System i

Bezpieczeństwo
Serwery System i - bezpieczeństwo internetowe

Wersja 6 wydanie 1

System i

Bezpieczeństwo
Serwery System i - bezpieczeństwo internetowe

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 29.

To wydanie dotyczy systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) wersja 6, wydanie 1, modyfikacja 0, a także wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Serwery System i - bezpieczeństwo internetowe

Dostęp do Internetu z sieci LAN wymaga ponownej analizy wymagań w zakresie bezpieczeństwa.

Zintegrowane rozwiązania programowe oraz architektura bezpieczeństwa platformy IBM System i pozwalają stworzyć mocną linię obrony przed potencjalnymi zagrożeniami ze strony Internetu oraz intruzami. Wykorzystanie tych elementów bezpieczeństwa gwarantuje klientom, pracownikom i partnerom handlowym dostęp do niezbędnych informacji w bezpiecznym środowisku.

W niniejszej kolekcji tematów opisano znane zagrożenia oraz ich wpływ na cele związane z Internetem i e-biznesem. Przedstawione zostały także kryteria porównywania ryzyka z korzyściami płynącymi ze stosowania różnych zabezpieczeń dostępnych w systemie. Zawarto tu również praktyczne wskazówki dotyczące wdrożenia planu bezpieczeństwa sieci, który będzie dopasowany do konkretnej sytuacji.

Plik PDF z informacjami na temat platformy System i oraz bezpieczeństwa internetowego

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby wyświetlić lub pobrać wersję PDF tego dokumentu, kliknij odsyłacz Serwery System i - bezpieczeństwo internetowe (około 456 KB).

Można przeglądać lub pobrać następujące tematy pokrewne:

- Wykrywanie włamań (około 285 KB). Użytkownik może utworzyć strategię wykrywania włamań, w ramach której nadzorowane są podejrzane zdarzenia w sieci TCP/IP, na przykład niepoprawnie utworzone pakiety IP. Można również utworzyć aplikację analizującą dane kontrolne i powiadamiającą administratora ochrony o potencjalnych włamaniach w sieci TCP/IP.
- Odwzorowanie tożsamości w przedsiębiorstwie (EIM) (około 1954 KB). EIM jest mechanizmem odwzorowywania osoby lub jednostki (na przykład usługi) do odpowiednich tożsamości użytkownika w różnych rejestrach użytkowników w przedsiębiorstwie.
- Pojedyncze logowanie (około 1203 KB). Procedura pojedynczego logowania zmniejsza liczbę logowań, które użytkownik musi wykonać, jak też liczbę haseł, za pomocą których użytkownik uzyskuje dostęp do wielu aplikacji i systemów.
- Planowanie i konfigurowanie bezpieczeństwa systemu (około 3992 KB). Temat o planowaniu i konfigurowaniu bezpieczeństwa systemu zawiera informacje dotyczące efektywnego i systematycznego planowania oraz konfigurowania elementów bezpieczeństwa na poziomie systemu.

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Pojęcia pokrewne

Wykrywanie włamań

Odwzorowywanie tożsamości dla przedsiębiorstwa (Enterprise Identity Mapping - EIM)

Pojedyncze logowanie

Planowanie i konfigurowanie bezpieczeństwa systemu

Uwagi dotyczące platformy System i oraz bezpieczeństwa internetowego

Zagadnienia bezpieczeństwa internetowego są bardzo ważne. Ten temat zawiera przegląd zabezpieczeń systemu i5/OS i jego mocnych stron w tym zakresie.

Po podłączeniu platformy System i do Internetu zazwyczaj należy zadać sobie pytanie jaka wiedza o bezpieczeństwie i Internecie jest potrzebna. Poniżej znajdują się wszystkie niezbędne informacje na ten temat.

Potrzebna wiedza zależy od sposobu, w jaki ma być wykorzystywany Internet. Pierwszym kontaktem z Internetem jest zapewnienie użytkownikom sieci wewnętrznej dostępu do stron WWW i internetowej poczty elektronicznej. Może być również potrzebne przesyłanie ważnych informacji z jednego ośrodka do innego. Internet można też wykorzystać do handlu elektronicznego lub do utworzenia sieci ekstranet pomiędzy firmą a jej partnerami handlowymi i dostawcami.

Przed rozpoczęciem korzystania z Internetu należy zdecydować, do czego Internet będzie służył i w jaki sposób będzie się go użytkować. Podjęcie decyzji dotyczących używania Internetu i bezpieczeństwa internetowego może być złożonym procesem.

Uwaga: Uwaga: użytkownicy nie znający terminów związanych z bezpieczeństwem i Internetem mogą w trakcie czytania tej dokumentacji korzystać ze wspólnej terminologii dotyczącej bezpieczeństwa.

Do opracowania własnych celów i strategii bezpieczeństwa konieczne jest ustalenie metod korzystania z Internetu i prowadzenia e-biznesu, zrozumienie zagadnień związanych z bezpieczeństwem, a także poznanie dostępnych narzędzi, ich funkcji i możliwości ochrony. Na decyzje dotyczące strategii bezpieczeństwa wpływa wiele czynników. Po rozszerzeniu obszaru zainteresowania organizacji na Internet strategia bezpieczeństwa staje się fundamentem należytego zabezpieczenia posiadanych systemów i zasobów.

Funkcje związane z bezpieczeństwem w systemie i5/OS

Niezależnie od funkcji specjalnie przeznaczonych do ochrony systemu od strony Internetu, architektura bezpieczeństwa w systemie operacyjnym i5/OS charakteryzuje się następującymi elementami:

- Zintegrowane zabezpieczenia, bardzo trudne do obejścia w porównaniu z zabezpieczeniami innych systemów, opartych na dodatkowych pakietach oprogramowania.
- Oparta na obiektach architektura powoduje, że tworzenie i rozprzestrzenianie się wirusów jest trudne technicznie. W systemie operacyjnym i5/OS plik nie może udawać programu, a jeden program nie może zmieniać drugiego. Funkcje zapewniania integralności systemu i5/OS wymagają używania dostarczonych z systemem interfejsów, aby uzyskać dostęp do obiektów. Nie można uzyskiwać dostępu do obiektów bezpośrednio za pomocą ich adresu w systemie. Nie można pobrać offsetu (przesunięcia) i zamienić go we wskaźnik ani samodzielnie utworzyć wskaźnika. Manipulacja wskaźnikami jest popularną techniką używaną przez hakerów w innych systemach.
- Elastyczność pozwala ustawić zabezpieczenia systemu w sposób zgodny ze specyficznymi wymaganiami. Można skorzystać z programu Security Planner, który pomaga dobrać parametry bezpieczeństwa najbardziej dopasowane do potrzeb.

Zaawansowane funkcje bezpieczeństwa w systemie i5/OS

System operacyjny i5/OS zawiera także kilka specjalnych zabezpieczeń mających na celu rozszerzenie ochrony systemu, gdy jest on podłączony do Internetu. W zależności od sposobu używania Internetu można korzystać z jednego z wymienionych poniżej rozwiązań.

- Sieci VPN (Virtual Private Network) są rozszerzeniem prywatnej sieci intranet firmy na sieć publiczną, na przykład na Internet. Sieci VPN można używać do ustanawiania chronionych połączeń prywatnych, polegających na tworzeniu prywatnego tunelu w sieci publicznej. Możliwość tworzenia sieci VPN to zintegrowana funkcja systemu operacyjnego i5/OS, dostępna za pośrednictwem interfejsu programu System i Navigator.
- Reguły pakietów to zintegrowana funkcja systemu operacyjnego i5/OS, dostępna za pośrednictwem interfejsu programu System i Navigator. Przy użyciu tych reguł można skonfigurować filtr pakietów IP i reguły translacji adresów sieciowych (NAT) w celu sterowania przepływem przychodzących i wychodzących pakietów TCP/IP.
- Obsługa protokołów Secure Sockets Layer (SSL) umożliwia skonfigurowanie aplikacji do korzystania z SSL w celu ustanawiania chronionych połączeń pomiędzy aplikacjami serwera i ich klientami. Protokół SSL pierwotnie był przeznaczony do zabezpieczania przeglądarek WWW i aplikacji serwera, ale mogą go wykorzystywać także inne aplikacje. Wiele aplikacji umożliwia obecnie korzystanie z SSL, między innymi IBM HTTP Server for i5/OS, System i Access for Windows, protokół File Transfer Protocol (FTP), Telnet i inne.

  Pojęcia pokrewne

  “Cele i strategie bezpieczeństwa” na stronie 6
  Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

  “Bezpieczna prywatna komunikacja za pośrednictwem sieci VPN” na stronie 26
  Sieć VPN (Virtual Private Network), czyli rozszerzenie intranetu przedsiębiorstwa w ramach istniejącej sieci publicznej lub prywatnej, może pomóc zapewnić prywatność i bezpieczeństwo komunikacji wewnątrz organizacji.

  “Scenariusz: plany dotyczące e-biznesu firmy JKL Toy Company” na stronie 8
  Typowy scenariusz opisany na przykładzie firmy JKL Toy Company, która zdecydowała się na rozszerzenie swojej działalności biznesowej na Internet, może być pomocny przy przygotowywaniu własnych planów dotyczących e-biznesu.

  Informacje pokrewne

  Łączenie z Internetem

  Narzędzie eServer Security Planner

  Filtrowanie IP i translacja adresów sieciowych

  Protokół Secure Sockets Layer

  AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet

Planowanie bezpieczeństwa internetowego

Podczas opracowywania planów użytkowania Internetu należy wziąć pod uwagę potrzeby związane z bezpieczeństwem.

Należy zgromadzić szczegółowe informacje na temat planowanego sposobu korzystania z Internetu oraz udokumentować konfigurację sieci wewnętrznej. W oparciu o tak zebrane informacje można precyzyjnie określić istniejące potrzeby w zakresie bezpieczeństwa sieci.

Podczas sporządzania dokumentacji nie można na przykład pominąć:
- aktualnej konfiguracji sieci,
- informacji dotyczących konfiguracji serwerów DNS i poczty elektronicznej,
- połączenia z dostawcą usług internetowych,
- usług, jakie będą używane za pośrednictwem Internetu,
- usług, jakie będą oferowane użytkownikom Internetu.

Udokumentowane informacje tego typu są pomocne przy określaniu części systemu podatnych na atak i zabezpieczeń, które są niezbędne do zminimalizowania tych zagrożeń.

Załóżmy, że podjęto decyzję, iż użytkownicy sieci wewnętrznej mogą korzystać z usługi Telnet podczas łączenia się z hostami w ośrodku badawczym. Użytkownicy wewnętrzni potrzebują tej usługi, aby opracowywać nowe produkty dla

firmy. Pojawia się jednak problem poufnych danych płynących przez sieć Internet bez żadnej ochrony. Jeśli konkurencja przechwyci i wykorzysta dane, to firma może stanąć w obliczu zagrożenia finansowego. Po określeniu potrzeb (Telnet) i związanych z nimi niebezpieczeństw (ujawnienie poufnych danych) możliwe jest określenie, jakie dodatkowe zabezpieczenia należy wdrożyć, aby zapewnić poufność danych (na przykład SSL).

Bezpieczeństwo poprzez obronę warstwową

Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

Strategia bezpieczeństwa to podstawa niezbędna do planowania zabezpieczeń podczas projektowania nowych aplikacji lub rozszerzania posiadanej sieci. Opisuje zakres odpowiedzialności użytkownika, na przykład za ochronę poufnych informacji lub tworzenie haseł, które nie są łatwe do odgadnięcia.

Uwaga: Należy opracować i wprowadzić taką strategię bezpieczeństwa organizacji, która minimalizuje zagrożenia dla sieci wewnętrznej. Poprawnie skonfigurowane wbudowane opcje zabezpieczające systemu operacyjnego i5/OS pozwalają uniknąć wielu czynników ryzyka. Połączenie systemu z Internetem wymaga jednak wprowadzenia dodatkowych środków bezpieczeństwa w celu właściwego zabezpieczenia sieci wewnętrznej.

Prowadzenie działalności gospodarczej poprzez Internet niesie ze sobą wiele zagrożeń. Tworząc strategię bezpieczeństwa, należy zrównoważyć możliwość świadczenia usług i kontrolowania dostępu do funkcji i danych. W przypadku komputerów w sieci zapewnienie bezpieczeństwa jest trudniejsze, ponieważ kanał komunikacyjny jest otwarty na atak.

Niektóre usługi internetowe są szczególnie podatne na pewne typy ataków. Z tego względu sprawą kluczowej wagi jest zdanie sobie sprawy z zagrożeń związanych z każdą usługą, która będzie używana lub udostępniana. Ponadto znajomość możliwych zagrożeń pozwala na zdefiniowanie zbioru precyzyjnych celów związanych z bezpieczeństwem.

Niektórzy użytkownicy Internetu świadomie próbują zagrozić bezpieczeństwu komunikacji przez Internet. Na poniższej liście opisano kilka typowych zagrożeń:

- **Ataki pasywne**

  Podczas ataku pasywnego intruz ogranicza się do obserwacji ruchu w sieci, usiłując zdobyć poufne informacje. Takie ataki mogą następować w sieci (śledzenie łącza komunikacyjnego) lub w systemie (zastąpienie komponentu systemowego koniem trojańskim, który podstępnie przechwytuje dane). Bardzo trudno wykryć ataki pasywne. Dlatego też należy założyć, że wszystkie dane przesyłane przez Internet są przez kogoś przechwytywane.
- **Ataki aktywne**

  Podczas ataku aktywnego intruz usiłuje złamać zabezpieczenia systemu i dostać się do systemów w sieci. Istnieje kilka rodzajów ataków aktywnych:
  - **Próby dostępu do systemu** - napastnik usiłuje wykorzystać luki w zabezpieczeniach, aby uzyskać dostęp do systemu klienckiego lub serwera i przejąć nad nim kontrolę.
  - **Oszukiwanie** - napastnik próbuje przedostać się przez zabezpieczenia, podszywając się pod użytkownika lub system zaufany, a później skłonić system do przesłania mu tajnych informacji.
  - **Odmowa usługi** - napastnik próbuje zakłócić lub zakończyć działanie systemu zmieniając kierunek przepływu danych w sieci lub bombardując system śmieciami.
  - **Atak kryptograficzny** - napastnik próbuje zgadnąć lub wykraść hasło albo próbuje deszyfrować zaszyfrowane dane za pomocą specjalizowanych narzędzi.

Obrona wielowarstwowa

Potencjalne zagrożenia w Internecie mogą wystąpić na różnych poziomach, dlatego niezbędne jest zastosowanie wielu warstw obrony. Ogólnie rzecz ujmując, przy łączeniu z Internetem nie należy się zastanawiać, czy wystąpią próby włamania do systemu lub ataki typu odmowa usługi. Należy z góry założyć, że problemy tego typu na pewno wystąpią. Najlepszą obroną jest zatem przemyślany, uprzedzający zagrożenia atak. Skorzystanie z podejścia warstwowego podczas planowania strategii bezpieczeństwa internetowego gwarantuje, że intruz, który przedrze się przez pierwszą warstwę obrony, zostanie zatrzymany przez następną warstwę.

Strategia bezpieczeństwa musi zawierać środki ochrony w poszczególnych warstwach tradycyjnego modelu przetwarzania sieciowego. Podsumowując, zabezpieczenia należy planować od najprostszych (bezpieczeństwo na poziomie systemu) do najbardziej złożonych (bezpieczeństwo na poziomie transakcji).

Bezpieczeństwo na poziomie systemu
Zabezpieczenia systemu to ostatnia linia obrony przed próbami dostępu do systemu poprzez Internet. Dlatego też pierwszym punktem kompleksowej strategii bezpieczeństwa internetowego musi być prawidłowe skonfigurowanie podstawowych zabezpieczeń systemu.

Bezpieczeństwo na poziomie sieci
Zabezpieczenia sieci kontrolują dostęp do systemu operacyjnego i5/OS i do innych systemów w sieci. Gdy sieć zostaje podłączona do Internetu, należy upewnić się, że stosowany jest odpowiedni poziom zabezpieczeń sieci, który pozwoli ochronić zasoby wewnętrznej sieci przed dostępem bez uprawnień i wtargnięciem. Najczęściej stosowane jest rozwiązanie oparte na zaporze firewall. Dostawca usług internetowych może stanowić ważny element w planie zabezpieczenia sieci. Schemat bezpieczeństwa sieciowego powinien informować, jakie zabezpieczenia są dostarczane przez dostawcę usług internetowych. Mogą to być na przykład reguły filtrowania dla połączeń z routerem dostawcy usług internetowych i środki ostrożności dotyczące publicznej usługi DNS.

Bezpieczeństwo na poziomie aplikacji
Zabezpieczenia na poziomie aplikacji sterują interakcją użytkownika z określonymi aplikacjami. Należy skonfigurować zabezpieczenia dla każdej używanej aplikacji. Szczególny nacisk należy położyć na zabezpieczanie tych aplikacji, które będą używane lub dostarczane za pośrednictwem Internetu. Takie aplikacje i usługi są narażone na nieprawidłowe użycie przez nieuprawnionych użytkowników szukających dostępu do systemów sieciowych. Wybrane zabezpieczenia powinny chronić przed ryzykiem naruszenia bezpieczeństwa zarówno po stronie klientów, jak i serwerów.

Bezpieczeństwo na poziomie transmisji
Zabezpieczenia na poziomie transmisji chronią przesyłanie danych przez sieć i między sieciami. Podczas komunikacji przez niezaufaną sieć, taką jak Internet, nie ma możliwości sprawdzenia przepływu pakietów od nadawcy do odbiorcy. Pakiety oraz przenoszone przez nie dane przepływają przez wiele różnych systemów, nad którymi nie ma kontroli. Jeśli nie zostaną ustawione zabezpieczenia, takie jak na przykład korzystanie przez aplikacje z protokołu SSL, przepływające dane będą dostępne dla każdego, każdy będzie mógł je przejrzeć i wykorzystać. Zabezpieczenia na poziomie transmisji chronią dane przepływające pomiędzy granicami obszarów o różnych poziomach bezpieczeństwa.

Tworząc ogólną strategię bezpieczeństwa w Internecie należy utworzyć osobne reguły dla każdej warstwy. Ponadto należy opisać sposób, w jaki każdy zestaw reguł współpracuje z innymi przy zapewnianiu bezpieczeństwa sieci na potrzeby firmy.

Pojęcia pokrewne

“Poziomy bezpieczeństwa dla podstawowego zakresu gotowości internetowej” na stronie 10
Przed podłączeniem do Internetu należy określić, jaki poziom bezpieczeństwa jest niezbędny do ochrony systemu.

“Bezpieczeństwo na poziomie sieci” na stronie 11
Aby ochronić zasoby wewnętrzne, należy wybrać odpowiednie mechanizmy bezpieczeństwa na poziomie sieci.

“Bezpieczeństwo na poziomie aplikacji” na stronie 16
W przypadku wielu popularnych aplikacji i usług internetowych ryzykiem dotyczącym bezpieczeństwa można zarządzać na kilka sposobów.

“Opcje zabezpieczania transmisji” na stronie 22
Aby zabezpieczyć dane przepływające przez niezaufaną sieć, na przykład Internet, należy wdrożyć odpowiednie środki bezpieczeństwa. Środki te obejmują protokół Secure Sockets Layer (SSL), oprogramowanie System i Access for Windows oraz połączenia przez sieci VPN (Virtual Private Network).

“Cele i strategie bezpieczeństwa” na stronie 6
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

“Bezpieczeństwo poczty elektronicznej” na stronie 19
Korzystanie z poczty elektronicznej w sieci Internet lub innej sieci niezaufanej powoduje zagrożenia systemu, przed którymi nie chroni zapora firewall.

Odsyłacze pokrewne

 System i Security Guide for IBM i5/OS Version 5 Release 4

Cele i strategie bezpieczeństwa

Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

Strategia bezpieczeństwa

Użycie bądź udostępnienie dowolnej usługi internetowej stwarza zagrożenie bezpieczeństwa systemu i sieci, do której jest on podłączony. Strategia bezpieczeństwa to zestaw reguł dotyczących czynności związanych z zasobami komunikacyjnymi i komputerowymi należącymi do jednej organizacji. Reguły te obejmują takie zagadnienia, jak ochrona fizyczna, ochrona personelu, ochrona administracyjna i bezpieczeństwo sieci.

Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu. Stanowi podstawę niezbędną do planowania zabezpieczeń podczas projektowania nowych aplikacji lub rozszerzania posiadanej sieci. Opisuje zakres odpowiedzialności użytkownika, na przykład za ochronę poufnych informacji lub tworzenie haseł, które nie są łatwe do odgadnięcia. Strategia bezpieczeństwa powinna też określać sposób monitorowania skuteczności podjętych zabiegów. Stałe monitorowanie tego typu pozwala wykrywać na bieżąco podejmowane próby obejścia zastosowanych zabezpieczeń.

Aby opracować własną strategię bezpieczeństwa, należy precyzyjnie zdefiniować cele związane z bezpieczeństwem. Po utworzeniu strategii bezpieczeństwa należy podjąć kroki w celu wdrożenia reguł w niej zawartych. Działania te obejmują szkolenie pracowników oraz instalację sprzętu i oprogramowania niezbędnego do wdrożenia tych reguł. Ponadto, gdy wprowadzane są zmiany w środowisku przetwarzania, należy aktualizować strategię bezpieczeństwa, aby zapewnić identyfikację i neutralizację zagrożeń związanych z wprowadzonymi zmianami.

Strategia bezpieczeństwa

Podczas tworzenia i wdrażania strategii bezpieczeństwa należy precyzyjnie określić jej cele. Cele związane z bezpieczeństwem należą do jednej lub kilku wymienionych kategorii:

Ochrona zasobów
: Zapewnia dostęp do zasobów systemu tylko uprawnionym użytkownikom. Mocną stroną platformy System i jest możliwość zabezpieczenia wszystkich typów zasobów systemowych. Należy dokładnie zdefiniować kategorie użytkowników mających dostęp do systemu. W ramach tworzenia strategii bezpieczeństwa należy także zdefiniować uprawnienia dostępu, jakie będą miały grupy użytkowników.

Uwierzytelnianie
: Sprawdzenie, czy zasób (człowiek lub komputer) znajdujący się po drugiej stronie sesji rzeczywiście jest tym, za co lub kogo się podaje. Niezawodne uwierzytelnianie chroni system przed użytkownikami, którzy - używając fałszywych danych identyfikacyjnych - usiłują uzyskać dostęp do systemu. Do uwierzytelniania systemy zwykle wykorzystują nazwy i hasła użytkowników; bezpieczniejszą metodą są certyfikaty cyfrowe, które ponadto przynoszą inne korzyści w zakresie bezpieczeństwa. Po podłączeniu systemu do sieci publicznej, takiej jak Internet, uwierzytelnianie użytkowników uzyskuje nowy wymiar. Istotną różnicą pomiędzy siecią Internet i intranet jest to, że można mieć zaufanie do podanej tożsamości użytkownika wpisującego się do systemu. Dlatego też należy wziąć pod uwagę używanie lepszych metod uwierzytelniania, niż tradycyjne sprawdzanie nazwy użytkownika i hasła podczas logowania. Uwierzytelnieni użytkownicy mogą mieć różne typy uprawnień, w zależności od nadanych im poziomów uprawnień.

Nadawanie uprawnień
: Pewność, że osoba lub komputer znajdujący się po drugiej stronie sesji ma uprawnienia do wykonania żądania. Nadawanie uprawnień to proces określania, kto lub co może uzyskać dostęp do zasobu systemu lub wykonać w systemie określoną czynność. Zazwyczaj nadawanie uprawnień jest częścią uwierzytelniania.

Integralność

Pewność, że napływające informacje są identyczne z wysłanymi. Zrozumienie integralności wymaga zrozumienia koncepcji integralności danych i integralności systemu.

- **Integralność danych**: Dane są zabezpieczone przed nieuprawnionymi zmianami lub manipulacjami. Integralność danych chroni przed niebezpieczeństwem manipulacji, polegającym na nieuprawnionym przechwytywaniu i zmienianiu informacji. Oprócz ochrony danych przechowywanych w sieci mogą być potrzebne dodatkowe zabezpieczenia w celu zapewnienia integralności podczas wprowadzania danych do systemu z niezaufanego źródła. Jeśli napływające do systemu dane pochodzą z sieci publicznej, potrzebne są zabezpieczenia, które pozwolą:
  - chronić dane przed ich podsłuchaniem i interpretowaniem - w tym celu zwykle stosuje się szyfrowanie;
  - upewniać się, że transmisja nie została zmieniona (integralność danych);
  - udowodnić, że transmisja miała miejsce (nieodrzucanie). W przyszłości może być potrzebny elektroniczny odpowiednik listu poleconego.
- **Integralność systemu**: system dostarcza spójne, oczekiwane wyniki przy zachowaniu spodziewanej wydajności. W systemie operacyjnym i5/OS integralność systemu jest często przeoczanym elementem bezpieczeństwa, dlatego że jest podstawową częścią architektury i5/OS. Przykładowo, architektura systemu i5/OS sprawia, że przy poziomie bezpieczeństwa równym 40 lub 50 imitowanie lub modyfikowanie programu systemu operacyjnego staje się wyjątkowo trudne.

Nieodrzucanie

Dowód przeprowadzenia transakcji lub wysłania albo odebrania wiadomości. Użycie certyfikatów cyfrowych i szyfrowania z kluczem publicznym do podpisywania transakcji, komunikatów i dokumentów obsługuje nieodrzucanie. Zarówno nadawca, jak i odbiorca zgadzają się, że odbyła się wymiana. Za dowód wystarcza opatrzenie danych cyfrowym podpisem.

Poufność

Pewność, że tajne informacje pozostają prywatne i nie są widoczne dla podglądaczy. Poufność jest kluczowym elementem pełnej ochrony danych. Szyfrowanie danych za pomocą certyfikatów cyfrowych i protokołu SSL lub połączenie przez sieć VPN (Virtual Private Network) pomaga zapewnić poufność danych podczas przesyłania ich przez sieci niezaufane. Strategia bezpieczeństwa powinna określać sposób ochrony poufności informacji wewnątrz sieci lokalnej i poza nią.

Kontrolowanie działań związanych z bezpieczeństwem

Monitorowanie zdarzeń związanych z bezpieczeństwem w celu protokołowania pomyślnych i niepomyślnych (odrzuconych) prób dostępu. Zapisy pomyślnie zakończonych prób dostępu informują o wykonywanych w systemie czynnościach i zachowaniu użytkowników. Zapisy niepomyślnie zakończonych (odrzuconych) prób dostępu informują o próbach przełamania zabezpieczeń lub trudnościach z uzyskaniem dostępu do systemu.

Pojęcia pokrewne

“Uwagi dotyczące platformy System i oraz bezpieczeństwa internetowego” na stronie 2
Zagadnienia bezpieczeństwa internetowego są bardzo ważne. Ten temat zawiera przegląd zabezpieczeń systemu i5/OS i jego mocnych stron w tym zakresie.

“Bezpieczeństwo poprzez obronę warstwową” na stronie 4
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

Konfigurowanie programu DCM

Protokół SSL (Secure Socket Layer)

“Scenariusz: plany dotyczące e-biznesu firmy JKL Toy Company” na stronie 8
Typowy scenariusz opisany na przykładzie firmy JKL Toy Company, która zdecydowała się na rozszerzenie swojej działalności biznesowej na Internet, może być pomocny przy przygotowywaniu własnych planów dotyczących e-biznesu.

Scenariusz: plany dotyczące e-biznesu firmy JKL Toy Company

Typowy scenariusz opisany na przykładzie firmy JKL Toy Company, która zdecydowała się na rozszerzenie swojej działalności biznesowej na Internet, może być pomocny przy przygotowywaniu własnych planów dotyczących e-biznesu.

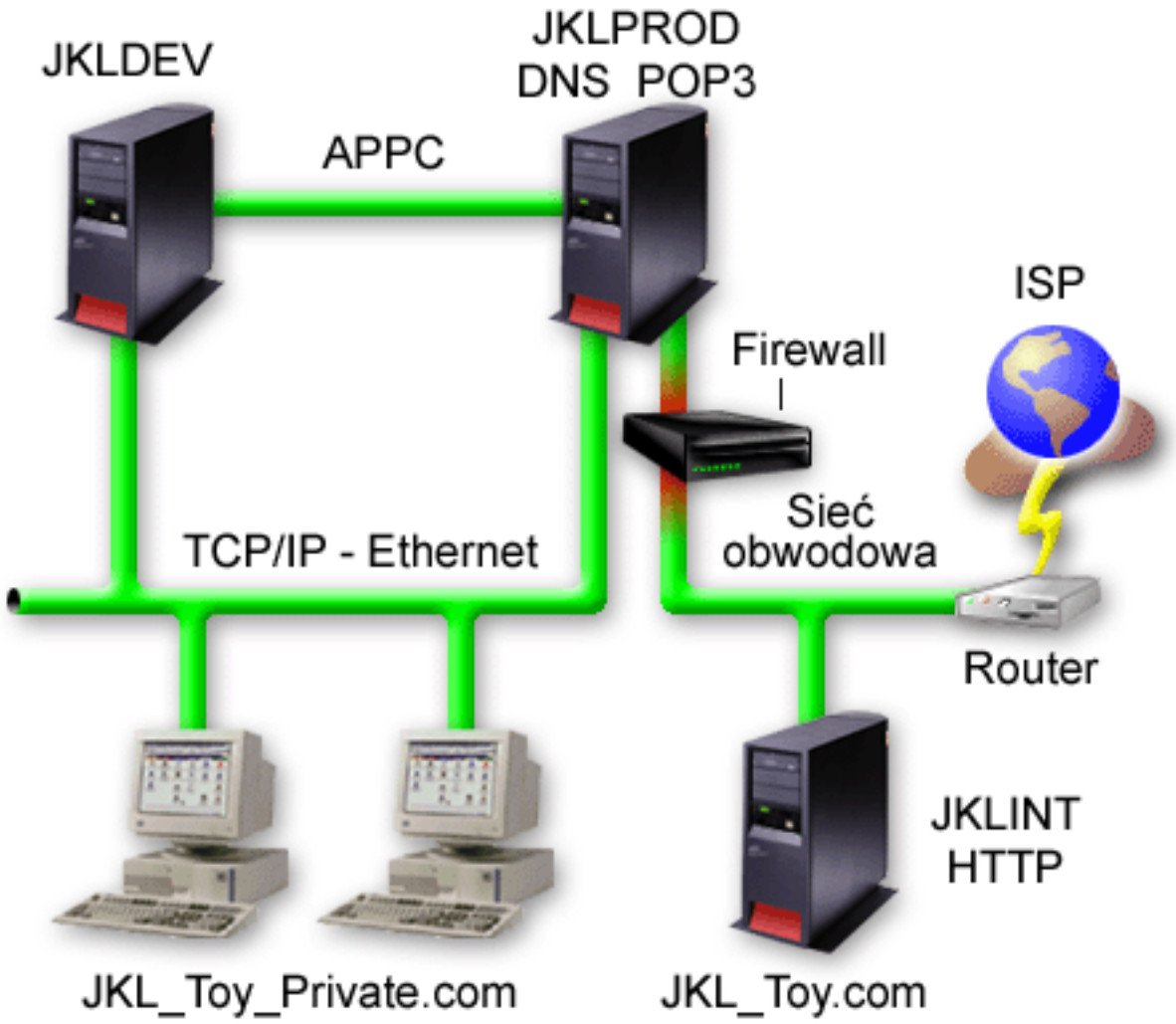
Firma JKL Toy Company jest małym, ale szybko rozwijającym się producentem zabawek. Prezes jest zadowolony z rozwoju firmy oraz z nowego systemu operacyjnego i5/OS, który pozwala nad nim zapanować. Za administrację systemu i jego bezpieczeństwo odpowiedzialna jest Anna Kowalska - kierownik działu księgowości.

Firma od lat z powodzeniem korzysta ze swojej strategii bezpieczeństwa dotyczącej wewnętrznych aplikacji. Obecnie planowane jest użycie intranetu do efektywniejszej wewnętrznej komunikacji. Ponadto firma rozważa możliwość wykorzystania Internetu dla celów biznesowych. W planach jest wykreowanie wizerunku firmy w Internecie, włącznie z utworzeniem katalogu elektronicznego oraz wykorzystanie Internetu do transmisji ważnych danych ze zdalnych miejsc do głównego biura. Ponadto firma chce zapewnić pracownikom laboratorium projektów dostęp do Internetu dla celów badawczych i projektowych. Poza tym ma zamiar umożliwić klientom korzystanie z własnego serwisu WWW do składania bezpośrednich zamówień. Anna tworzy raport o możliwych specyficznych zagrożeniach związanych z taką działalnością i o tym, jakie zabezpieczenia powinna zastosować firma, aby je zminimalizować. Jest ona odpowiedzialna za zaktualizowanie firmowej strategii bezpieczeństwa i zastosowanie w praktyce środków, których firma zdecyduje się użyć.

Cele rozszerzenia obecności w Internecie są następujące:

- promowanie ogólnego wizerunku firmy i jej obecności jako część ogólnej kampanii reklamowej,
- dostarczanie katalogu produktów online dla klientów i personelu sprzedaży,
- poprawienie obsługi klienta,
- umożliwienie pracownikom dostępu do poczty elektronicznej i sieci WWW.

Upewniwszy się, że wdrożono należycie podstawowe zabezpieczenia systemu, firma JKL Toy Company postanowiła nabyć i wdrożyć zaporę firewall, aby zapewnić ochronę na poziomie sieci. Firewall będzie chronić sieć wewnętrzną przed wieloma potencjalnymi zagrożeniami związanymi z Internetem. Na poniższym rysunku przedstawiono konfigurację sieci i Internetu w firmie.



Jak wynika z rysunku, w firmie JKL Toy Company działają dwa systemy podstawowe. Jeden z nich jest przeznaczony do obsługi aplikacji projektowych (JKLDEV), a drugi na potrzeby aplikacji produkcyjnych (JKLPROD). Oba systemy obsługują dane i aplikacje o newralgicznym znaczeniu. Dlatego też nie jest wskazane uruchamianie aplikacji internetowych na tych systemach. W celu uruchomienia tego rodzaju aplikacji podjęto decyzję o dodaniu nowego systemu (JKLINT).

Nowy system umieszczono w sieci obwodowej. Pomiędzy nim a wewnętrzną siecią firmową umieszczono firewall, aby zapewnić lepszą separację własnej sieci od Internetu. Separacja ta zmniejsza niebezpieczeństwo ze strony Internetu, na które narażone są systemy wewnętrzne. Wyznaczając nowy system tylko do roli serwera internetowego, firma zmniejsza złożoność zarządzania bezpieczeństwem sieci.

Firma nie uruchamia na nowym systemie żadnych aplikacji o newralgicznym znaczeniu. Na tym etapie planów dotyczących e-biznesu nowy system udostępnia jedynie statyczny, publicznie dostępny serwis WWW. Jednak firma chce zaimplementować środki bezpieczeństwa, aby zabezpieczyć system i publicznie dostępny serwis WWW przed przerwaniem działania czy innymi możliwymi atakami. Dlatego firma będzie zabezpieczać system zarówno za pomocą reguł filtrowania pakietów i reguł translacji adresu sieciowego, jak i podstawowych środków bezpieczeństwa.

W miarę jak firma będzie dostarczała bardziej zaawansowane aplikacje dostępne publicznie (handel elektroniczny czy dostęp do sieci ekstranet) implementowane będą bardziej zaawansowane środki bezpieczeństwa.

Pojęcia pokrewne

"Cele i strategie bezpieczeństwa" na stronie 6
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

"Uwagi dotyczące platformy System i oraz bezpieczeństwa internetowego" na stronie 2
Zagadnienia bezpieczeństwa internetowego są bardzo ważne. Ten temat zawiera przegląd zabezpieczeń systemu i5/OS i jego mocnych stron w tym zakresie.

"Bezpieczeństwo na poziomie sieci" na stronie 11
Aby ochronić zasoby wewnętrzne, należy wybrać odpowiednie mechanizmy bezpieczeństwa na poziomie sieci.

"Opcje zabezpieczania transmisji" na stronie 22
Aby zabezpieczyć dane przepływające przez niezaufaną sieć, na przykład Internet, należy wdrożyć odpowiednie środki bezpieczeństwa. Środki te obejmują protokół Secure Sockets Layer (SSL), oprogramowanie System i Access for Windows oraz połączenia przez sieci VPN (Virtual Private Network).

Poziomy bezpieczeństwa dla podstawowego zakresu gotowości internetowej

Przed podłączeniem do Internetu należy określić, jaki poziom bezpieczeństwa jest niezbędny do ochrony systemu.

Zabezpieczenia systemu to ostatnia linia obrony przed próbami dostępu do systemu poprzez Internet. Pierwszym punktem kompleksowej strategii bezpieczeństwa internetowego musi być prawidłowe skonfigurowanie podstawowych zabezpieczeń systemu i5/OS. Aby upewnić się, że system spełnia minimalne wymagania dotyczące bezpieczeństwa, należy wykonać poniższe czynności:

- Ustaw poziom bezpieczeństwa (wartość systemowa QSECURITY) na 50. Wartość 50 zapewnia najwyższy stopień bezpieczeństwa integralności danych, co jest zalecane podczas pracy w środowiskach o wysokim poziomie ryzyka, do których należy Internet.

  Uwaga: Jeśli aktualnie ustawiony jest poziom bezpieczeństwa niższy niż 50, to może wystąpić potrzeba aktualizacji procedur operacyjnych albo aplikacji. Należy skonsultować się z dokumentacją platformy System i poświęconą kwestiom bezpieczeństwa.
- Należy ustawić wartości systemowe dotyczące bezpieczeństwa na co najmniej tak restrykcyjne, jak zalecane ustawienia. W celu skonfigurowania zalecanych zabezpieczeń można skorzystać z kreatora ochrony w programie System i Navigator.
- Należy upewnić się, że żaden profil użytkownika, w tym profile użytkowników dostarczone przez IBM, nie ma hasła domyślnego. Aby to sprawdzić, należy użyć komendy Analiza domyślnych haseł (Analyze Default Passwords - ANZDFTPWD).
- Aby chronić ważne zasoby systemowe, należy korzystać z uprawnień do obiektów. Należy zastosować restrykcyjne podejście do systemu. Oznacza to, że domyślnie nikt (PUBLIC *EXCLUDE) nie powinien mieć uprawnień do zasobów systemowych, takich jak biblioteki i katalogi. Na dostęp do tych zasobów można zezwolić jedynie kilku użytkownikom. W środowisku Internetu ograniczenie dostępu za pomocą menu nie jest wystarczające.
- Koniecznie trzeba ustawić uprawnienia do obiektów w systemie.

W celu uzyskania pomocy przy konfigurowaniu minimalnych wymagań w zakresie bezpieczeństwa systemu można użyć narzędzia eServer Security Planner lub kreatora ochrony, dostępnego za pośrednictwem interfejsu programu System i Navigator. Narzędzie Security Planner generuje zestaw zaleceń dotyczących bezpieczeństwa w oparciu o odpowiedzi użytkownika na szereg zadanych pytań. Z zaleceń tych można skorzystać podczas konfigurowania zabezpieczeń systemu odpowiednio do potrzeb. W przeciwieństwie do narzędzia Security Planner, kreator może automatycznie skonfigurować zabezpieczenia.

Poprawne skonfigurowanie wbudowanych opcji zabezpieczających systemu i5/OS i zarządzanie nimi umożliwia zminimalizowanie wielu zagrożeń. Połączenie systemu z Internetem wymaga jednak wprowadzenia dodatkowych środków bezpieczeństwa w celu właściwego zabezpieczenia sieci wewnętrznej. Po upewnieniu się, że ogólny poziom bezpieczeństwa systemu jest dobry, należy skonfigurować dodatkowe zabezpieczenia, co stanowi część wszechstronnego planu bezpieczeństwa związanego z wykorzystaniem Internetu.

Pojęcia pokrewne

“Bezpieczeństwo poprzez obronę warstwową” na stronie 4
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

Odsyłacze pokrewne

Wartość systemowa poziomu bezpieczeństwa

Bezpieczeństwo

Bezpieczeństwo na poziomie sieci

Aby ochronić zasoby wewnętrzne, należy wybrać odpowiednie mechanizmy bezpieczeństwa na poziomie sieci.

Przy łączeniu się z niezaufaną siecią strategia bezpieczeństwa musi opisywać całkowity schemat bezpieczeństwa, w tym opis środków, które zostaną zaimplementowane na poziomie sieci. Jednym z lepszych sposobów dostarczenia pełnego zestawu środków bezpieczeństwa na poziomie sieci jest zainstalowanie zapory firewall.

Dostawca usług internetowych może być ważnym elementem w planie zabezpieczania sieci. Schemat bezpieczeństwa sieciowego powinien informować, jakie zabezpieczenia są dostarczane przez dostawcę usług internetowych. Mogą to być na przykład reguły filtrowania dla połączeń z routerem dostawcy usług internetowych i środki ostrożności dotyczące publicznej usługi DNS.

Firewall w ogólnym planie zabezpieczania systemu z pewnością stanowi jedną z głównych linii obrony, ale nie powinien być jedyną taką linią. Potencjalne zagrożenia w Internecie mogą wystąpić na różnych poziomach, dlatego niezbędne jest zastosowanie wielu warstw obrony.

Podłączając system lub sieć wewnętrzną do Internetu, należy rozważyć zastosowanie firewalla jako głównej linii obrony przeciwko atakom. Wprawdzie produkt IBM Firewall for the i5/OS nie jest już oferowany i obsługiwany, jednak na rynku dostępnych jest wiele innych produktów pełniących analogiczne funkcje.

Ponieważ komercyjne firewalle udostępniają pełny wachlarz technologii związanych z bezpieczeństwem sieciowym, przedsiębiorstwo JKL Toy Company zdecydowało się na ochronę sieci za pomocą jednego z takich produktów. Wybrany firewall nie chroni systemu operacyjnego, więc firma zdecydowała się wykorzystać dodatkowe zabezpieczenie w postaci reguł pakietów systemu i5/OS. Pozwala to tworzyć filtry i reguły translacji adresów sieciowych do sterowania przepływem pakietów dla serwera internetowego.

Pojęcia pokrewne

“Bezpieczeństwo poprzez obronę warstwową” na stronie 4
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

“Scenariusz: plany dotyczące e-biznesu firmy JKL Toy Company” na stronie 8
Typowy scenariusz opisany na przykładzie firmy JKL Toy Company, która zdecydowała się na rozszerzenie swojej działalności biznesowej na Internet, może być pomocny przy przygotowywaniu własnych planów dotyczących e-biznesu.

Wykrywanie włamań

Informacje pokrewne

All You Need to Know When Migrating from IBM Firewall for AS/400

Zapory firewall

Zapora firewall to blokada umieszczona na granicy między chronioną siecią wewnętrzną a siecią niezaufaną, taką jak Internet.

W większości firm firewalli używa się do bezpiecznego podłączenia sieci wewnętrznej do Internetu, chociaż firewall może także oddzielać jedną sieć wewnętrzną od drugiej.

Firewall pełni funkcję pilnie strzeżonych wrót (*punktu styczności*) między bezpieczną siecią wewnętrzną a siecią niezaufaną. Jego funkcje są następujące:

- pozwala użytkownikom w obrębie sieci wewnętrznej korzystać ze z góry określonych zasobów znajdujących się w sieci zewnętrznej,
- uniemożliwia nieuprawnionym użytkownikom z sieci zewnętrznej korzystanie z zasobów sieci wewnętrznej.

Zastosowanie firewalla jako bramy do Internetu (lub innej sieci) zdecydowanie zwiększa bezpieczeństwo sieci wewnętrznej. W ten sposób uproszczone zostaje też administrowanie bezpieczeństwem sieci, ponieważ firewall jest w stanie zrealizować wiele dyrektyw zapisanych w strategii bezpieczeństwa.

Jak działa firewall

Aby zrozumieć sposób działania firewalla, należy wyobrazić sobie sieć jako budynek, do którego dostęp trzeba kontrolować. Jedynym wejściem jest hall. W hallu znajdują się: recepcjoniści, strażnicy, kamery wideo rejestrujące zachowanie gości oraz czytniki identyfikatorów sprawdzające tożsamość wchodzących do budynku osób.

Te środki zaradcze mogą dobrze funkcjonować, gdy chodzi o ochronę dostępu do budynku. Lecz jeśli osobie nie mającej uprawnień uda się dostać do wnętrza budynku, środki ochrony zastosowane w hallu przestają mieć znaczenie. Aby wykryć podejrzane zachowanie intruza, należałoby śledzić każdy jego krok w budynku.

Elementy składowe firewalla

Firewall składa się ze sprzętu i oprogramowania, które wspólnie zapobiegają nieautoryzowanemu dostępowi do części sieci. Elementy składowe firewalla to:

- **Sprzęt**

  Sprzętowe składniki firewalla to zwykle osobny komputer lub inne urządzenie, którego wyłącznym zadaniem jest uruchamianie oprogramowania zapory.
- **Oprogramowanie**

  Oprogramowanie firewalla to szereg różnych aplikacji. Od strony bezpieczeństwa sieci, firewall realizuje poniższe funkcje za pośrednictwem różnych technologii:
  - filtrowanie pakietów IP
  - usługi translacji adresów sieciowych
  - serwer SOCKS
  - serwery proxy dla różnych usług, takich jak HTTP, Telnet, FTP itp.
  - przekazywanie poczty
  - rozdzielony system DNS
  - protokołowanie
  - monitorowanie w czasie rzeczywistym

  Uwaga: Niektóre firewalle oferują także usługi sieci VPN, które pozwalają zestawiać szyfrowane sesje między danym firewallem a innymi zgodnymi zaporami.

Korzystanie z funkcji firewalla

Aby zapewnić użytkownikom wewnętrznym bezpieczny dostęp do usług w Internecie, można użyć serwerów proxy lub SOCKS bądź reguł translacji adresów sieciowych (NAT) firewalla. Serwery proxy i SOCKS przerywają połączenia TCP/IP na firewallu, aby ukryć dane z sieci wewnętrznej przed siecią niezaufaną. Serwery te udostępniają dodatkowe możliwości protokołowania.

Translacji adresu sieciowego (NAT) można użyć do zapewnienia użytkownikom Internetu łatwego dostępu do systemu publicznego za firewallem. Zapora nadal chroni sieć, ponieważ usługa NAT ukrywa wewnętrzne adresy IP.

Dodatkowa ochrona sieci wewnętrznej płynie z możliwości uruchomienia osobnego serwera DNS na potrzeby firewalla. Efektywnie działają wtedy dwa serwery DNS: jeden obsługujący żądania wyłącznie z sieci wewnętrznej i drugi obsługujący żądania dotyczące zasobów sieci zewnętrznej, w tym żądania samego firewalla. Pozwala to ograniczyć dostęp z zewnątrz do informacji na temat systemów w sieci wewnętrznej.

Definiując strategię działania firewalla, łatwo odnieść wrażenie, że wystarczy zabronić wszystkiego, co stanowi zagrożenie i dopuścić wszystko inne. Jednakże ze względu na fakt, że przestępcy komputerowi ciągle wymyślają nowe metody ataku, należy być na to przygotowanym i przewidzieć sposoby zabezpieczenia. Nawiązując do przykładu z budynkiem, konieczne jest bezustanne monitorowanie wnętrza, aby mieć pewność, że nikt nie zdołał ominąć wszystkich zabezpieczeń przy wejściu. Generalnie, bardziej kosztowne i pracochłonne jest naprawianie skutków włamań niż zapobieganie im.

W przypadku firewalla najlepszą strategią jest zezwolenie na działanie tylko tych aplikacji, które zostały wypróbowane i okazały się godne zaufania. Zgodnie z tym założeniem, konieczne jest zdefiniowanie wyczerpującej listy usług, które muszą być uruchomione w połączeniu z firewallem. Każda z usług charakteryzowana jest kierunkiem połączenia (z zewnątrz do wewnątrz lub z wewnątrz na zewnątrz). Należy ponadto zestawić listę użytkowników, którzy będą uprawnieni do korzystania z poszczególnych usług, jak również listę komputerów, z których mogą napływać żądania połączeń z daną usługą.

W jaki sposób firewall chroni sieć

Firewall instalowany jest w miejscu połączenia sieci wewnętrznej z Internetem (lub inną siecią niezaufaną). Można wtedy ograniczyć możliwe punkty wejścia do sieci wewnętrznej. Firewall stanowi pojedynczy i jedyny punkt styku między siecią wewnętrzną a Internetem. Dysponowanie pojedynczym punktem styku pozwala zachować większą kontrolę nad dozwolonym przepływem danych do sieci i wypływem danych z sieci na zewnątrz.

Dla świata zewnętrznego firewall jest widoczny jako pojedynczy adres. Udostępnia on zasoby sieci niezaufanych za pośrednictwem serwerów proxy lub SOCKS albo usługi translacji adresów sieciowych, ukrywając rzeczywiste adresy funkcjonujące w sieci wewnętrznej. Tym sposobem firewall strzeże poufności danych w sieci wewnętrznej. Ochrona poufności informacji na temat sieci wewnętrznej jest jedną z metod obrony przed atakiem przez podszycie się pod uprawnionego użytkownika (spoofing).

Firewall pozwala kontrolować przepływ informacji między siecią wewnętrzną a zewnętrzną w obie strony, minimalizując tym samym niebezpieczeństwo ataku. Firewall filtruje cały ruch przychodzący do sieci, dopuszczając tylko ściśle określone pakiety skierowane pod ściśle określone adresy. Pozwala to zmniejszyć ryzyko nieuprawnionego dostępu do systemów wewnętrznych za pośrednictwem takich usług, jak Telnet lub FTP.

Czego firewall nie może zapewnić

Firewall w znacznym stopniu uodparnia system na niektóre rodzaje ataków, lecz powinien być tylko jednym z elementów kompleksowego zabezpieczenia sieci. Firewall nie zapewnia na przykład ochrony danych wysyłanych poprzez Internet przy użyciu takich aplikacji, jak poczta SMTP, usługi FTP lub sesje Telnet. Jeśli dane te nie zostaną przed wysłaniem zaszyfrowane, osoba o złych intencjach może przechwycić je na drodze do miejsca przeznaczenia.

Reguły pakietów systemu i5/OS

Reguły pakietów systemu operacyjnego i5/OS mogą zostać zastosowane do zabezpieczenia systemu. Reguły pakietów to funkcje systemu operacyjnego i5/OS dostępne za pośrednictwem interfejsu programu System i Navigator.

Reguł pakietów można użyć do skonfigurowania dwóch głównych technologii związanych z bezpieczeństwem internetowym, które umożliwiają sterowanie przepływem pakietów TCP/IP:

- Translacja adresu sieciowego (NAT)
- Filtrowanie pakietów IP

Ponieważ translacja NAT i filtrowanie pakietów IP są wbudowanymi częściami systemu operacyjnego i5/OS, stanowią one ekonomiczną metodę zabezpieczania systemu. W niektórych przypadkach te technologie zabezpieczeń mogą

dostarczać wszystkiego co jest potrzebne, bez konieczności dodatkowych zakupów. Jednak nie utworzą one prawdziwej, funkcjonalnej zapory firewall. Można korzystać z samego zabezpieczania pakietów IP lub w połączeniu z firewallem, w zależności od potrzeb i celów związanych z bezpieczeństwem.

Uwaga: Bezpieczeństwo systemu powinno być ważniejsze niż koszty. Aby mieć pewność maksymalnego zabezpieczenia systemu produkcyjnego, należy rozważyć użycie firewalla.

Translacja adresu sieciowego i filtrowanie pakietów IP

Translacja adresu sieciowego (NAT) polega na modyfikacji źródłowego lub docelowego adresu IP pakietów przesyłanych w systemie. Translacja NAT stanowi bardziej przezroczystą alternatywę dla serwerów proxy i SOCKS, pracujących na firewallu. Upraszcza także konfigurowanie sieci, umożliwiając łączenie sieci o niekompatybilnych strukturach adresowania. Używając reguł NAT można korzystać z systemu operacyjnego i5/OS jako bramy pomiędzy dwoma sieciami o niezgodnych schematach adresowania. Można także używać NAT do ukrywania prawdziwych adresów IP jednej sieci przez dynamiczne podstawianie jednego lub wielu adresów zamiast adresów prawdziwych. Ponieważ filtrowanie pakietów IP i NAT uzupełniają się wzajemnie, są często wspólnie używane w celu lepszej ochrony sieci.

Utrzymywanie publicznego serwera WWW znajdującego się za firewallem jest znacznie prostsze przy korzystaniu z NAT. Publiczne adresy IP dla serwera WWW ulegają translacji na prywatne wewnętrzne adresy IP. Redukuje to liczbę zarejestrowanych adresów IP i minimalizuje wpływ na istniejącą sieć. Zapewnia to także dostęp do Internetu użytkownikom wewnętrznym, ukrywając prywatne wewnętrzne adresy IP.

Filtrowanie pakietów IP daje możliwość wybiórczego blokowania lub zabezpieczania ruchu IP w oparciu o informacje z nagłówków pakietów. Kreator konfiguracji internetowej w programie System i Navigator pozwala szybko i łatwo skonfigurować podstawowe reguły filtrowania w celu zablokowania niepożądanego ruchu w sieci.

Filtrowania pakietów IP można użyć do:

- Utworzenia zestawu reguł filtrowania w celu określenia, którym pakietom IP zezwolić na wejście do sieci, a którym zabronić dostępu. Reguły filtrowania stosuje się do interfejsu fizycznego (na przykład Token Ring lub Ethernet). Można stosować te same reguły do wielu interfejsów fizycznych lub stosować różne reguły do każdego interfejsu.
- Utworzenia reguł, które przyjmują lub odrzucają określone pakiety w oparciu o następujące informacje z nagłówka:
  - adres IP miejsca docelowego pakietu,
  - protokół adresu źródłowego IP (na przykład TCP, UDP itp.),
  - port docelowy (na przykład port 80 dla HTTP),
  - port źródłowy,
  - kierunek datagramu IP (przychodzący lub wychodzący),
  - przekazany lub lokalny.
- Ochrony aplikacji w systemie przed dostępem ze strony niepożądanego lub zbędnego ruchu w sieci. Można także zapobiegać przepływowi pakietów do innych systemów. Obejmuje to pakiety Internet Control Message Protocol (ICMP) niskiego poziomu (na przykład pakiety PING), dla których nie jest wymagany żaden określony serwer aplikacji.
- Określenia, czy reguły filtrowania mają tworzyć w protokole systemowym pozycje zawierające informacje na temat pakietów i spełniania reguły. Gdy informacja zostanie zapisana jako pozycja protokołu systemowego, nie można już jej zmienić. Protokół jest idealnym narzędziem do kontrolowania aktywności w sieci.

Reguły filtrowania pakietów pozwalają zabezpieczyć systemy komputerowe przez odrzucanie lub akceptowanie pakietów IP w zależności od zdefiniowanego kryterium. Reguły translacji adresów sieciowych umożliwiają ukrycie informacji z systemu wewnętrznego przed użytkownikami z zewnątrz poprzez zamianę prywatnych adresów IP na jeden adres publiczny. Wprawdzie filtrowanie pakietów IP i reguły translacji adresów sieciowych są rdzennymi technologiami bezpieczeństwa sieciowego, ale nie dają tego samego poziomu ochrony, co w pełni funkcjonalny produkt, jakim jest firewall. Należy bardzo starannie przeanalizować potrzeby i cele w zakresie bezpieczeństwa przed podjęciem decyzji o wyborze między pełnym produktem typu firewall a regułami filtrowania pakietów systemu i5/OS.

Pojęcia pokrewne

Translacja adresu sieciowego (NAT)

Filtrowanie pakietów IP

Wykrywanie włamań

Częścią procesu *wykrywania włamań* jest zbieranie informacji dotyczących prób nieautoryzowanego dostępu i ataków poprzez sieć TCP/IP. Ogólna strategia bezpieczeństwa powinna zawierać sekcję poświęconą wykrywaniu włamań.

Termin *wykrywanie włamań* jest w dokumentacji systemu i5/OS używany w dwóch znaczeniach. W pierwszym znaczeniu odnosi się do zapobiegania i wykrywania ryzyka naruszenia bezpieczeństwa. Na przykład intruz może próbować włamać się do systemu przy użyciu nieprawidłowego identyfikatora użytkownika lub też niedoświadczony użytkownik ze zbyt dużymi uprawnieniami może zmieniać istotne obiekty w bibliotekach systemowych.

W drugim znaczeniu wykrywanie włamań odnosi się do nowej funkcji wykrywania włamań, która monitoruje podejrzany ruch w systemie na podstawie strategii. Użytkownik może utworzyć strategię wykrywania włamań, w ramach której nadzorowane są podejrzane zdarzenia mające swoje źródło w sieci TCP/IP.

Wybór opcji bezpieczeństwa sieci w systemie i5/OS

Opcje bezpieczeństwa sieci należy wybrać w oparciu o plany użycia Internetu.

Rozwiązania chroniące sieć przed dostępem użytkowników, którzy nie posiadają uprawnień, oparte są z reguły na zaporach firewall. W celu ochrony systemu można wybrać w pełni funkcjonalny firewall lub wprowadzić wybrane technologie zabezpieczania sieci będące częścią implementacji TCP/IP w systemie i5/OS. Implementacja ta obejmuje reguły pakietów (filtrowanie pakietów IP i translację adresów sieciowych - NAT) oraz serwer proxy HTTP for i5/OS, który jest programem licencjonowanym.

Wybór między regułami pakietów a firewallem zależy od środowiska sieciowego, wymagań odnośnie dostępu i potrzeb dotyczących zabezpieczeń. Podłączając system lub sieć wewnętrzną do Internetu bądź innej niezaufanej sieci, należy rozważyć zastosowanie firewalla jako głównej linii obrony przeciwko atakom.

Firewall jest w takiej sytuacji zabezpieczeniem najbardziej godnym polecenia, jako wyspecjalizowane urządzenie z odpowiednim oprogramowaniem i ograniczoną liczbą interfejsów do kontaktu z siecią zewnętrzną. Tymczasem technologie chronionego dostępu do Internetu w ramach implementacji TCP/IP w systemie i5/OS to platforma ogólnego przeznaczenia, która udostępnia na zewnątrz mnóstwo interfejsów i aplikacji.

Uwaga: Warto użyć zarówno firewalla, jak i zintegrowanych zabezpieczeń sieci systemu i5/OS. Pomoże to ochronić system przed atakami z wewnątrz (zza firewalla) i wszelkimi atakami, które ominą firewall ze względu na złą konfigurację lub inne powody.

Ta różnica jest istotna z wielu względów. Na przykład, dedykowany produkt typu firewall nie realizuje żadnych funkcji ani aplikacji poza tymi, które wchodzą w skład samego firewalla. Jeśli więc atakującemu uda się nawet obejść firewall i zyskać do niego dostęp, nie będzie mógł uczynić wiele złego. Jeśli natomiast atakujący ominie standardowe zabezpieczenia TCP/IP wbudowane w system, zyska potencjalnie dostęp do wielu przydatnych aplikacji, usług i danych. Nic nie powstrzyma go przed zniszczeniem tego systemu lub przed użyciem go w celu przedostania się do innych systemów w sieci.

Podobnie jak w przypadku wszystkich decyzji dotyczących ochrony, należy rozważyć potencjalne korzyści przez porównanie z koniecznymi kosztami. Innymi słowy, trzeba przeanalizować priorytety związane z działaniem sieci i zastanowić się nad poziomem ryzyka, jaki jesteśmy w stanie zaakceptować i nad ceną, jaką jesteśmy gotowi zapłacić za jego minimalizowanie. Poniższa tabela zawiera zestaw wskazówek pomocnych w podjęciu decyzji, kiedy można poprzestać na standardowych zabezpieczeniach TCP/IP, a kiedy należy użyć wyspecjalizowanego firewalla. Na podstawie tabeli łatwiej będzie ustalić, czy w danej sytuacji konieczny jest firewall, standardowe zabezpieczenia TCP/IP, czy też obie te techniki.

Technologia ochrony	Preferowane użycie zabezpieczeń TCP/IP w systemie i5/OS	Preferowane użycie dedykowanego firewalla
Filtrowanie pakietów IP	• Zapewnienie dodatkowej ochrony dla pojedynczego systemu operacyjnego i5/OS, takiego jak publicznie dostępny serwer WWW lub system intranetowy z ważnymi danymi. • Ochrona podsieci w obrębie firmowego intranetu, kiedy system operacyjny i5/OS działa jako brama (router) na potrzeby pozostałej części sieci. • Kontrolowanie komunikacji z częściowo zaufanym partnerem w ramach sieci prywatnej lub ekstranetu, przy czym system operacyjny i5/OS pełni funkcję bramy.	• Ochrona całej sieci firmowej od strony połączenia z Internetem lub z inną siecią niezaufaną. • Ochrona dużej podsieci, w której panuje nasilony przepływ pakietów, przed pozostałą częścią sieci firmy.
Translacja adresu sieciowego (NAT)	• Możliwość połączenia dwóch sieci prywatnych o niezgodnych strukturach adresowania. • Możliwość ukrycia adresów w podsieci przed mniej zaufaną siecią.	• Możliwość ukrycia adresów klientów korzystających z Internetu lub innej sieci niezaufanej. Alternatywa wobec serwerów Proxy i SOCKS. • Udostępnienie usług systemu znajdującego się w sieci prywatnej klientom w sieci Internet.
Serwer proxy	• Pośredniczenie w połączeniach ze zdalnymi miejscami w sieci firmowej, gdy centralny firewall daje dostęp do Internetu.	• Pośredniczenie w połączeniach całej sieci firmowej z Internetem.

Odsyłacze pokrewne

Filtrowanie IP i translacja adresów sieciowych

HTTP Server for i5/OS

Informacje pokrewne

AS/400 Internet Security Scenarios: A Practical Approach

Bezpieczeństwo na poziomie aplikacji

W przypadku wielu popularnych aplikacji i usług internetowych ryzykiem dotyczącym bezpieczeństwa można zarządzać na kilka sposobów.

Zabezpieczenia na poziomie aplikacji sterują interakcją użytkownika z określonymi aplikacjami. Należy skonfigurować zabezpieczenia dla każdej używanej aplikacji. Szczególny nacisk należy położyć na zabezpieczanie tych aplikacji, które będą używane lub dostarczane za pośrednictwem Internetu. Takie aplikacje i usługi są narażone na nieprawidłowe użycie przez nieuprawnionych użytkowników szukających dostępu do systemów sieciowych. Używane zabezpieczenia powinny chronić przed ryzykiem naruszenia bezpieczeństwa zarówno po stronie klientów, jak i serwerów.

Chociaż bezpieczeństwo każdej używanej aplikacji ma duże znaczenie, zabezpieczenia na poziomie aplikacji są jedynie małym fragmentem kompleksowej strategii bezpieczeństwa.

Pojęcia pokrewne

“Bezpieczeństwo poprzez obronę warstwową” na stronie 4
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

Bezpieczeństwo serwera WWW

Udostępniając serwis WWW, nie należy dawać odwiedzającym wglądu w ustawienia serwera ani w kod użyty do wygenerowania strony. Strona powinna szybko się ładować oraz być łatwa i przyjemna w odbiorze, a kwestie techniczne powinny pozostać w ukryciu.

Administratorzy muszą upewnić się, że działania związane z bezpieczeństwem nie wpłyną negatywnie na atrakcyjność serwisu WWW i że faktycznie będą implementować wybrane modele bezpieczeństwa. W tym celu należy wybrać odpowiednie zabezpieczenia wbudowane w serwer IBM HTTP Server for i5/OS.

Rozdział dokumentacji technicznej (Redbook) IBM HTTP Server (powered by Apache)  poświęcony wdrażaniu zabezpieczeń zawiera opis sposobów użycia uwierzytelniania, kontroli dostępu i szyfrowania do zwiększania bezpieczeństwa.

Protokół Hypertext Transfer Protocol (HTTP) dostarcza możliwości wyświetlania danych, ale nie umożliwia ich zmiany w zbiorze bazy danych. Czasem jednak konieczne jest napisanie aplikacji, które muszą aktualizować zbiory bazy danych. Na przykład może zajść potrzeba tworzenia formularzy, które po wypełnieniu aktualizują bazę danych i5/OS. W tym celu można użyć programów Common Gateway Interface (CGI).

Innym zabezpieczeniem są serwery proxy. Otrzymują one żądania skierowane do innych serwerów, a następnie realizują je, przekazują dalej, przekierowują lub odrzucają.

Serwer HTTP utrzymuje protokół dostępu, którego można używać do monitorowania zarówno pomyślnych, jak i niepomyślnych prób dostępu do serwera.

Poza programami CGI na stronie WWW można używać języka Java. Przed dodaniem programów w języku Java do stron WWW należy zrozumieć zagadnienia związane z bezpieczeństwem tego języka.

Pojęcia pokrewne

"Java i bezpieczeństwo internetowe"
We współczesnych środowiskach informatycznych coraz większą popularność zyskują programy napisane w języku Java. Należy być przygotowanym na zarządzanie czynnikami bezpieczeństwa związanymi z tym językiem.

Informacje pokrewne

Proxy server types and uses for HTTP Server (powered by Apache)

Security tips for HTTP Server

Common Gateway Interface

Java i bezpieczeństwo internetowe

We współczesnych środowiskach informatycznych coraz większą popularność zyskują programy napisane w języku Java. Należy być przygotowanym na zarządzanie czynnikami bezpieczeństwa związanymi z tym językiem.

Zapora firewall zapewnia dobrą ochronę przed większością zagrożeń ze strony Internetu, nie zabezpiecza jednak przed wieloma zagrożeniami związanymi z językiem Java. Strategia bezpieczeństwa powinna szczegółowo określać zasady zabezpieczenia systemu od strony trzech sposobów zastosowania języka Java: aplikacji, apletów i serwletów. Ponadto wymagane jest zrozumienie zasad interakcji między językiem Java i zabezpieczeniami zasobów pod względem uwierzytelniania i autoryzacji programów Java.

Aplikacje w języku Java

Jako język, Java ma kilka cech charakterystycznych, które chronią programistów przed popełnieniem nieumyślnych błędów, powodujących problemy z integralnością (inne języki powszechnie używane do tworzenia aplikacji dla komputerów osobistych, takie jak C lub C++, nie chronią programistów przed nieumyślnymi błędami w takim stopniu, jak Java). Język Java korzysta przykładowo z mechanizmów silnej typizacji, czyli ścisłego narzucania reguł typizacji bez wyjątków, które chronią programistę przed używaniem obiektów w niezamierzony sposób. Java nie pozwala na manipulację wskaźnikami, co chroni programistę przed przypadkowym dostępem poza pamięć przeznaczoną dla

programu. Z perspektywy tworzenia aplikacji język Java można więc traktować jak inne języki programowania wysokiego poziomu. Należy stosować te same reguły bezpieczeństwa dla tworzenia aplikacji jak w przypadku innych języków programowania używanych w systemie.

Aplety w języku Java

Aplety Java to niewielkie programy napisane w języku Java, które można stosować na stronach HTML. Są one uruchamiane na klientach, ale mogą uzyskać dostęp do systemu operacyjnego i5/OS. Program korzystający z interfejsu Open Database Connectivity (ODBC) lub program pracujący w standardzie AAPC (advanced program-to-program communications - zaawansowana komunikacja program-program) uruchomiony na komputerze osobistym w sieci również może uzyskać dostęp do systemu operacyjnego, kiedy na przykład system jest wykorzystywany do udostępniania aplikacji lub pełni funkcję serwera WWW. Ogólnie aplety Java mogą nawiązać sesję tylko z tym systemem operacyjnym i5/OS, z którego pochodzą. Dlatego też aplet Java może uzyskać dostęp do systemu operacyjnego i5/OS z podłączonego komputera osobistego tylko wtedy, gdy aplet pochodzi z tego systemu i5/OS.

Aplet może próbować podłączyć się do dowolnego portu TCP/IP systemu. Nie musi komunikować się z serwerem oprogramowania napisanym w języku Java. Jednak w przypadku systemów napisanych za pomocą bibliotek IBM Toolbox for Java aplet musi dostarczyć identyfikator użytkownika i hasło podczas nawiązywania połączenia z serwerem. Wszystkie systemy opisane w tej dokumentacji to systemy operacyjne i5/OS. (Serwer aplikacji napisany w języku Java nie musi korzystać z biblioteki IBM Toolbox for Java). Zwykle klasa IBM Toolbox for Java prosi użytkownika przy pierwszym połączeniu o identyfikator i hasło.

Aplet może wykonywać operacje w systemie operacyjnym i5/OS tylko wtedy, gdy profil użytkownika ma do nich uprawnienia. Dlatego dobry schemat zabezpieczania zasobów jest bardzo ważny na początku stosowania apletów w języku Java w celu rozszerzenia aplikacji o nowe funkcje. Gdy system przetwarza żądania z apletów, nie korzysta z wartości ograniczonych możliwości w profilu użytkownika.

Przeglądarka apletów pozwala testować aplet w systemie operacyjnym i5/OS. Nie podlega jednak ograniczeniom przeglądarki związanym z bezpieczeństwem. Dlatego też należy korzystać z przeglądarki apletów tylko do testowania własnych apletów, nigdy zaś do uruchamiania apletów pochodzących z zewnątrz. Aplety w języku Java często zapisują dane na napędzie komputera PC użytkownika, co może dać apletowi okazję do destrukcyjnego działania. Jednak tożsamość apletu Java można określić, podpisując go za pomocą certyfikatu cyfrowego. Podpisany aplet może zapisywać dane na lokalnym napędzie komputera osobistego, nawet jeśli domyślne ustawienia przeglądarki zabraniają tego. Podpisany aplet może także pisać na odwzorowanych napędach systemu, ponieważ komputer osobisty traktuje je jak napędy lokalne.

W przypadku własnych apletów Java pochodzących z własnego systemu może być wskazane korzystanie z podpisów cyfrowych. Należy jednak pouczyć użytkowników, aby nie akceptowali podpisanych apletów z nieznanego źródła.

Już od wersji V4R4 możliwe jest korzystanie z biblioteki IBM Toolbox for Java w celu skonfigurowania protokołu SSL (Secure Sockets Layer). Zabezpieczanie aplikacji w języku Java za pomocą SSL możliwe jest też za pomocą pakietu IBM Developer Toolkit for Java. Zastosowanie protokołu SSL z aplikacjami w języku Java polega na szyfrowaniu danych przesyłanych między klientem a serwerem, takich jak identyfikator i hasło użytkownika. W celu skonfigurowania zarejestrowanych programów w języku Java na potrzeby protokołu SSL, można posłużyć się programem Digital Certificate Manager (DCM).

Serwlety w języku Java

Serwlety to komponenty serwera napisane w języku Java, które dynamicznie rozszerzają funkcjonalność serwera WWW, nie zmieniając przy tym kodu serwera. Serwer aplikacji IBM WebSphere Application Server wchodzący w skład pakietu IBM Web Enablement for i5/OS umożliwia obsługę serwletów w systemie operacyjnym i5/OS.

Konieczne jest korzystanie z funkcji bezpieczeństwa zasobów wobec obiektów serwletów, z których korzysta system. Jednak zastosowanie w serwlecie funkcji bezpieczeństwa zasobów nie wystarczy do jego całkowitego zabezpieczenia. Gdy serwer WWW załaduje serwlet, funkcje bezpieczeństwa zasobów nie zapobiegną uruchomieniu go także przez innych. Dlatego funkcji bezpieczeństwa zasobów należy używać w połączeniu z funkcjami i dyrektywami

bezpieczeństwa serwera HTTP. Nie należy na przykład zezwalać serwletom na działanie wyłącznie w profilu serwera WWW. Niezależnie od tego należy korzystać z zabezpieczeń zapewnianych przez narzędzia użyte do utworzenia serwletu, na przykład takie, które zawiera WebSphere Application Server for i5/OS.

Aby dowiedzieć się więcej na temat działań zwiększających ogólny poziom bezpieczeństwa od strony języka Java, można skorzystać z następujących materiałów:

- IBM Developer Kit for Java - bezpieczeństwo w języku Java.
- IBM Toolbox for Java - klasy bezpieczeństwa.
- Zagadnienia związane z ochroną przeglądarek internetowych.

Uwierzytelnianie i autoryzowanie dostępu do zasobów w języku Java

Biblioteka IBM Toolbox for Java zawiera klasy bezpieczeństwa umożliwiające weryfikowanie tożsamości użytkowników oraz, opcjonalnie, przypisywanie tej tożsamości do wątku w systemie operacyjnym obsługującego aplikację lub serwlet działające w systemie operacyjnym i5/OS. Następnie sprawdzanie ochrony zasobów będzie się odbywało dla przypisanej tożsamości.

Pakiet IBM Developer Kit for Java zapewnia obsługę usług uwierzytelniania i autoryzacji języka Java (JAAS), które są standardem rozszerzającym funkcjonalność standardowej edycji Java 2 Software Development Kit (J2SDK). Obecnie J2SDK obejmuje funkcje kontroli dostępu bazujące na pochodzeniu kodu i na jego podpisie.

Zabezpieczanie aplikacji Java za pomocą protokołu SSL

Protokołu SSL (Secure Sockets Layer) można używać do zabezpieczania komunikacji w aplikacjach i5/OS tworzonych przy użyciu pakietu IBM Developer Kit for Java. Aplikacje klienckie korzystające z biblioteki IBM Toolbox for Java także mogą korzystać z zalet SSL. Proces włączania obsługi SSL we własnych aplikacjach Java różni się od procesu włączania SSL w aplikacjach pochodzących z innych źródeł.

Pojęcia pokrewne

“Bezpieczeństwo serwera WWW” na stronie 17
Udostępniając serwis WWW, nie należy dawać odwiedzającym wglądu w ustawienia serwera ani w kod użyty do wygenerowania strony. Strona powinna szybko się ładować oraz być łatwa i przyjemna w odbiorze, a kwestie techniczne powinny pozostać w ukryciu.

Konfigurowanie programu DCM

Usługi uwierzytelniania

Informacje pokrewne

Usługa uwierzytelniania i autoryzowania w języku Java

protokół SSL

Bezpieczeństwo poczty elektronicznej

Korzystanie z poczty elektronicznej w sieci Internet lub innej sieci niezaufanej powoduje zagrożenia systemu, przed którymi nie chroni zapora firewall.

Należy koniecznie zrozumieć istotę tych zagrożeń, aby upewnić się, że w strategii bezpieczeństwa opisano sposoby ich minimalizacji.

Poczta elektroniczna nie różni się od innych form komunikacji. Przed wysłaniem poufnych informacji pocztą elektroniczną ważne jest zapewnienie dyskrecji. Ponieważ wiadomość pocztowa, zanim dotrze do celu, musi przejść przez wiele systemów, możliwe jest jej przechwycenie i odczytanie. Dlatego celowe jest podjęcie kroków zmierzających do odpowiedniego zabezpieczenia wiadomości poczty elektronicznej.

Powszechne zagrożenia związane z pocztą elektroniczną

Istnieją pewne zagrożenia powiązane z korzystaniem z poczty elektronicznej:

- **Zalanie (flooding)** to atak polegający na spowodowaniu odmowy usługi, w trakcie którego system zalewany jest olbrzymią ilością poczty elektronicznej. Stosunkowo proste jest utworzenie programu generującego i wysyłającego miliony wiadomości pocztowych (nawet pustych) na wybrany serwer w celu jego przepełnienia i unieruchomienia. W przypadku braku odpowiednich zabezpieczeń system będący celem ataku może zostać zablokowany (odmowa usługi), ponieważ jego dysk zostanie zapełniony bezużytecznymi wiadomościami. Innym powodem, dla którego system może przestać reagować na wywołania, jest zaangażowanie wszystkich jego zasobów w przetwarzanie poczty wysłanej w złej wierze.
- **Rozsyłanie spamu**, czyli poczta elektroniczna zawierająca śmieci (junk e-mail), to inny popularny typ ataku za pośrednictwem poczty elektronicznej. Przy rosnącej liczbie firm prowadzących działalność handlową w sieci Internet, można zaobserwować eksplozję niechcianej, wysyłanej bez żądania poczty powiązanej z tymi firmami. Są to pocztowe śmieci, wysyłane do dużych list dystrybucyjnych użytkowników poczty elektronicznej, wypełniające skrzynki wszystkich użytkowników.
- **Poufność** jest także zagrożona podczas wysyłania poczty elektronicznej do innej osoby za pośrednictwem Internetu. Taki e-mail, zanim dotrze do adresata, przejdzie przez wiele systemów. Jeśli wiadomość nie została zaszyfrowana, haker może przechwycić i odczytać pocztę w dowolnym miejscu wzdłuż trasy dostarczania.

Opcje zabezpieczania poczty elektronicznej

Aby zabezpieczyć się przed zalewem wiadomości oraz otrzymywaniem niepożądanych przesyłek, należy odpowiednio skonfigurować serwer poczty elektronicznej. Większość aplikacji serwerowych daje możliwość ochrony przed tego rodzaju atakami. Ponadto, celem zapewnienia sobie dodatkowej ochrony, można nawiązać współpracę z dostawcą usług internetowych.

Ewentualna konieczność zastosowania dodatkowych środków zabezpieczających zależy od żądanego poziomu poufności danych, jak również od funkcji ochronnych oferowanych przez posiadane aplikacje obsługi poczty. Na przykład, czy wystarczy ochrona poufności treści listu elektronicznego? Czy konieczne jest zachowanie w ukryciu wszystkich informacji związanych z wiadomością elektroniczną, takich jak źródłowy i docelowy adres IP?

Niektóre aplikacje mają wbudowane zabezpieczenia, które mogą zapewnić wymaganą ochronę. Na przykład produkt Lotus Notes Domino ma kilka zintegrowanych zabezpieczeń, takich jak możliwość szyfrowania całego dokumentu lub wybranych pól w dokumencie.

W celu zaszyfrowania poczty program Lotus Notes Domino tworzy unikalny klucz publiczny i klucz prywatny dla każdego użytkownika. Wiadomość szyfrowana jest za pomocą klucza prywatnego użytkownika, a więc odczytać ją mogą tylko użytkownicy dysponujący odpowiednim kluczem publicznym. Aby adresat mógł odczytać list, klucz publiczny musi zostać uprzednio przekazany odbiorcy wiadomości. Po otrzymaniu zaszyfrowanej poczty program Lotus Notes Domino użyje klucza publicznego nadawcy do odszyfrowania wiadomości.

Informacje na temat korzystania z funkcji szyfrowania w Lotus Notes można znaleźć w plikach pomocy elektronicznej tego programu.

Kiedy zachodzi potrzeba zapewnienia wyższego poziomu poufności dla poczty lub innych danych wymienianych z innym oddziałem firmy, ze zdalnie połączonym użytkownikiem lub z partnerem handlowym, do wyboru jest kilka opcji.

Jeśli aplikacja serwera poczty elektronicznej obsługuje protokół SSL, funkcji tej można użyć do zestawiania chronionych sesji komunikacyjnych między serwerem a klientami poczty. SSL oferuje ponadto możliwość opcjonalnego uwierzytelniania klienta, pod warunkiem że możliwość taką przewidziano także w aplikacji klienta. Ponieważ cała sesja jest szyfrowana, SSL zapewnia przy okazji integralność danych w trakcie ich przesyłania.

Inną opcją jest skonfigurowanie połączenia VPN. Systemu można użyć do skonfigurowania różnych połączeń VPN, w tym między klientami zdalnymi a systemem. Przy korzystaniu z sieci VPN wszystkie dane przesyłane między dwoma punktami końcowymi są szyfrowanie, co gwarantuje zarówno poufność, jak i integralność danych.

Pojęcia pokrewne

“Bezpieczeństwo protokołu FTP”
Protokół FTP umożliwia przesyłanie plików między klientem (użytkownikiem w innym systemie) a serwerem. Należy być świadomym zagrożeń, jakie mogą się pojawić przy używaniu protokołu FTP, aby strategia bezpieczeństwa właściwie opisywała sposób ich minimalizowania.

“Bezpieczeństwo poprzez obronę warstwową” na stronie 4
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

Sieci Virtual Private Network (VPN)

Odsyłacze pokrewne

Terminologia dotycząca bezpieczeństwa

Informacje pokrewne

Lotus Domino Reference Library

Lotus Documentation

Lotus Notes and Domino R5.0 Security Infrastructure Revealed

Lotus Domino for AS/400 Internet Mail and More

Bezpieczeństwo protokołu FTP

Protokół FTP umożliwia przesyłanie plików między klientem (użytkownikiem w innym systemie) a serwerem. Należy być świadomym zagrożeń, jakie mogą się pojawić przy używaniu protokołu FTP, aby strategia bezpieczeństwa właściwie opisywała sposób ich minimalizowania.

Można także korzystać z funkcji zdalnego wykonywania komend, aby przekazywać komendy do systemu serwera. Dlatego też protokół FTP jest przydatny przy pracy ze zdalnymi systemami lub przy przenoszeniu plików pomiędzy systemami. Jednak korzystanie z FTP w sieci Internet lub w innych sieciach niezaufanych wiąże się z pewnymi zagrożeniami. Zrozumienie tych zagrożeń pomoże zabezpieczyć system.

- Schemat uprawnień do obiektów może nie zapewniać wystarczającej ochrony, gdy w systemie działa serwer FTP.

  Na przykład uprawnienia publiczne do obiektów mogą mieć wartość *USE, ale w danym momencie większość użytkowników ma do nich zablokowany dostęp za pomocą funkcji bezpieczeństwa menu. (Funkcje bezpieczeństwa menu zapobiegają wykonywaniu przez użytkowników czynności nie będących jedną z opcji ich menu). Użytkowników FTP nie obejmują ograniczenia dotyczące menu i dlatego mogą odczytywać wszystkie obiekty w systemie.

  Poniżej przedstawiono kilka możliwości zapobiegania takim zagrożeniom:

  – Uaktywnij pełne funkcje bezpieczeństwa obiektów w systemie i5/OS (innymi słowy, zmień model zabezpieczeń z bezpieczeństwa menu na bezpieczeństwo obiektów. Jest to najlepsza i najbardziej bezpieczna opcja).
  – Napisz program obsługi wyjścia dla protokołu FTP, aby ograniczyć dostęp do plików, które mogą być przekazywane przez FTP. Programy obsługi wyjścia powinny zapewniać ochronę przynajmniej na poziomie oferowanym przez program menu. Wielu administratorów będzie prawdopodobnie chciało wprowadzić jeszcze bardziej restrykcyjną kontrolę dostępu przez FTP. Opcja ta obejmuje tylko protokół FTP, a nie inne interfejsy, takie jak ODBC (open database connectivity), DDM (distributed data management) czy DRDA (Distributed Relational Database Architecture).

    Uwaga: Uprawnienie *USE do pliku pozwala użytkownikowi pobrać dany plik. Uprawnienie *CHANGE pozwala użytkownikowi przesłać dany plik.
- Haker może wykorzystać protokół FTP do przeprowadzenia na serwer ataku polegającego na spowodowaniu odmowy usługi i zablokowania profili użytkowników w systemie. Atak tego typu polega na wielokrotnie powtarzanych próbach zalogowania się w profilu użytkownika za pomocą błędnego hasła, aż profil zostanie zablokowany. Zablokowanie profilu następuje po tym, jak liczba nieudanych prób logowania osiągnie wartość maksymalną, równą trzy.

Zmniejszenie ryzyka ataku wymaga pójścia na pewne kompromisy. Dążenie do zwiększenia poziomu bezpieczeństwa systemu zwykle wiąże się z utrudnieniami w dostępie dla zwykłych użytkowników. Serwer FTP zazwyczaj wymusza ograniczanie wartości parametru QMAXSIGN, aby odebrać hakerom możliwość wykonywania wielokrotnych prób logowania, gdyż mogłoby to się skończyć odgadnięciem przez nich hasła. Oto kilka sposobów postępowania, które warto rozważyć:

- Użycie programu obsługi wyjścia logowania się do serwera FTP, aby odrzucić żądania zalogowania profili użytkowników systemowych oraz profili użytkowników, którym wprost odebrano prawo dostępu do FTP. (Przy korzystaniu z takiego programu obsługi wyjścia, próby zalogowania dla profilu bez prawa dostępu, odrzucone przez punkt wyjścia logowania się do serwera FTP, nie są zliczane w limicie prób logowania QMAXSIGN).
- Użycie programu obsługi wyjścia w celu wskazania określonych komputerów, z których dany profil użytkownika może łączyć się z serwerem FTP. Jeśli na przykład osoba z działu księgowości ma dostęp do FTP, należy zezwolić temu profilowi użytkownika na dostęp do serwera FTP tylko z komputerów o adresach IP z zakresu przydzielonego działowi księgowości.
- Użycie programu obsługi wyjścia logowania do zapisywania nazwy użytkownika i adresu IP wszystkich prób zalogowania się do usługi FTP. Protokoły te należy przeglądać regularnie i jeśli profil użytkownika został zablokowany przez maksymalną liczbę prób hasła, należy za pomocą informacji o adresie IP zidentyfikować napastnika i podjąć odpowiednie środki.
- Użyj systemu wykrywania włamań, aby wykryć ataki polegające na spowodowaniu odmowy usługi.

Dodatkowo, punkty wyjścia serwera FTP można wykorzystać w celu zapewnienia dostępu użytkownikom anonimowym. Skonfigurowanie chronionego anonimowego serwera FTP wymaga programów obsługi wyjścia dla punktów wyjścia logowania do serwera FTP oraz sprawdzania poprawności żądania serwera FTP.

Sesje komunikacyjne z serwerem FTP mogą być zabezpieczane za pomocą protokołu SSL. Protokół SSL umożliwia szyfrowanie wszystkich danych przesyłanych w ramach sesji FTP, co zapewnia poufność między innymi nazwy i hasła użytkownika. Ponadto serwer FTP może korzystać z certyfikatów cyfrowych w celu uwierzytelniania klienta.

Dodatkowo można rozważyć korzystanie z anonimowego użytkownika FTP, aby zapewnić wygodny sposób dostępu do materiałów jawnych. Anonimowy FTP umożliwia niezabezpieczony dostęp (bez hasła) do wybranych informacji w systemie zdalnym. System zdalny określa, które informacje mają być ogólnie dostępne. Takie informacje są dostępne publicznie i mogą być przeczytane przez kogokolwiek. Przed skonfigurowaniem anonimowego użytkownika FTP należy uwzględnić ryzyko dotyczące bezpieczeństwa i rozważyć zabezpieczenie serwera FTP za pomocą programów obsługi wyjścia.

Pojęcia pokrewne

“Bezpieczeństwo poczty elektronicznej” na stronie 19
Korzystanie z poczty elektronicznej w sieci Internet lub innej sieci niezaufanej powoduje zagrożenia systemu, przed którymi nie chroni zapora firewall.

Zadania pokrewne

Konfigurowanie anonimowego dostępu przez protokół FTP

Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP

Informacje pokrewne

Zabezpieczanie protokołu FTP

Zabezpieczanie serwera FTP za pomocą protokołu SSL

Opcje zabezpieczania transmisji

Aby zabezpieczyć dane przepływające przez niezaufaną sieć, na przykład Internet, należy wdrożyć odpowiednie środki bezpieczeństwa. Środki te obejmują protokół Secure Sockets Layer (SSL), oprogramowanie System i Access for Windows oraz połączenia przez sieci VPN (Virtual Private Network).

Przypomnijmy, że scenariusz dla firmy JKL Toy Company obejmował dwa podstawowe systemy. Jeden wykorzystywany dla potrzeb projektowania, a drugi do zastosowań produkcyjnych. Oba systemy obsługują dane i

aplikacje o newralgicznym znaczeniu. Dlatego też firma zdecydowała się na dodanie nowego systemu w sieci obwodowej, który służyć będzie do celów związanych z działaniem intranetu i dostępem do Internetu.

Ustanowienie sieci obwodowej daje pewność, że istnieje fizyczna separacja pomiędzy siecią wewnętrzną a Internetem. Separacja ta zmniejsza niebezpieczeństwo ze strony Internetu, na które narażone są systemy wewnętrzne. Wyznaczając nowy system tylko do roli serwera internetowego, firma zmniejsza złożoność zarządzania bezpieczeństwem sieci.

Potrzeby związane z bezpieczeństwem w Internecie powodują, że firma IBM dostarcza ciągle nowych ofert w zakresie zabezpieczeń, aby zapewnić bezpieczne środowisko sieciowe dla e-biznesu w Internecie. W przypadku sieci mającej podłączenie do Internetu konieczne jest wdrożenie odpowiedniego poziomu bezpieczeństwa zarówno z punktu widzenia systemu, jak i z punktu widzenia aplikacji. Przesyłanie danych poufnych w obrębie firmowej sieci intranet, czy też przez połączenie z Internetem, zwiększa potrzebę zastosowania silniejszych zabezpieczeń. Aby uniknąć tych zagrożeń, należy użyć funkcji zapewniających ochronę danych przesyłanych za pośrednictwem Internetu.

Zagrożenia związane z przesyłaniem informacji poprzez niezaufane systemy można zminimalizować za pomocą dwóch funkcji systemu operacyjnego i5/OS przeznaczonych specjalnie do zabezpieczania danych na poziomie transmisji: komunikacji z użyciem protokołu SSL i połączeń przez sieć VPN.

Protokół SSL jest standardem branżowym do zabezpieczania komunikacji między klientami i serwerami. Pierwotnie był przeznaczony do użycia w przeglądarkach WWW, ale liczba innych aplikacji korzystających z tego protokołu wciąż wzrasta. W systemie operacyjnym i5/OS są to między innymi:

- IBM HTTP Server for i5/OS (oryginalny lub oparty na serwerze Apache),
- serwer FTP,
- serwer Telnet,
- Distributed Relational Database Architecture (DRDA) i serwer zarządzania danymi rozproszonymi (distributed data management - DDM),
- Centrum Zarządzania programu System i Navigator,
- serwer usług katalogowych (LDAP),
- aplikacje System i Access for Windows, w tym System i Navigator, jak również aplikacje napisane z użyciem aplikacyjnego interfejsu programistycznego System i Access for Windows,
- programy opracowane za pomocą pakietu Developer Kit for Java oraz aplikacje klienta korzystające z biblioteki IBM Toolkit for Java,
- programy opracowane z użyciem interfejsów programistycznych SSL, które mogą służyć do włączania obsługi protokołu SSL przez aplikacje. Więcej informacji dotyczących tworzenia aplikacji korzystających z protokołu SSL można znaleźć w temacie Secure Sockets Layer APIs.

Niektóre z tych aplikacji obsługują także uwierzytelnianie klienta za pośrednictwem certyfikatów cyfrowych. Protokół SSL korzysta z certyfikatów cyfrowych podczas uwierzytelniania stron komunikacji i podczas tworzenia chronionego połączenia.

Sieci Virtual Private Network

Aby nawiązać bezpieczny kanał komunikacyjny między dwoma punktami końcowymi można użyć połączeń przez sieć VPN (Virtual Private Network). Podobnie jak w przypadku połączenia SSL dane przemieszczające się pomiędzy dwoma punktami końcowymi mogą być szyfrowane, co gwarantuje ich poufność i integralność. Połączenia VPN pozwalają ograniczyć przepływ ruchu do podanych punktów końcowych i ograniczyć typy pakietów, których można używać w połączeniu. Dlatego też połączenia VPN dostarczają pewnego poziomu bezpieczeństwa sieciowego, pomagając zabezpieczyć zasoby sieciowe przed niepowołanym dostępem.

Wybór metody

Zarówno SSL jak i VPN mają w założeniu zapewnić bezpieczeństwo uwierzytelniania oraz poufność i integralność danych. Wybór jednego z tych rozwiązań zależy od kilku czynników. Należy rozważyć takie okoliczności, jak to, z kim

nawiązywana jest komunikacja, za pomocą jakich aplikacji, w jakim stopniu sesja komunikacyjna ma być zabezpieczona i jakie ustępstwa pod względem kosztów i wydajności można ponieść w celu zapewnienia bezpieczeństwa komunikacji.

Ponadto aplikacje mające współpracować z protokołem SSL muszą zostać specjalnie skonfigurowane pod tym kątem. Wiele aplikacji jeszcze nie może korzystać z protokołu SSL. Inne, takie jak Telnet czy System i Access for Windows, zostały uzupełnione o taką możliwość. Sieci VPN natomiast pozwalają na zabezpieczenie całego ruchu pakietów IP przepływającego pomiędzy określonymi punktami końcowymi.

Na przykład w obecnej konfiguracji sieci partnerzy handlowi mogą korzystać z zasobów wewnętrznej sieci firmy za pośrednictwem serwera HTTP w sesjach chronionych protokołem SSL. Jeśli serwer WWW jest jedyną aplikacją, która wymaga zabezpieczenia podczas komunikacji między siecią wewnętrzną a partnerem handlowym, przechodzenie na technikę VPN może nie być potrzebne. Jeśli jednak zakres form komunikacji będzie poszerzany, połączenie VPN może mieć rację bytu. Może zaistnieć również sytuacja, w której wymagane jest zabezpieczenie ruchu we fragmencie sieci, a chcemy uniknąć konfigurowania każdego klienta i serwera do korzystania z SSL. Można wtedy utworzyć połączenie VPN między gatewayami w tej części sieci. Rozwiązanie takie pozwala zabezpieczyć ruch, pozostając niezauważalne dla serwerów i klientów po obu stronach połączenia.

Pojęcia pokrewne

“Bezpieczeństwo poprzez obronę warstwową” na stronie 4
Strategia bezpieczeństwa definiuje obiekty, które mają być chronione, i oczekiwania wobec użytkowników systemu.

“Scenariusz: plany dotyczące e-biznesu firmy JKL Toy Company” na stronie 8
Typowy scenariusz opisany na przykładzie firmy JKL Toy Company, która zdecydowała się na rozszerzenie swojej działalności biznesowej na Internet, może być pomocny przy przygotowywaniu własnych planów dotyczących e-biznesu.

Odsyłacze pokrewne

Interfejsy API do bezpiecznych połączeń przez gniazda

Informacje pokrewne

Protokół SSL

Sieci Virtual Private Network (VPN)

Korzystanie z certyfikatów cyfrowych w połączeniu z protokołem SSL

Certyfikaty cyfrowe stanowią podstawę do korzystania z protokołu SSL dla bezpiecznej komunikacji i są dobrą metodą uwierzytelniania.

System operacyjny i5/OS umożliwia łatwe tworzenie i zarządzanie certyfikatami cyfrowymi dla systemów i użytkowników za pomocą zintegrowanego programu Digital Certificate Manager (DCM).

Ponadto istnieje możliwość skonfigurowania niektórych aplikacji, takich jak IBM HTTP Server for i5/OS, aby korzystały z certyfikatów cyfrowych w celu zapewnienia lepszych metod uwierzytelniania klientów niż nazwy i hasła użytkownika.

Czym jest certyfikat cyfrowy

Certyfikat cyfrowy to dokument elektroniczny, który potwierdza tożsamość właściciela certyfikatu w podobny sposób jak paszport. Zaufana strona pośrednicząca, nazywana ośrodkiem certyfikacji (CA), wystawia certyfikaty cyfrowe dla użytkowników i serwerów. Zaufanie do ośrodka certyfikacji stanowi fundament zaufania do certyfikatu jako dokumentu uwierzytelniającego.

Każdy ośrodek certyfikacji ma własną strategię określającą dane identyfikacyjne konieczne do wystawienia certyfikatu. Niektóre spośród ośrodków certyfikacji wymagają niewielu informacji, na przykład tylko nazwy wyróżniającej. Nazwa wyróżniająca to nazwisko osoby lub nazwa systemu, dla których ośrodek certyfikacji ma wydać cyfrowy adres certyfikatu i cyfrowy adres poczty elektronicznej. Dla każdego certyfikatu jest generowany klucz prywatny i publiczny.

Certyfikat zawiera klucz publiczny, a przeglądarka lub plik chroniony przechowuje klucz prywatny. Pary kluczy skojarzone z certyfikatem mogą być używane do podpisywania i szyfrowania danych, takich jak komunikaty i dokumenty wysyłane pomiędzy użytkownikami i serwerami. Podpisy cyfrowe zapewniają wiarygodność źródła i chronią integralność danych.

Wiele aplikacji jeszcze nie może korzystać z protokołu SSL. Inne, takie jak Telnet czy System i Access for Windows, zostały uzupełnione o taką możliwość.

Pojęcia pokrewne

Konfigurowanie programu DCM

Protokół SSL

Odsyłacze pokrewne

Terminologia dotycząca bezpieczeństwa

Zabezpieczanie dostępu przez Telnet za pomocą protokołu SSL

Możliwe jest takie skonfigurowanie serwera Telnet, aby sesje komunikacyjne Telnet były zabezpieczane za pomocą protokołu SSL.

Pierwszym krokiem podczas konfigurowania serwera Telnet na potrzeby protokołu SSL jest użycie programu Digital Certificate Manager (DCM) w celu utworzenia certyfikatu serwera. Domyślnie serwer Telnet obsługuje zarówno połączenia zabezpieczone, jak i niezabezpieczone. Można jednak skonfigurować usługę Telnet tak, aby dozwolone były tylko sesje zabezpieczone. Ponadto serwer Telnet może wymagać dodatkowego uwierzytelniania klientów przez żądanie od nich certyfikatów cyfrowych.

Ochrona sesji Telnet przez SSL daje wiele korzyści z punktu widzenia bezpieczeństwa systemu. Oprócz uwierzytelniania serwera, wszystkie dane są szyfrowane przed wysłaniem ich za pomocą protokołu Telnet. Po ustanowieniu sesji SSL wszystkie dane protokołu Telnet, łącznie z identyfikatorem użytkownika i wymianą haseł, są szyfrowane.

Najważniejszym czynnikiem do rozważania przy stosowaniu serwera Telnet jest ważność informacji używanych w sesji klienta. Zastosowanie protokołu SSL na serwerze Telnet jest szczególnie wskazane, jeśli przesyłane dane są cenne lub poufne. Po utworzeniu certyfikatu cyfrowego dla aplikacji Telnet serwer Telnet jest w stanie obsługiwać sesje klientów zarówno z użyciem protokołu SSL, jak i bez niego. Jeśli strategia bezpieczeństwa wymaga, aby sesje Telnet zawsze były szyfrowane, można zablokować wszystkie sesje Telnet, które nie używają SSL. Jeśli nie ma potrzeby użycia serwera Telnet obsługującego SSL, można wyłączyć port SSL. Użyciem protokołu SSL w sesjach Telnet można sterować za pomocą komendy Zmiana atrybutów Telnet (Change Telnet Attributes - CHGTELNA) i jej parametru Zezwalaj na użycie protokołu SSL (Allow Secure Sockets Layer - ALWSSL). Aby upewnić się, że żadne aplikacje nie mogą używać portów korzystających lub niekorzystających z SSL zgodnie z założeniami, można też wprowadzić ograniczenie za pomocą komendy Dodanie ograniczenia portu TCP/IP (Add TCP/IP Port Restriction - ADDTCPPORT).

Więcej informacji na temat usługi Telnet wraz ze wskazówkami dotyczącymi jej zabezpieczania za pomocą protokołu SSL i bez niego zawiera Centrum informacyjne IBM Systems - oprogramowanie. Informacje te są wymagane przy korzystaniu z usługi Telnet w systemie operacyjnym i5/OS.

Pojęcia pokrewne

Scenariusz Telnet: zabezpieczanie programu Telnet za pomocą protokołu SSL

Planowanie na potrzeby programu DCM

Informacje pokrewne

Telnet

Bezpieczne połączenia z oprogramowaniem System i Access for Windows przy użyciu protokołu SSL

Aby zabezpieczyć sesję komunikacji z oprogramowaniem System i Access for Windows, można je skonfigurować, aby korzystało z protokołu Secure Sockets Layer (SSL).

Kiedy używany jest protokół SSL, wszystkie pakiety sesji oprogramowania System i Access for Windows są szyfrowane. Dzięki temu danych nie można odczytać w momencie przekazywania ich pomiędzy lokalnym i zdalnym hostem.

Informacje pokrewne

Administrowanie protokołem Secure Sockets Layer (SSL)

Bezpieczeństwo w języku Java

Klasy bezpieczeństwa

Bezpieczna prywatna komunikacja za pośrednictwem sieci VPN

Sieć VPN (Virtual Private Network), czyli rozszerzenie intranetu przedsiębiorstwa w ramach istniejącej sieci publicznej lub prywatnej, może pomóc zapewnić prywatność i bezpieczeństwo komunikacji wewnątrz organizacji.

Kierując się wzrostem popularności sieci VPN oraz wysokim poziomem zapewnianego przez nie bezpieczeństwa, w firmie JKL Toy poważnie rozważane jest wdrożenie takiej sieci w celu przesyłania danych przez Internet. Firma ta wykupiła niedawno inną małą firmę wytwarzającą zabawki i zamierza z nią współdziałać. Konieczne jest utworzenie kanału wymiany informacji między dwiema firmami. Obie firmy mają systemy operacyjne i5/OS i połączenie VPN, które zapewnia należyte bezpieczeństwo danych przesyłanych między dwoma sieciami. Utworzenie sieci VPN jest rozwiązaniem tańszym niż używanie tradycyjnych linii niekomutowanych.

Lista zastosowań, w których sieć VPN sprawdza się najlepiej:

- zdalny dostęp dla użytkowników spoza firmy lub przebywających w terenie,
- połączenia głównej siedziby firmy z komputerami pracowników pracujących w domu i z oddziałami lokalnymi,
- komunikacja między firmami.

W przypadku braku ograniczeń w dostępie użytkowników do newralgicznych systemów mogą pojawić się pewne zagrożenia. Bez opracowania precyzyjnych reguł dostępu do systemu istnieje zagrożenie utraty kontroli nad poufnością danych firmy. Należy opracować plan, który pozwoli ograniczyć dostęp do systemu tylko do tych osób, które muszą wspólnie użytkować dane w systemie. Sieć VPN umożliwia zachowanie kontroli nad przesyłanymi danymi, zapewniając przy tym tak istotne z punktu widzenia bezpieczeństwa funkcje, jak uwierzytelnianie stron i ochrona poufności danych. Po utworzeniu wielu połączeń VPN w każdym z nich można zdefiniować, kto ma mieć dostęp do których systemów. Na przykład działy księgowości i kadr mogą być połączone poprzez odrębną sieć VPN.

Zezwolenie użytkownikom na łączenie się z systemem poprzez Internet oznacza stworzenie możliwości przepływu ważnych dla firmy informacji przez publicznie dostępne sieci komunikacyjne, gdzie dane te są narażone na ataki. Do metod zabezpieczenia przekazywanych danych należą szyfrowanie oraz uwierzytelnianie komunikujących się stron, co służy ochronie poufności danych i uniemożliwia ingerencję osób niepowołanych. Sieci VPN stanowią rozwiązanie jednego z aspektów ogólnego problemu ochrony danych: zabezpieczenia przepływu danych między systemami. Sieć VPN chroni dane przesyłane między dwoma punktami końcowymi połączenia. Dodatkowo można użyć funkcji reguł pakietów w celu określenia, jakie pakiety IP mogą być przesyłane w ramach sieci VPN.

Sieć VPN można utworzyć w celu zestawienia połączenia, w którym ochronie podlegają dane przekazywane między dwoma zaufanymi punktami, nad którymi mamy kontrolę. Należy jednak nadal zwracać uwagę na zakres dostępu zapewnianego partnerom w sieci VPN. W połączeniu VPN zachodzi szyfrowanie danych przesyłanych przez sieci publiczne. Jednak zależnie od konfiguracji, dane przesyłane przez Internet nie muszą być przesyłane za pomocą połączenia VPN. W takim wypadku szyfrowanie danych może nie dotyczyć danych przesyłanych w obrębie sieci wewnętrznych komunikujących się przez połączenie VPN. Z tego powodu należy dokładnie planować konfigurowanie każdego połączenia VPN. Należy upewnić się, że partner sieci VPN otrzymał dostęp tylko do tych hostów lub zasobów sieci wewnętrznej, do których miał go otrzymać.

Na przykład dostawca może potrzebować informacji o częściach znajdujących się na składzie. Informacje te są w bazie danych używanej do aktualizacji stron WWW w sieci intranet. Należy pozwolić dostawcy na bezpośredni dostęp do tych stron poprzez połączenie VPN. Dostawca nie powinien jednak uzyskać dostępu do zasobów systemowych, takich jak sama baza danych. Możliwe jest takie skonfigurowanie sieci VPN, aby przepływ danych między dwoma punktami

końcowymi odbywał się tylko z użyciem portu 80. Port 80 jest domyślnym portem używanym przez protokół HTTP. Dlatego też dostawca może wysyłać żądania i odbierać odpowiedzi tylko przez to połączenie.

VPN należy do środków bezpieczeństwa na poziomie sieci, ponieważ możliwe jest zdefiniowanie rodzaju pakietów, jakie mogą być przekazywane w ramach sieci VPN. Sieci VPN nie działają jednak tak jak firewall podczas regulacji przepływu pakietów przychodzących do systemu i wychodzących z niego. Ponadto połączenie VPN nie jest jedynym sposobem zabezpieczenia komunikacji między systemem operacyjnym i5/OS a innymi systemami. Zależnie od potrzeb lepszym rozwiązaniem może się okazać protokół SSL.

To, czy poziom bezpieczeństwa zapewniany przez sieć VPN odpowiada potrzebom, zależy od chronionego obiektu. Zależy także od zmian, które zamierza się wprowadzić w celu zapewnienia tego poziomu bezpieczeństwa. Podobnie jak w przypadku każdej decyzji podejmowanej odnośnie zabezpieczeń, należy przemyśleć wpływ sieci VPN na strategię bezpieczeństwa.

Pojęcia pokrewne

"Uwagi dotyczące platformy System i oraz bezpieczeństwa internetowego" na stronie 2
Zagadnienia bezpieczeństwa internetowego są bardzo ważne. Ten temat zawiera przegląd zabezpieczeń systemu i5/OS i jego mocnych stron w tym zakresie.

Sieć VPN (Virtual Private Networks)

Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of
Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE “AS IS” BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszym dokumencie oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Umowie Licencyjnej IBM na Kod Maszynowy lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Informacje dotyczące interfejsu programistycznego

W niniejszej publikacji na temat platformy System i oraz bezpieczeństwa internetowego opisano planowane interfejsy programistyczne, pozwalające na pisanie programów umożliwiających korzystanie z usług systemu operacyjnego IBM i5/OS.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

Domino
Distributed Relational Database Architecture (DRDA)
i5/OS
IBM
IBM (logo)
Lotus Notes
Notes
System i
WebSphere

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Java oraz wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

Drukowane w USA