniu go w kontekście uprawnień przewidzianych dla tego programu. Zazwyczaj taki podrzucony kod zakłada konto nowego, uprzywilejowanego

[1] Szmit M.: *Informatyka w zarządzaniu* Warszawa 2003, def. „System informacyjny jest to zbiór wszystkich elementów (i relacji pomiędzy nimi) odgrywających rolę w procesie przepływu informacji w organizacji".
[2] Ibidem „System informatyczny jest to skomputeryzowana część systemu informacyjnego, a zatem jest to zbiór wszystkich elementów (i relacji pomiędzy nimi) odgrywających rolę w procesie przepływu informacji wykorzystujących przy tym techniczne środki przetwarzania informacji".
[3] Kusina B.: *Zarządzanie bezpieczeństwem teleinformatycznym*, Materiały szkoleniowe firmy EduSoft.
[4] *Vademecum teleinformatyka II*, Praca zbiorowa, wydanie specjalne Networld, Wyd. IDG Poland SA, Warszawa 2002.

użytkownika. Umożliwia to włamywaczowi legalne wejście do systemu przez zalogowanie się na to konto.

Ataki aplikacyjne. Wraz z rozwojem Internetu pojawiły się powszechnie stosowane aplikacje, takie jak serwery webowe, serwery poczty elektronicznej czy serwery DNS. Takie aplikacje są częstym celem włamywaczy, gdyż – z definicji – nastawione są na ciągłe oczekiwanie na komunikację z Internetu, a użytkownicy zewnętrzni mogą uzyskiwać do nich dostęp bez pośrednictwa zapór (ścian) ogniowych.

Do ataków na serwer webowy wykorzystywane są odpowiednio przygotowane zlecenia protokołu HTTP, uznawane za legalne z punktu widzenia ściany ogniowej, ale wykorzystujące słabe punkty serwera i umożliwiające dostęp do poufnych informacji zgromadzonych w bazach danych lub wykonania własnego programu na zaatakowanym serwerze webowym.

Innym przypadkiem są serwery DNS, po opanowaniu których można łatwo manipulować bazą adresową Internetu, kierując poufne informacje pod podmienione adresy fizyczne.

Główne rodzaje ataków

Przepełnienie bufora ***(Buffer overflow)***[5]. Przepełnienie bufora jest popularną metodą ataku na serwery internetowe. Jest ono możliwe, gdy oprogramowanie serwera aplikacji zawiera błędy logiczne, które mogą być wykorzystane przez włamywacza do wysyłania łańcuchów danych o rozmiarach przekraczających bufor wejściowy. Można w ten sposób uzyskiwać uprawnienia do zasobów serwera i wykonywać własne programy na serwerze. Wyszukiwanie hostów podatnych na tego typu ataki odbywa się zwykle metodą skanowania portów, która umożliwia znalezienie słabych punktów (luk) w zabezpieczeniach systemu operacyjnego.

Wirusy, robaki i konie trojańskie[6]. O ile przepełnienie bufora może powodować szkody w odniesieniu do połączeń z Internetem, o tyle konie trojańskie i inne programy złośliwe zwykle powodują utratę zbiorów danych, wymuszając u administratorów konieczność realizacji przedsięwzięć z zakresu ochrony antywirusowej i archiwizacji danych. Wirusy są poważnym zagrożeniem, tym bardziej, że coraz trudniej je wykryć, a ich procedury niszczące mogą wahać się od wyświetlenia jakiegoś napisu na ekranie połączonego z zawieszeniem komputera, odegraniem melodyjki, ponownego startu systemu, zamiany miejscami fragmentów przypadkowego pliku, aż do zamazania wybranych sektorów na dysku i sformatowania dysku twardego.

Koń trojański jest wirusem komputerowym, choć zasada jego działania znacznie odbiega od działania tradycyjnego wirusa. Koń trojański nie powiela i nie rozprzestrzenia się samodzielnie. Komputer – ofiara infekowana jest tylko poprzez umyślne zainstalowanie przez użytkownika programu – nosiciela. Nosicielem tym może być jakikolwiek program instalowany na komputerze. Podczas instalacji, koń trojański, który wkomponowany jest w kod programu, instaluje się w tle, a więc nie jest widoczny dla użytkownika. Bardzo często wirusy te rozsyłane są za pomocą poczty elektronicznej w formie zainfekowanych animacji lub zdjęć, choć najbardziej chyba przewrotnym typem koni trojańskich są programy podające się za narzędzia antywirusowe. Cele ataków konia trojańskiego mogą być różne. Głównie jest to przejęcie kontroli nad zainfekowanym komputerem lub zdobycie przechowywanych na nim informacji. Najbardziej znanym koniem trojańskim był program stworzony przez hakerów z grupy Cult of the Dead Cow pod nazwą Back Orifice 2000. Pakiet ten służył do administracji komputerów wyposażonych w systemy Windows. W rzeczywistości jednak wszystkie zdobyte informacje o sieci były przesyłane bezpośrednio do hakerów. Wirus ten jest dość trudny do wykrycia, gdyż działa bez widocznych z zewnątrz przejawów aktywności, tzn. nie jest wyświetlany na liście menadżera zadań[7].

Fałszowanie adresu IP ***(IP Address Spoofing)***[8]. Technika ta polega na podszywaniu się osoby nieuprawnionej pod zaufane adresy IP w celu przejścia przez system ochrony, opierający się wyłącznie na adresach IP. Większość ścian ogniowych wykrywa i zapobiega przekazywaniu pakietów z fałszywym adresem zwrotnym.

Łatwe hasła[9]. Programy do łamania haseł są zdolne do wypróbowania tysięcy kombinacji haseł w ciągu minuty i mogą wykorzystać fakt niewłaściwie wybranego hasła w celu przejęcia konta użytkownika lub, w gorszym przypadku, administratora. Aby się przed tym zabezpieczyć, stosuje się politykę wymuszania zmian haseł i stosowanie haseł „trudnych" (tzn. w postaci fraz, a nie pojedynczych wyrazów, z wykorzystaniem znaków specjalnych). Hasła stosuje się też dla ruterów, przełączników i innego wyposażenia infrastruktury sieciowej.

Uprowadzenie sesji ***(Session Hijacking)***[10]. Odgadując numer sekwencyjny IP, włamywacz przejmuje istniejące połączenie między dwoma komputerami i gra rolę jednej strony takiego połączenia. Legalny użytkownik zostaje rozłączony, a włamywacz „dziedziczy" możliwość dostępu do

[5] *Vademecum teleinformatyka II,* Praca zbiorowa, wydanie specjalne Networld, Wyd. IDG Poland SA, Warszawa 2002.
[6] Stallings W.: Ochrona danych w sieci i intersieci, Wyd. Naukowo-Techniczne, Warszawa 1997.
[7] http://bezpieczna-siec.com/ataki2-opisy.htm
[8] Vademecum teleinformatyka II, Praca zbiorowa, wydanie specjalne Networld, Wyd. IDG Poland SA, Warszawa 2002.
[9] Ibidem
[10] *Vademecum teleinformatyka II*, Praca zbiorowa, wydanie specjalne Networld, Wyd. IDG Poland SA, Warszawa 2002.

danych w aktualnej sesji. Możliwość taką stwarza niewłaściwa implementacja randomizacji numerów sekwencyjnych w stosie protokołów TCP/IP systemu operacyjnego. **Namierzanie sieci *(Network Snooping)* lub podsłuch sieciowy *(Network Sniffing)***[11]. Włamywacz może użyć analizatora protokołów lub innych narzędzi do odczytywania ruchu sieciowego i uzyskiwania w ten sposób istotnych danych. Działanie takie może być przygotowaniem do przeprowadzenia innych rodzajów ataków – np. uprowadzenie sesji lub przechwycenie nazw użytkowników i haseł przesyłanych tekstem jawnym z tradycyjnych aplikacji, takich jak telnet.

Technika podsłuchu sieciowego została stworzona na potrzeby administratorów i polega ona na „podsłuchiwaniu" wszystkich pakietów krążących po sieci komputerowej. Analiza takich pakietów pozwalała na łatwe wychwycenie jakichkolwiek nieprawidłowości w funkcjonowaniu sieci. Dzięki monitorowaniu pracy sieci, administrator widzi jej słabe i mocne punkty, np. źle skonfigurowany przełącznik czy miejsca szczególnie obciążone. Sniffing jako narzędzie administracyjne stwarzało ogromne możliwości diagnostyczne. Zalety Sniffingu zostały również zauważone przez hakerów. Możliwość przechwycenia wszystkich informacji wymienianych poprzez sieć stanowiło dla nich olbrzymią zachętę. Do analizy „śledzonych" pakietów stworzyli oni własne oprogramowanie, które umożliwia wychwycenie ważnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe. Zagrożenie wynikające z możliwości „podsłuchiwania" sieci jest tak duże, iż wręcz niezbędnym jest zabezpieczenie systemu przed tego typem ataku, gdyż wypływ tajnych informacji z firmy może być dla niej bardzo groźny.

Back Door – Tylne drzwi[12]. Jest to pozostawiona przez projektantów oprogramowania ukryta możliwość wniknięcia do systemu użytkownika bez posiadania uprawnień do tego typu ingerencji. Istnienie tylnych drzwi stanowi „furtkę" dla obsługi technicznej danego systemu, np. w sytuacji, gdy administrator zagubi lub po prostu zapomni hasła. Dane potrzebne do takiego „zalogowania" się są ściśle tajne i znane tylko kilku osobom mającym do tego uprawnienia. Problem pojawia się w momencie, gdy haker uzyska dostęp do tych informacji. Dzięki nim może wtargnąć do systemu użytkownika i uzyskać dostęp, np. do danych składowanych na twardym dysku. Jedną z najgłośniejszych spraw tego typu było odkrycie tylnych drzwi w oprogramowaniu firmy X, służącym do korzystania z Microsoft Network. Pozwalały one na dostęp do wszystkich danych składowanych na lokalnych dyskach twardych użytkowników. Informacje zdobyte w ten sposób miały później służyć do identyfikacji

[11] (http://bezpieczna-siec.com/ataki2-opisy.htm)
[12] http://bezpieczna-siec.com/ataki2-opisy.htm)

osób, które posiadały nielegalne kopie programów Microsoft.

Port Scanning – skanowanie portów[13]. Za pomocą tej techniki można zorientować się, jakie są aktualnie używane i udostępnione porty komunikacyjne na serwerze ofiary. Jako że każda usługa ma ściśle przypisany port – w prosty sposób można dowiedzieć się, czy na wybranym serwerze działa serwer FTP, serwer pocztowy, czy WWW. W znacznym stopniu ułatwia to hakerowi zaplanowanie ataku. Istnieje kilka odmian skanowania portów, różniących się efektywnością, trudnością wykrycia czy rodzajem skanowanych portów. Ponieważ skanowanie portów jest także popularne jako narzędzie diagnostyczne stosowane przez administratorów, nie jest ono w żaden sposób zakazane.

DoS – Denial of Service – Odmowa usługi[14]. Atak typu DoS – Denial of Service jest jednym ze skuteczniejszych sposobów unieruchomienia serwera sieciowego. Głównym celem takiego ataku jest częściowe zablokowanie dostępu do wybranych usług, np. www czy e-mail lub całkowite unieruchomienie serwera. W skrajnych przypadkach dochodzi nawet do zupełnego zawieszenia pracy systemu – co wymaga podniesienia takiego systemu poprzez fizyczną interwencję administratora, czyli RESET. Atak ten polega na wysyłaniu w krótkim czasie bardzo dużej ilości zapytań do serwera sieciowego. Serwer na każde zapytanie stara się odpowiedzieć, haker natomiast nie czekając na odpowiedz ze strony serwera, ciągle wysyła kolejne zapytania. Doprowadza to do sytuacji, w której serwer jest wręcz „zalany" zapytaniami i nie nadąża z odpowiedziami. Wzrasta obciążenie systemu i kiedy ilość zapytań przekroczy możliwości obliczeniowe serwera, następuje jego blokada.

Typowe przykłady ataków DoS. Współczesne środowiska biznesowe praktycznie nie mogą funkcjonować w sposób efektywny bez ośrodka webowego – technika ta staje się podstawową formą komunikacji z klientami i partnerami handlowymi firm w ramach tzw. e-biznesu. Problemem każdego publicznego ośrodka webowego jest umiejętność zachęcenia użytkowników do jego odwiedzania, a jednocześnie zapewnienie wysokiego poziomu ochrony danych, aplikacji webowych i serwerów.

Do penetrowania ośrodków webowych używane są różne techniki, które można sklasyfikować w trzech grupach ataków[15]:

- na serwery webowe
- na aplikacje webowe
- ataki pośrednie.

Ataki na serwery webowe wykorzystują zlecenia protokołu HTTP wysyłane do serwera webowego. Ściany ogniowe, przechwytujące ruch, zazwyczaj koncentrują się na analizie parametrów komunikacyjnych tego ruchu (adresy IP źródła i przeznaczenia, port przeznaczenia), nie weryfikując pola danych pakietów. Zlecenia pozornie legalne są dostarczane do serwera webowego i normalnie obsługiwane. Włamywacze wykorzystują ten fakt do uruchomienia własnego kodu na serwerze, uzyskania uprzywilejowanych uprawnień dostępu (np. założenie nowego użytkownika z uprawnieniami administratora) i w konsekwencji przejęcia kontroli nad maszyną.

Ataki na aplikacje webowe obejmują kategorie:

- DoS – blokowanie usług
- zmiana zawartości stron webowych
- przechwytywanie istotnych informacji korporacyjnych lub o użytkownikach (np. numery kart kredytowych).

Źródłem słabych punktów w aplikacjach webowych są najczęściej błędy projektowe. Błędnie zaprojektowane skrypty CGI mogą być wykorzystane do wykonywania szkodliwych akcji. Powszechnym problemem aplikacji webowych jest słaba kontrola wprowadzanych danych.

Ataki pośrednie wykorzystują oprócz popularnego portu 80 (HTTP) inne drogi włamania do serwera webowego. Może to być, np. port 21 (FTP) – niektóre serwery FTP zawierają luki, które mogą być wykorzystane przez atakującego do przechwycenia poufnych danych lub uzyskania uprawnień administratora. Innym zazwyczaj otwartym portem jest port przypisany systemowi nazw domenowych DNS. Włamanie do serwera DNS umożliwia zmiany w tablicach trasowania pakietów, czego efektem może być, np. przekierowywanie ważnych informacji poczty elektronicznej na maszynę atakującego.

Podsumowanie

Zagrożenia logistycznych systemów informatycznych nasuwają wnioski:

1. bezpieczeństwo systemów informatycznych wymaga myślenia i działania prewencyjnego
2. każde naruszenie bezpieczeństwa może być przyczyną wielu problemów, np. finansowych, dystrybucji, zaopatrzenia itp.
3. ochronie podlega zarówno poufność, jak i autentyczność danych
4. jednolite zasady tworzenia bezpieczeństwa sieci komputerowych są trudne do określenia (każdą sieć należy rozpatrywać indywidualnie)
5. personel mający dostęp do systemów informatycznych powinien być wykształcony a ponadto sprawdzony i wiarygodny.

[13] http://bezpieczna-siec.com/ataki2-opisy.htm)
[14] Vademecum teleinformatyka II, Praca zbiorowa, wydanie specjalne Networld, Wyd. IDG Poland SA, Warszawa 2002.
[15] Ochrona informacji w sieci przedsiębiorstwa, Dodatek specjalny Networld, nr 5/2003.