safety of information
information and communication system

Zygmunt STRZYŻAKOWSKI[1]
Katarzyna KWIECIEŃ[2]

BEZPIECZEŃSTWO INFORMACJI W TRANSPORTOWYCH SYSTEMACH TELEINFORMATYCZNYCH

W artykule przedstawiono wybrane metody dostępu do mediów transmisyjnych zagrażające bezpieczeństwu przesyłanych informacji oraz techniczne zabezpieczenia, które mogą znaleźć zastosowanie w obiekcie transportowym. Zaprezentowano założenia projektowe budowy bezpiecznego styku sieci firmowej z Internetem wraz przykładem rozwiązania dla małej i rozbudowanej sieci.

SAFETY OF INFORMATION IN DATA COMMUNICATION NETWORKS FOR TRANSPORT

The paper presents selected methods of access to broadcasting media threatening the security of information transmitted and technical safeguards that can be used in the facility transport. Presents the conceptual design the construction of a secure corporate network interface to the Internet and example solutions for small and dense network.

1. WSTĘP

Systemy teleinformatyczne umożliwiają przedsiębiorstwom transportowym na większą wydajność oraz optymalizację procesu przy wykonywaniu usług dla klientów i obsłudze magazynów oraz pozwalają na integrację różnych systemów, dzięki czemu dane z systemu klienta mogą być przesyłane do systemu operatora, co skraca czas oraz zapobiega powstawaniu błędów. Technologie te mogą wspomagać zarządzanie środkami transportu oraz optymalizować trasy samochodów. Mogą również udoskonalać proces załadunku i wskazywać, jak powinien być rozmieszczony towar w samochodzie. Systemy śledzenia przesyłek pozwalają informować klientów on-line, gdzie aktualnie znajduje się przesyłka.

Biorąc pod uwagę tak szerokie spektrum zastosowań, informacje przetwarzane w systemach teleinformatycznych powinny być one dobrze chronione. W dalszej części artykułu skupiono się na wybranych metodach dostępu do mediów transmisyjnych, technicznych zabezpieczeniach stosowanych w systemach teleinformatycznych oraz możliwościach zabezpieczenia informacji w obiekcie transportowym.

[1] Politechnika Radomska, z.strzyzakowski@pr.radom.pl
[2] Politechnika Radomska, kgkwiecien@wp.pl

2. METODY DOSTĘPU DO MEDIÓW TRANSMISYJNYCH

Najczęściej stosowane są media miedziane, światłowodowe i radiowe. Istnieją różne techniki pozyskiwania, modyfikowania i uniemożliwiania przekazywania informacji sygnału transmitowanego w poszczególnych mediach [1].

Przy pomocy sprzęgacza optycznego część mocy sygnału może być wyprowadzona na zewnątrz światłowodu [4, 6] (do innego włókna). Fizyczny dostęp do włókna jest możliwy zarówno na stacji oraz na pewnych odcinkach trasy optycznej. Można wyróżnić dwie metody związane ze stosowaniem sprzęgaczy optycznych. Pierwsza z nich polega na rozłączeniu lub przecięciu światłowodu i wprowadzeniu sprzęgacza. Sytuacja taka zostanie odnotowana przez operatora, lecz nie przez użytkownika, ponieważ zadziała automatyczne przełączenie dokonywane z reguły w czasie mniejszym od 50 ms [5]. Druga metoda jest pozbawiona konieczności rozłączenia, ponieważ stosuje się sprzęgacze, w których sygnał jest pozyskiwany dzięki wyciekowi sygnału z przegięcia włókna o małym promieniu, a straty mocy na przegięciu są mniejsze od 1% [4]. Pozyskany w ten sposób sygnał może być wprowadzony do odpowiedniego interfejsu odbiorczego. Wybór odpowiedniego odbiornika (urządzenia sieciowego lub analizatora) jest możliwy przy znajomości technologii oraz standardu transmitowanego sygnału. Jeżeli jest on nieznany, można go określić, stosując dostępną aparaturę diagnostyczno-pomiarową. Ze zdekodowanego sygnału można pozyskać nie tylko informacje przekazywane przez użytkowników sieci, lecz także dotyczące jej konfiguracji. Ingerencja w tor światłowodowy może być zauważona i zarejestrowana przez operatora, gdy dokonano przerwania włókna światłowodowego. Jeśli w tor zostaje włączony dowolny sprzęgacz optyczny, to po stronie odbiorczej maleje moc dostarczana do odbiornika. Jest to spadek rzędu od 0,1 do 2 dB, a ponieważ trasy optyczne są projektowane z pewnym zapasem energetycznym, spadek mocy tego rzędu nie spowoduje generacji informacji o zdarzeniu, alarmu czy pojawienia się błędów transmisyjnych. Większość urządzeń umożliwia monitorowanie wartości odbiorczej mocy sygnału z poziomu systemu zarządzania. Jej zmiany w małym zakresie nie generują alarmów [3].

Zdecydowana większość systemów optycznych pracuje w pełnym dupleksie z wykorzystaniem dwu włókien. Często wystarczy monitorowanie jednego toru, aby uzyskać informacje o korespondencji i jej treści między użytkownikami.

Informacje przesyłane w światłowodzie mogą być zmodyfikowane z wykorzystaniem logicznego systemu *back-to-back* i wiąże się to z ingerencją w tor optyczny. Po takim zabiegu fizycznym modyfikacja informacji w pewnym uogólnieniu może odbywać się na dwa sposoby: „udawanie" użytkowników końcowych lub wprowadzenie użytkownika dodatkowego. Oprócz łatwości, z jaką można pozyskać informacje z toru światłowodowego, należy zwrócić uwagę na bardzo dużą ilość informacji oraz różnorodność jej źródeł i typów.

W wypadku tzw. mediów miedzianych mamy do czynienia z mniejszą ilością informacji. Nie można stwierdzić, że technika ingerencji w tego rodzaju medium jest łatwiejsza, ponieważ zależy to od trybu transmisji sygnałów cyfrowych (w wypadku sygnałów analogowych sytuacja jest o wiele prostsza). W dwutorowym trybie transmisji, jeśli sygnał jest monitorowany z wykorzystaniem fizycznego dołączenia się do toru interfejsem o wysokiej impedancji, sytuacja jest bardzo prosta. Ta sama metoda w wypadku jednotorowego trybu transmisji jest bardziej złożona i skomplikowana. Podobne jest, gdy do nasłuchu stosuje się zjawisko indukowania sygnału w sąsiednich torach. Metoda

wykorzystująca przenik w torach miedzianych nie zawsze znajduje zastosowanie, w większości wypadków jest ona bardzo skomplikowana, wyjątek stanowi telefonia analogowa. Mnogość technologii i standardów wymaga indywidualnego podejścia do zagadnienia.

Istnieją systemy, w których monitorowanie torów miedzianych jest możliwe jedynie poprzez włączenie w tor dodatkowego urządzenia. Ingerencja taka powinna być odnotowana przez operatorów sieci. Włączenie dodatkowego urządzenia w tor umożliwia zarówno nasłuchiwanie informacji, jak i jej modyfikację z zastosowaniem technik, których zasada działania jest taka sama jak zasada wykorzystywana w technikach światłowodowych [3].

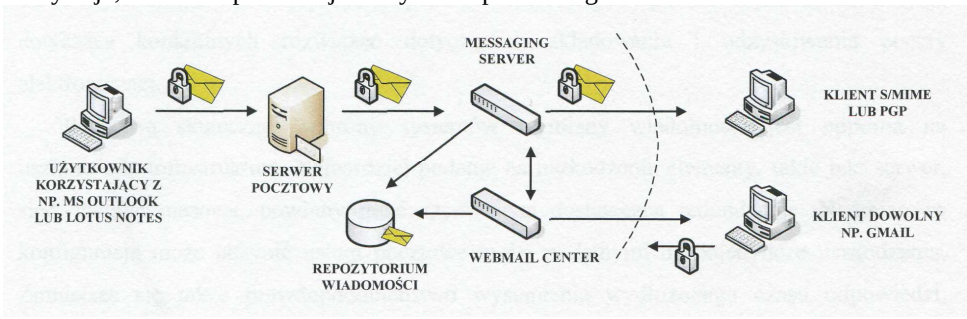
3. TECHNICZNE ŚRODKI ZABEZPIECZAJĄCE MOŻLIWE DO ZASTOSOWANIA W OBIEKCIE TRANSPORTOWYM

Techniczne środki zabezpieczające obejmują m.in. bezpieczeństwo poczty elektronicznej, szyfrowanie danych (kryptografia), zapory sieciowe, bezpieczne zasilanie, ochronę przed szkodliwym oprogramowaniem, systemy wykrywania włamań, zabezpieczenia sieci WLAN oraz ochronę transmisji z VPN.

Jednym ze sposobów ochrony poczty elektronicznej jest obrona przed spamem. Istnieje oprogramowanie wykrywające spam na poziomie klienta, ale dla większości organizacji lepszym rozwiązaniem jest pozbywanie się ich na poziomie serwera pocztowego. Dzięki temu można zatrzymać niechcianą korespondencję w sposób oszczędzający czas użytkownika. Wiadomości z zakwestionowaną zawartością są usuwane automatycznie lub pozostawiane do analizy. Większość pól nagłówkowych zdefiniowanych w standardzie SMTP (*ang. Simple Mail Transfer Protocol*) można weryfikować i autoryzować. Wyróżnić można dwa rodzaje tej techniki - weryfikacja (sprawdzana jest wiarygodność adresu nadawcy: jeżeli znajdująca się w adresie domena nie zostanie potwierdzona odpowiedzią z serwera DNS (*ang. Domain Name System*), to wiadomość taka jest uznawana za spam i powinna być odrzucona) i autoryzacja (polega na kontrolowaniu, z jakiej domeny lub adresu pochodzi odebrana przesyłka, i na tej podstawie decyduje się, czy ma być ona odebrana czy odrzucona). Wartym zauważenia mechanizmem walki ze spamem jest także tarpitting, który jest uaktywniany w momencie, gdy przesyłka nadchodzi z domeny lub adresu, który figuruje na liście generatorów spamów. Ponadto istnieje możliwość zastosowania filtrów, które analizują treść wiadomości, pod kątem wystąpienia odpowiednich łańcuchów znaków wskazujących, że jest to spam. Specyficznym rodzajem spamu jest tzw. phishing. W celu ograniczenia tego procederu wprowadzono standardy uwierzytelniające jak np. SPF (*ang. Sender Policy Framework*). Inną technologią pozwalającą na weryfikowanie autentyczności i integralności maili jest DKIM (*ang. Domain Key Identified Mail*), który definiuje strukturę uwierzytelniania poczty elektronicznej używającą kryptografii kluczy publicznych. Udostępnia weryfikację źródła treści informacji i ochronę tożsamości nadawcy informacji, a także integralność przekazywanej wiadomości, pozostawiając jednocześnie dotychczasową funkcjonalność poczty internetowej.

Jednym z istotnych problemów związanych z pocztą elektroniczną jest możliwość utraty poufności informacji przysyłanych w ten sposób. Środkiem zapobiegawczym jest szyfrowanie, które może zostać usprawnione poprzez zastosowanie bramowych rozwiązań szyfrujących, które zapewnią utrzymanie jednolitej polityki poufności korespondencji

elektronicznej. W łatwy sposób integrują się z dostępnymi systemami poczty elektronicznej oraz wykonują szyfrowanie w sposób przezroczysty dla użytkownika końcowego. Jak pokazuje rysunek 1 poczta wychodząca wysyłana jest do serwera bramowego w celu przetworzenia, zaś poczta przychodząca jest najpierw przetwarzana przez bramę, która ją deszyfruje, a rezultat przekazuje do systemu pocztowego.



Rys. 1. Bramowy system szyfrowania poczty elektronicznej.

Dla odbiorców dysponujących szyfrowaniem ze swojego punktu końcowego oferowane są dodatkowe mechanizmy, takie jak możliwość szyfrowania transportu wiadomości, a nie tylko samej wiadomości.

Podstawą skutecznej ochrony systemów wymiany wiadomości jest odporna na uszkodzenia infrastruktura. Najbardziej podatne na uszkodzenia elementy, takie jak: serwer, sieć, pamięć masowa, powinny mieć zapewnioną dostateczną redundancję. Nadmiarowa konfiguracja może uczynić usługi pocztowe mniej podatnymi na pojedyncze uszkodzenia. Metodą stosunkowo niedrogą jest magazynowanie danych na pamięciach dyskowych.

Szyfrowanie zapewnia poufność i prywatność zarówno w odniesieniu do plików utrzymywanych na serwerze czy też danych przesyłanych poprzez sieć. Stosowane są dwie podstawowe metody szyfrowania. W metodzie symetrycznej, ten sam tajny klucz jest wykorzystywany zarówno do szyfrowania jak i deszyfrowania wiadomości. Natomiast w szyfrowaniu asymetrycznym, zwanym także szyfrowaniem z kluczem jawnym, używa się pary kluczy, z których jeden jest tajny (prywatny) a drugi jawny (publiczny). Klucz publiczny jest ogólnie dostępny, zaś klucz prywatny jest znany tylko właścicielowi klucza i chroniony przed innymi użytkownikami. Któregokolwiek ze związanych ze sobą kluczy można użyć do szyfrowania, drugiego do deszyfrowania. Dzięki takiej konstrukcji każdy użytkownik może odszyfrować to, co zostało zaszyfrowane kluczem prywatnym. Jednocześnie tylko posiadacz klucza prywatnego może odszyfrować to, co ktokolwiek zaszyfrował jego kluczem publicznym.

Zagrożeniem dla procesu bezpiecznej wymiany dokumentów z zastosowaniem szyfrowania asymetrycznego jest możliwość zastąpienia klucza publicznego jednej z korespondujących stron kluczem publicznym intruza. Aby zapobiec takiej sytuacji, należy stworzyć mechanizm zwany procesem certyfikacji klucza, który potwierdzałby autentyczność używanego klucza i prawo do korzystania z niego przez daną osobę, firmę czy instytucję.

Rozwój kryptografii kluczy publicznych doprowadził do możliwości używania samej idei kluczy publicznych i prywatnych w innych obszarach ochrony informacji. Za przykład może posłużyć system RSA pozwalający na wymianę informacji tajnych i tworzenie podpisów cyfrowych. Podpis cyfrowy polega na dodawania unikatowych danych do dokumentu w taki sposób, że generować je może jedynie właściciel unikatowego klucza szyfrującego, ale każdy, kto posiada odpowiedni klucz deszyfrujący, może weryfikować autentyczność takiego podpisu. Strona odbierająca wiadomość z załączonym podpisem deszyfruje podpis kluczem publicznym (lub tajnym) w celu odtworzenia źródłowego abstraktu wiadomości, używa takiej samej funkcji haszującej i porównuje obie wartości - jeżeli są takie same, to podpis jest autentyczny, jeżeli nie, to wiadomość może pochodzić z innego źródła, niż podano, lub została po drodze zmieniona. Podpisy cyfrowe zapewniają autentyczność danych, ponieważ jakiekolwiek manipulowanie treścią wiadomości po jej podpisaniu unieważnia podpis. Zapewniają one również niezaprzeczalność źródła pochodzenia, ponieważ opierają się na niepowtarzalnym kluczu nadawcy.

Inną metodą kryptografii jest certyfikat cyfrowy, czyli elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowywane do określonej osoby i potwierdzają tożsamość tej osoby. Fizycznie jest to niewielki blok danych zawierający klucz publiczny użytkownika wraz z potwierdzeniem -w formie podpisu elektronicznego - jego autentyczności przez stronę trzecią, czyli wydawcę zapewnia infrastruktura klucza publicznegp - PKI (*ang. Public Key Infrastructure*).

Zapora sieciowa (firewall) jest jednym ze sposobów zabezpieczania sieci i systemów przed intruzami. Występować może w postaci sprzętowej lub programowej. Na zaporze można zdefiniować specjalna strefę zdemilitaryzowaną - DMZ (*ang. Demilitarized Zone*). Jest to podsieć, która izoluje od wewnętrznej sieci lokalne serwery udostępniające usługi na zewnątrz. W strefie zdemilitaryzowanej umieszczane są także te serwery usług świadczonych użytkownikom sieci wewnętrznej, które muszą kontaktować się z obszarem sieci zewnętrznej np. DNS, pocztowe, proxy. Stosowane są zapory na poziomie sieci, aplikacji czy analizujące stan połączenia.

Metoda filtrowania pakietów opiera się na kontroli pakietów wysyłanych oraz pobieranych przez konkretną sieć lokalną. Zapory pracujące na poziomie sieci są zazwyczaj routerami z zawansowanymi możliwościami filtrowania pakietów. Stosowane są także zapory sieciowe wykorzystujący aplikacje pośredniczące w standardowej komunikacji typu klient-serwer, zwane bramą proxy bądź bramą programową. Skuteczność działania zapór na poziomie aplikacji, oparta jest głównie na kontroli typu, a także objętości danych, które są wysyłane lub pobierane przez konkretną sieć lokalną. Ponieważ fizycznie rozgraniczają wewnętrzną sieć lokalną i sieć globalną efektywność działania tego typu zapór istotnie zwiększa jakość bezpieczeństwa.

Zapory analizujące stan połączenia potrafią przyporządkowywać pakiety do istniejących połączeń TCP i dzięki temu kontrolować całą transmisję. Systemy działające na poziomie transmisji nie wymagają specjalnych aplikacji typu klient obsługujących protokoły proxy. Tworzą na poziomie transmisji obwód łączący komputer-klient z serwerem i nie wymagają żadnej aplikacji do kontrolowania określonej usługi. Komputer-klient i serwer komunikują się ze sobą przez zaporę ogniową na poziomie transmisji.

Firewalle tego typu na bieżąco śledzą i analizują przechodzące przez nie połączenia, co pozwala na znacznie skuteczniejsze kontrolowanie ich zgodności z regułami. W związku z

tym określa się je mianem „dynamicznie filtrujących pakietów". Firewalle działające na poziomie transmisji, stanowią rozwiązanie kompromisowe pomiędzy szybkością filtrów pakietów, a bezpieczeństwem zapór poziomu aplikacji.

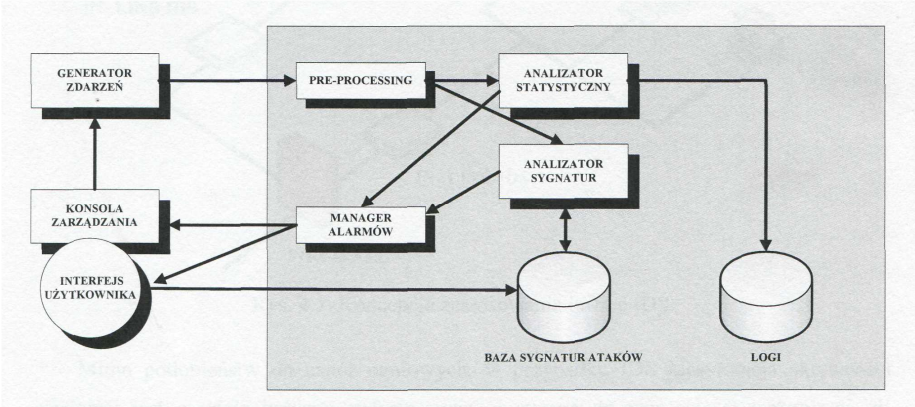
Zasilanie jest jednym z kluczowych czynników wpływających na prawidłowe działanie systemów teletransmisyjnych, a zarazem na bezpieczeństwo danych. Systemy zasilania gwarantowanego zabezpieczają przed przerwami zasilania oraz zakłóceniami (np. przepięcia). Składnikami takiego systemu są najczęściej zasilacze UPS oraz w miarę potrzeb: agregaty prądotwórcze, filtry, ograniczniki przepięć, wyłączniki różnicowoprądowe i inne urządzenia pomocnicze.

Zwiększenie niezawodności systemu zasilania uzyskuje się poprzez stosowania układów redundancyjnych UPS. W zależności od sposobu wzajemnej współpracy i stopnia zwielokrotnienia wyróżnia się układ kaskadowy, układ nadmiarowy N+1 oraz układ nadmiarowy 2N. Ważnym czynnikiem wpływającym na bezpieczeństwo zasilania jest stałe monitorowanie pracy urządzeń wchodzących w skład systemu oraz zapewnienie wzajemnej komunikacji z pozostałymi systemami zarządzania znajdującymi się w jego otoczeniu. Dostępne zasilacze UPS umożliwiają połączenia logiczne poprzez łącze szeregowe i są wyposażona w specjalne oprogramowanie pozwalające na monitorowania parametrów zasilacza i zasilania (np. wartości napięcia i obciążenia, czasu pracy z baterii).

Jednym z najbardziej rozpowszechnionych zagrożeń dla sieci teleinformatycznych są wirusy komputerowe, których rozprzestrzenianie odbywa się za pośrednictwem użytkowego oprogramowania. Wymienić można następujące rodzaje zabezpieczeń antywirusowych: skanery, monitory, szczepionki, programy zliczające sumy kontrolne, programy auto weryfikujące. W środowisku sieciowym przedsiębiorstwa istnieje możliwość zainfekowania dużej liczby jednostek w krótkim czasie. Dlatego też w takim otoczeniu stosowane są często bramy antywirusowe, które np. kontrolują przychodzące załączniki poczty elektronicznej i odrzucają te, które zawierają podejrzaną zawartość. Inną skuteczną metodą ochrony jest skanowanie dopiero w momencie dostępu.

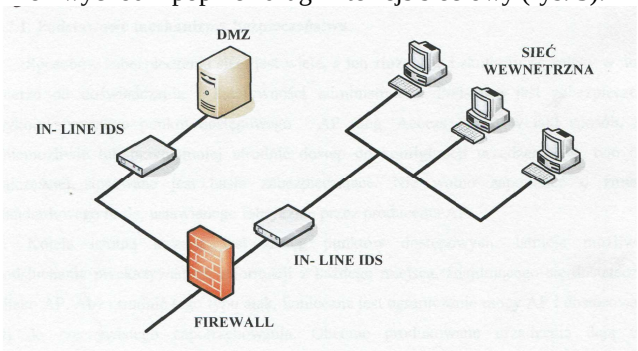
Wczesne wykrywanie i eliminowanie zagrożeń zapewniają skanery zabezpieczeń oraz systemy wykrywania intruzów - IDS (*ang. Intrusion Detection System*). Systemy IDS na podstawie analizy ruchu sieciowego identyfikują podejrzane i niedozwolone działania takie jak: próby penetracji, ataki destrukcyjne. Niektóre rozwiązania oparte o algorytmy heurystyczne, posiadają zdolność automatycznego dostosowywania się do specyfiki danej sieci. Wyróżnia się trzy podstawowe rodzaje systemów IDS: systemowy - Host IDS (umieszczany na serwerach, wykrywa wszystkie możliwe próby naruszenia bezpieczeństwa), sieciowy - Network IDS (analizuje dane pochodzące z wybranego segmentu sieci) oraz stacji sieciowej - Network Node IDS (wykorzystywane, gdy zachodzi konieczność analizy ruchu szyfrowanego). Schemat standardowego systemu IDS przedstawiono na rys. 2.

Podstawowymi technikami wykrywania ataków stosowane w systemach IDS są sygnatury, badanie częstości zdarzeń i przekraczania pewnych limitów w określonej jednostce czasu oraz wykrywanie anomalii statystycznych. Klasyczne systemy IDS są narzędziami pasywnymi, wykrywają potencjalne ataki, a reakcja najczęściej leży w gestii administratora, poza tym muszą być optymalnie skonfigurowane aby nie generowały zbyt często fałszywych alarmów. Wymienione wady eliminują rozwiązania IPS - Intrusion Prevention Systems. Są to systemy IDS rozbudowane o możliwości aktywnej reakcji na wykryte zdarzenia.



Rys. 2. Schemat standardowego systemu IDS

Do takiej grupy zalicza się tzw. in-line IDS, które mają architekturę zbliżoną do firewall. Ruch sieciowy wchodzi do urządzenia IDS jednym interfejsem, jest wewnątrz poddawany analizie i wychodzi poprzez drugi interfejs sieciowy (rys. 3).



Rys. 3. Koncepcja zastosowania in-line IDS.

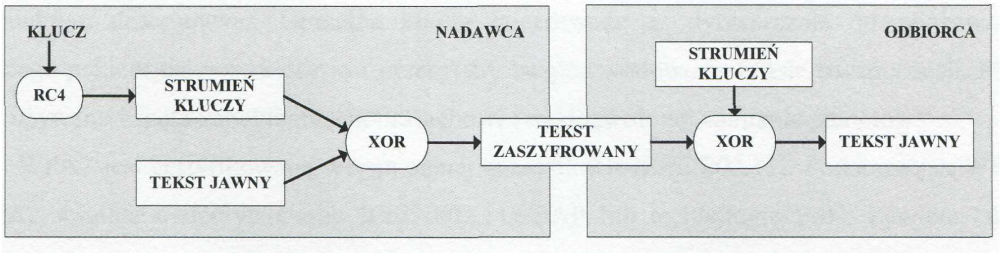
Mimo podobieństw do zapór ogniowych, w przypadku IDS klasyfikacja aktywności sieciowej jest o wiele bardziej zaawansowana i stosuje do tego więcej technologii. W znacznym uproszczeniu systemy IDS działają na podstawie dopasowywania sygnatur ataków. IDS-y stosują wiele różnych technik detekcji prób ataku. np. normalizatory i interpretery poszczególnych protokołów, sygnatury opisowe w miejsce konkretnych wzorców oraz metody heurystyczne [2].

Złożoność i skuteczność sposobów zabezpieczenia sieci zależy w dużej mierze od doświadczenia i kreatywności administratora. Podstawą jest zabezpieczenie wykorzystywanego punktu dostępowego - AP (*ang. Access Point*) w taki sposób, aby uniemożliwić lub przynajmniej utrudnić dostęp do konfiguracji urządzenia. W tym celu najczęściej stosowane jest hasło zabezpieczające. Kolejną istotną kwestią jest zasięg punktów dostępowych. Istnieje możliwość podsłuchania przekazywanych informacji z każdego miejsca, znajdującego się dostatecznie blisko AP. Aby utrudnić tego typu atak,

konieczne jest ograniczenie mocy AP i dostosowanie jej do rzeczywistego zapotrzebowania. Obecnie produkowane urządzenia dają taką możliwość.

Powszechnie stosowaną praktyką jest wyłączenie rozgłaszania przez AP nazwy sieci tzw. SSID (*ang. Service Set IDentifier*). SSID pełni rolę hasła, gdyż każdy użytkownik chcący się podłączyć do AP musi znać nazwę sieci. Innym typowym zabezpieczeniem, jest tzw. filtracja adresów MAC (*ang. Medium Access Control*). Technika ta sprowadza się do przechowywania w urządzeniu dostępowym informacji o adresach MAC kart sieciowych, które mogą legalnie łączyć się z siecią. Przy próbie połączenia, AP sprawdza czy adres MAC karty sieciowej podłączającego się klienta znajduje się na liście adresów uprawionych. Jeśli tak, klient uzyskuje dostęp do sieci.

Z uwagi na fakt, że transmisja bezprzewodowa jest łatwiejsza do przechwycenia niż transmisja w sieci przewodowej, stworzono protokół WEP (*ang. Wired Equivalent Privacy*), który podnosi bezpieczeństwo transmisji. Do szyfrowania i deszyfrowania stosowany jest ten sam klucz. Protokół bazuje na algorytmie szyfrującym RC4, który na podstawie klucza WEP (40 lub 104 bitowego) oraz 24 bitowego wektora inicjalizacyjnego generuje nieskończony pseudolosowy strumień kluczy, używany do szyfrowania tekstu jawnego oraz jego sumy kontrolnej. Szyfrowanie odbywa się poprzez użycie funkcji XOR na strumieniu kluczy oraz katenacji tekstu jawnego i jego sumy kontrolnej. Tak zaszyfrowana wiadomość z dołączonym wektorem inicjalizacyjnym przesyłana jest przez sieć. Odbiorca na podstawie wektora incjalizacyjnego dołączonego do wiadomości oraz klucza generuje strumień kluczy i dzięki własności operacji XOR odszyfrowuje wiadomość (rys. 4.).



Rys. 4. Schemat szyfrowania w protokole WEP

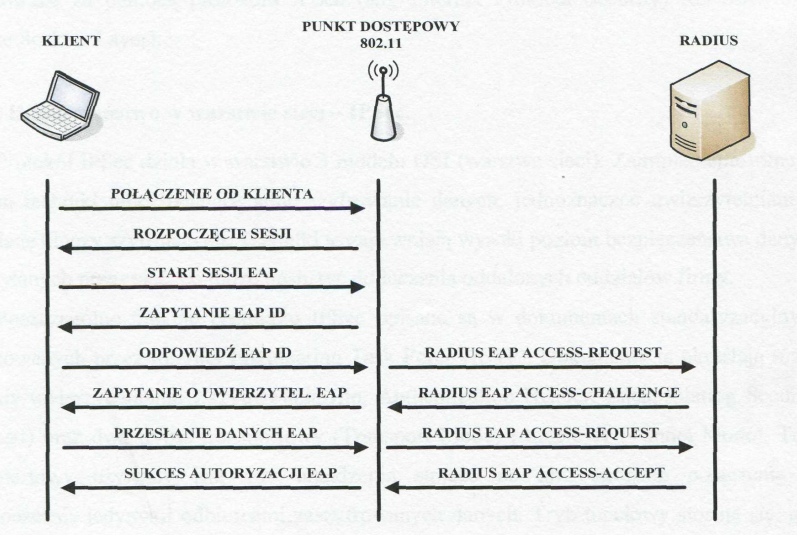
Słabością protokołu WEP jest wektor inicjalizacyjny. Przy zastosowaniu odpowiedniego oprogramowania osoba atakująca może monitorować sieć. Przy zgromadzeniu dostatecznej ilości ramek istnieje duże prawdopodobieństwo kolizji, czyli powtórzenia. Jedynym sposobem zapobiegnięcia kolizjom jest bardzo częsta zmiana klucza WEP. Dodatkowym problemem jest brak zdefiniowanego przez standard sposobu generowania wektorów inicjalizacyjnych.

Odpowiedzią na niedoskonałości WEP jest standard WPA (*ang. WiFi Protected Access*). WPA przewyższa starsze rozwiązanie silniejszym szyfrowaniem TKIP (*ang. Temporary Key Integrity Protocol*) oraz technologią MIC (*ang. Message Integrity Check*), dostarcza także odpowiedniego schematu uwierzytelnienia IEEE 802.1x/EAP (*ang. Extensible Authentication Protocol*) oraz wspiera technologię PSK (*ang. Pre-Shared Key*) [3]. Wyróżnia się dwa rodzaje WPA: Personal (opiera się na kluczu PSK długość od 8 do

63 znaków, bez którego nie jest możliwe połączenie z siecią) oraz Enterprise (korzystający z serwera RADIUS).

WPA2 jest certyfikowaną wersją pełnej specyfikacji IEEE 802.11i. Podobnie jak WPA, WPA2 wspiera uwierzytelnianie IEEE 802.11x/EAP lub technologię PSK. Zawiera także nowy zaawansowany mechanizm szyfrowania używający Counter-Mode/CBC-MAC Protocol (CCMP), nazywany AES (*ang. Advanced Encryption Standard*). CCMP jest nowym trybem operacji na bloku cyfr, która używa pojedynczego klucza zarówno do szyfrowania, jak i uwierzytelniania. CCMP posiada tryb Counter (CTR), do zapamiętywania szyfrowanych danych, i CBC-MAC (*ang. Cipher Błock Chaining Message Authentication Code*) do sprawdzania integralności danych. Wobec nieskuteczności powszechnych zabezpieczeń takich jak WEP czy listy dostępowe MAC, rozwiązaniem jest wprowadzenie ulepszonych metod uwierzytelniania oraz szyfrowania, co zapewnia WPA/WPA2.

RADIUS (*ang. Remote Authentication Dial-In User Service*) jest powszechnie stosowanym protokołem, umożliwiającym centralne uwierzytelnienie oraz ewidencjonowanie dostępu sieciowego[3]. Komunikaty RADIUS są przesyłane za pomocą protokołu UDP (*ang. User Datagram Protocol*). Przykład typowej sesji przedstawia rys. 5.



Rys. 5. Sesja uwierzytelniająca z wykorzystaniem serwera RADIUS.

Wirtualne sieci prywatne VPN zapewniają trzy elementy bezpieczeństwa transmisji danych: uwierzytelnianie, poufność oraz integralność. Jeśli połączenie VPN ma swój początek i koniec w sieci firmowej, może być realizowane za pomocą protokołu IPSec (*ang. Internet Protocol Security*) lub SSL (*ang. Secure Sockets Layer*).

Protokół IPSec działa w warstwie 3 modelu OSI (warstwa sieci). Zaimplementowane są w nim techniki umożliwiające silne szyfrowanie danych, jednoznaczne uwierzytelnianie i wymianę kluczy szyfrujących. Techniki te zapewniają wysoki poziom bezpieczeństwa

[3] RFC2865 (*Remote Authentication Dial-In User Services*) oraz RFC2866 (*RADIUS Accounting*).

danych przesyłanych przez sieć, co może posłużyć do łączenia oddalonych oddziałów firmy. Poszczególne funkcje protokołu IPSec opisane są w dokumentach standaryzacyjnych, które określają różne metody uwierzytelniania i szyfrowania (np. Authentication Header, Encapsulating Security Payload) oraz dwa tryby: transportowy (Transport Mode, urządzenia stojące po obu stronach połączenia są równocześnie jedynymi odbiorcami zaszyfrowanych danych) i tunelowy (Tunnel Mode, urządzenia realizujące połączenie VPN nie są ostatecznymi odbiorcami przesyłanych danych).

Wymiana kluczy, za pomocą których realizowane jest szyfrowanie połączenia IPSec odbywa się z użyciem protokołu IKE (*ang. Internet Key Exchange*), który umożliwia elastyczne zarządzania kluczami. IPSec znajduje również zastosowanie w połączeniu z technologiami bezprzewodowymi WLAN.

Protokół SSL zapewnia zdalny dostęp do aplikacji i danych za pośrednictwem przeglądarki internetowej. W takim rozwiązaniu kluczowym staje się usprawnienie uwierzytelniania HTTP, które zezwala na wielokrotne używanie danych wymaganych do logowania. Standard TLS (*ang. Transport Layer Security*) jest rozwinięciem SSL.

Podstawowy model SSL w architekturze klient/serwer umożliwia dostęp nieograniczonej liczbie systemów zdalnych, jednak taki model wymusza zastosowanie funkcji proxy na poziomie bramy SSL.

IPSec wykorzystuje połączenia tunelowe dla zapewnienia bezpiecznej transmisji danych, przy czym rodzaj tych danych nie jest istotny. SSL weryfikuje czy dany użytkownik ma odpowiednie prawa dostępu do konkretnej aplikacji. Sieci prywatne oparte na SSL muszą oferować mechanizmy monitorowania i kontroli praw dostępu.

4. BEZPIECZNY STYK SIECI TELETRANSMISYJNEJ PRZEDSIĘBIORSTWA TRANSPORTOWEGO Z INTERNETEM

Rozwiązania internetowe są wykorzystywane wewnętrznie w firmach oraz w ramach współpracy z partnerami i klientami. Technologie internetowe umożliwiają znaczne obniżenie kosztów i czasu przepływu informacji. Mimo niewątpliwych korzyści problemem jest wybór odpowiednich rozwiązań i integracja ich w jeden spójny system ochronny.

Jedną z podstawowych zasad bezpieczeństwa jest zasada minimalnych uprawnień, która polega na tym, ze osoby korzystające z systemu powinni dysponować tylko takim zakresem przywilejów, który zezwoli im na wykonywanie przydzielonych zadań. Inna zasadą jest tzw. dogłębna obrona, według której należy stosować więcej niż jeden mechanizm obrony przed atakiem. Zastosowanie większej ilości urządzeń uzupełniających i wspierających wzajemnie swoją funkcjonalność znacznie poprawia poziom bezpieczeństwa. Poza tym nadmiarowość i warstwowa struktura elementów bezpieczeństwa zmniejsza prawdopodobieństwo skutecznego ataku w przypadku awarii któregoś z nich. W ścisłym związku z powyższą strategią jest stosowanie zróżnicowanej obrony. Z uwagi na fakt, że systemy tego samego rodzaju posiadają te same wady, powinno stosować się nie tylko wiele poziomów zabezpieczeń, ale i zróżnicowane środki ochronne.

Fundamentalną teorią bezpieczeństwa jest zasada najsłabszego ogniwa. Każdy system zabezpieczeń ma słaby punkt, który napastnik będzie starał się odnaleźć i wykorzystać. Jeśli eliminacja słabych punktów obrony nie jest możliwa, należy na ich kontroli skupić szczególną uwagę. Najsłabsze ogniwo w całości rozwiązania z zakresu bezpieczeństwa

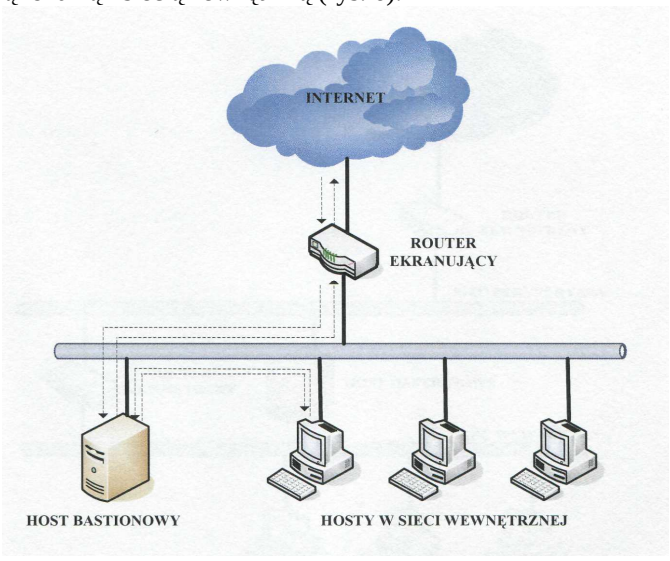
decyduje o ogólnym poziomie bezpieczeństwa, trzeba więc sprawić by było wystarczająco silne, proporcjonalnie do ryzyka.

Zasada zabezpieczenia poprzez utajnianie, polega na ograniczaniu informacji o systemie i sposobach jego działania. Niecelowe jest udostępnianie postronnym osobom informacji o zastosowanych technologiach, sposobach konfiguracji urządzeń zabezpieczających, co na pewno utrudni to ewentualny atak.

Infrastruktura sieciowa na styku sieci firmowej z Internetem powinna zapewniać bezpieczeństwo, wydajność, skalowalność i niezawodność. Z uwagi na fakt, że pojedyncze rozwiązania mogą nie zagwarantować satysfakcjonującego poziomu bezpieczeństwa, należy rozważyć wykorzystanie dostępnych technologii ochrony danych, takich jak: kontrola dostępu i tożsamości, wykrywanie ataków, weryfikacja autentyczności.

Podczas planowania systemu separującego sieć instytucji od Internetu, należy opracować odpowiednią architekturę systemu oraz wybrać takie oprogramowanie i sprzęt, które umożliwią wdrożenie przyjętej strategii ochrony. Najprostszym i najłatwiejszym do wdrożenia jest pojedynczy obiekt (*ang. single-box architecture*), w którym skupione są mechanizmy bezpieczeństwa. Z uwagi na ograniczenia wydajnościowe, stosowanie tej metody ochrony jest uzasadnione w przypadku nierozbudowanej infrastruktury sieciowej (np. zastosowanie routera ekranującego). Jako pojedynczy obiekt można zastosować hosta, posiadającego dwa interfejsy sieciowe i spełniającego rolę routera, pomiędzy tymi interfejsami.

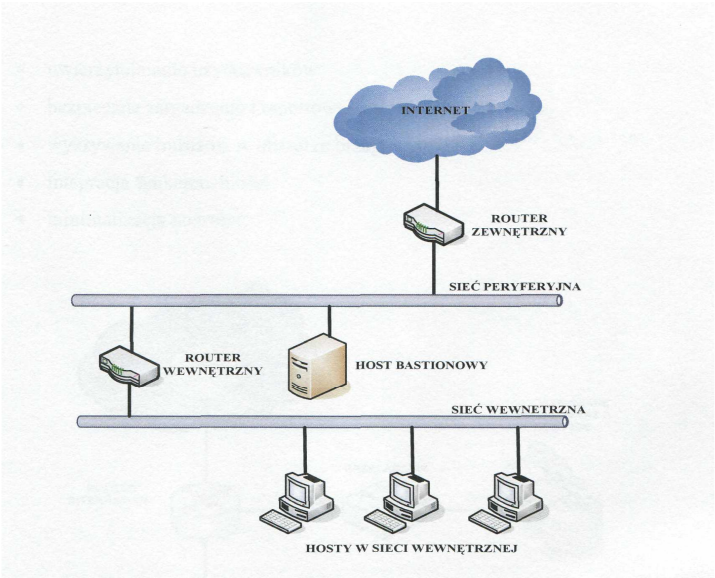
System zaporowy o architekturze ekranowanego hosta składa się z routera ekranującego (*ang. screening router*) oraz dedykowanej maszyny, określanej mianem hosta bastionowego (*ang. bastion host*). Oba komponenty są ze sobą ściśle zsynchronizowane. Router ekranujący jest wyposażony w mechanizm filtracji pakietów, który stanowi pierwszą linię ochrony i zapewnia, aby wszystkie przesyłane pakiety przechodziły przez host bastionowy tak, aby ten mógł kontrolować całość komunikacji sieciowej prowadzonej pomiędzy siecią lokalną i siecią zewnętrzną (rys. 6).



Rys. 6. Architektura ekranowanego hosta

Konfiguracja routera ekranującego, może pozwalać na nawiązywanie połączeń z lokalnej sieci z hostami w sieci zewnętrznej udostępniającymi wybrane usługi lub wymuszać stosowanie do tego celu wyłącznie pośrednictwa hosta bastionowego. Polityka bezpieczeństwa określa jakie typy usług i sposoby komunikacji będą dozwolone.

Najbardziej złożoną strukturę posiada architektura ekranowanej podsieci, która jest rozszerzeniem koncepcji ekranowanego hosta. Zakłada ona stworzenie oddzielnego segmentu sieci dla hosta bastionowego, umieszczonego pomiędzy siecią lokalną i siecią zewnętrzną (rys. 7). Ekranowana podsieć stanowi dodatkową fizyczną warstwę zabezpieczeń systemu, która ma za zadanie szczelnie odizolować sieć prywatną od świata zewnętrznego.



Rys. 7. Architektura ekranowanej podsieci.

Zaletą przedstawionego na rysunku 7 rozwiązania z dwoma routerami ekranującymi, podłączonymi do sieci peryferyjnej, jest to, iż w przypadku przeprowadzenia pomyślnej próby włamania na hosta bastionowego, intruz nie uzyskuje dostępu do sieci prywatnej ponieważ znajduje się w innej sieci fizycznej. Dodatkowo, zewnętrzna podsieć systemu może zostać wykorzystana do instalacji serwerów, które świadczą usługi na zewnątrz organizacji np. WWW, FTP.

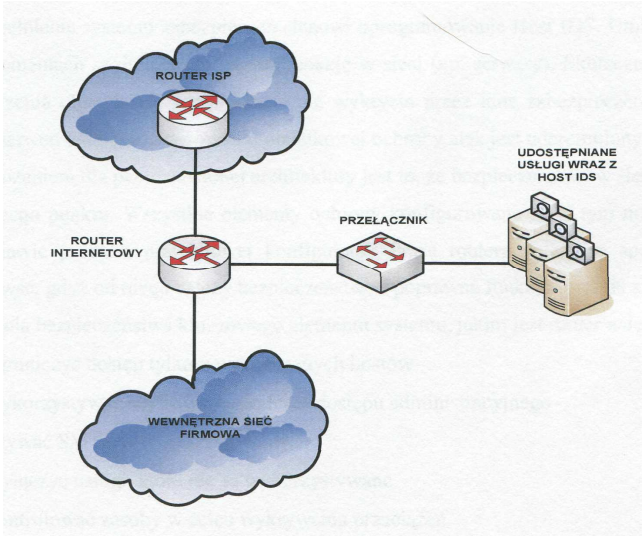
5. PRZYKŁAD ZABEZPIECZONEGO POŁĄCZENIA SIECI FIRMOWEJ Z INTERNETEM

Przykładową implementację uwzględniono dla małej sieci oraz dla sieci rozbudowanej. Rozwiązania sprzętowo-programowe oparto na technologii firmy Cisco.

Dla niewielkiej sieci, w której pracuje kilkudziesięciu użytkowników, najbardziej odpowiednim wydaje się rozwiązanie z integracją funkcji.

Pierwszą linię ochrony w konfiguracji zapewnia router operatora (ISP) – rys. 8. Podstawowa filtracja zapobiega podmianie źródłowych adresów IP (tzw. spoofing), a

konfigurowalne limity zabezpieczają łącze przed nadmiernym wykorzystaniem (flooding). Router na styku z siecią Internet pełni rolę firewalla, sondy IPS oraz może realizować połączenia VPN. W odróżnieniu od routera ISP, filtracja może być prowadzona w trybie stateful. Poza tym zapewniona jest ochrona przed atakami DoS (*ang. Denial of Service*) oraz istnieje możliwość zastosowania translacji adresów sieciowych - NAT (*ang. Network Addres Translation*). Terminacja tunelu VPN pozwala na tworzenie bezpiecznych połączeń szyfrowanych poprzez sieć Internet, zarówno dla użytkowników mobilnych, jak i innych oddziałów firmy. W tym punkcie przeprowadzana jest pierwsza autoryzacja użytkowników chcących uzyskać dostęp do zasobów wewnętrznych.



Rys. 8. Schemat połączenia z Internetem sieci filii przedsiębiorstwa.

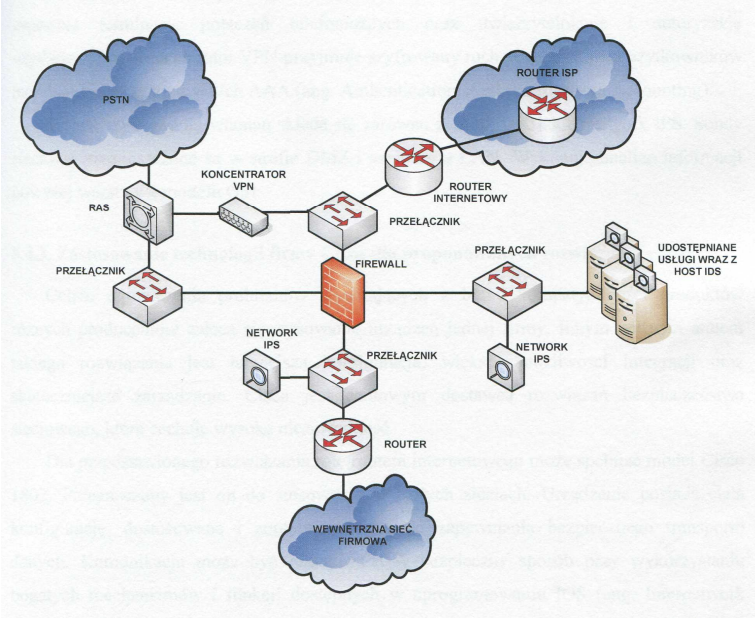
Przełączniki w strefie udostępniającej usługi dla zewnętrznych użytkowników, powinny być skonfigurowane w sposób uniemożliwiający przenikanie pomiędzy zasobami wewnętrznymi. Funkcjonalność Private VLAN, pozawala na określenie, które urządzenia mogą komunikować się ze sobą bezpośrednio. Uzupełnienie systemu zabezpieczeń stanowi oprogramowanie Host IDS. Umiejscowione jest na elementach spełniających istotną funkcję w sieci (np. serwery). Skuteczność takiego zabezpieczenia objawia się w momencie nie wykrycia przez inne zabezpieczenia sieciowe ataku na serwer, a dzięki zastosowaniu dodatkowej ochrony atak jest udaremniony.

Zagrożeniem dla przedstawionej architektury jest to, że bezpieczeństwo w sieci zależy od pojedynczego punktu. Wszystkie elementy ochrony konfigurowane są w tym miejscu, więc może się pojawić problem prawidłowej konfiguracji. Pracę routera należy w sposób ciągły monitorować, gdyż od niego zależy bezpieczeństwo i poprawne funkcjonowanie sieci.

Podczas budowy styku z Internetem rozbudowanej sieci przedsiębiorstwa zastosowanie zcentralizowanej formy ochrony okazuje się nieefektywne. Duża liczba obsługiwanych użytkowników zwiększa wymagania dotyczące wydajności routera, a reguły wymiany informacji pomiędzy licznymi hostami powodują złożoność konfiguracji. Dlatego też

sposobem na wymienione problemy jest zastosowanie architektury z dystrybucją zadań. Funkcje takie jak: trasowanie połączeń, filtrowanie pakietów, dostęp zdalny są realizowane przez dedykowane urządzenia (rys. 9).

Podstawą zaletą przedstawionej architektury jest brak jednego punktu przełamania systemu ochrony. Mimo, że poszczególne elementy systemu wykonują różne funkcje, to przełamanie któregokolwiek z nich nie powoduje uzyskanie nieograniczonego dostępu do sieci wewnętrznej.



Rys. 9. Schemat połączeń w warstwie brzegowej sieci centrali firmy

Podobnie w przypadku rozwiązania z integracją funkcji w jednym punkcie router operatora ISP, zapewnia podstawową ochronę przed spoofingiem i floodingiem. Router internetowy w przedsiębiorstwie nie skupia w sobie już wielu zadań. Jego rola sprowadza się do prostego filtrowania pakietów.

Zapora sieciowa jest realizowana przez dedykowane urządzenie, które prowadzi analizę ruchu sieciowego w trybie stateful oraz prostą analizę przesyłanych informacji powyżej warstwy 4 modelu OSI. Ponadto firewall chroni hosty przed atakami DoS. Przez zaporę przepływa ruch ze wszystkich segmentów sieci: internetowego, LAN, strefy zdemilitaryzowanej oraz zdalnego dostępu.

W części obsługującej dostęp zdalny, urządzenie RAS (*ang. Remote Access Server*) zapewnia terminację połączeń telefonicznych oraz uwierzytelnianie i autoryzację użytkowników. Koncentrator VPN przyjmuje szyfrowany ruch pochodzący od użytkowników mobilnych oraz umożliwia ich AAA (*ang. Authentication, Authorisation and Accounting*). System wykrywania włamań składa się zarówno z Host IDS, jak i Network IPS. Sondy sieciowe rozmieszczone są w strefie DMZ i segmencie LAN. Wykonują analizę informacji powyżej warstwy 4 modelu OSI.

Celem ograniczenia problemów wynikających z braku kompatybilności produktów różnych producentów zaleca się stosowanie urządzeń jednej firmy. Innym ważnym atutem takiego rozwiązania jest łatwiejsza konfiguracja, większe możliwości integracji oraz skuteczniejsze zarządzanie. Cisco jest czołowym dostawcą rozwiązań bezpieczeństwa sieciowego, które cechuje wysoka niezawodność.

Dla przedstawionego rozwiązania rolę routera internetowego może spełniać model Cisco 1802, przeznaczony do stosowania w małych sieciach. Urządzenie posiada stałą konfigurację, dostosowaną i zoptymalizowaną do zapewniania bezpiecznego transportu danych. Router 1802 wyposażono w porty WAN: ADSL dla ISDN i 10/100FE, a także zapasowy ISDN BRI S/T. Posiada również opcję AP 802.11 a/b/g. Zintegrowanie wielu funkcji sieciowych w jednym urządzeniu (routera z zapasowym połączeniem, przełącznika LAN, firewall-a, VPN, IPS, access point WLAN), przyczynia się do znacznej redukcji kosztów związanych z ich zakupem i późniejszą obsługą. Wydajny procesor pozwala na obsługę szerokopasmowego dostępu z włączonymi mechanizmami zapewniającymi bezpieczeństwo i poufność transmisji. Instalacja i konfiguracja urządzenia, dzięki dodatkowym narzędziom, jest wygodna i przejrzysta, a do tego możliwa z poziomu interfejsu WWW. Dla większych sieci, posiadających powyżej 100 węzłów rolę routera dostępowego, może pełnić urządzenie Cisco 2801. Rozwiązanie zostało zaprojektowane specjalnie dla zapewnienia szybkiej i bezpiecznej transmisji danych (w tym głosu).

Rolę przełączników mogą spełniać switche Catalyst 2950. W małych sieciach częstym zastosowaniem jest umieszczenie ich przy obsłudze farm serwerów, natomiast w rozbudowanych architekturach, pełnią zadania typowe dla urządzeń dostępu. W przełączniki Catalyst 2950 zaimplementowano wiele funkcji zapewniających zwiększenie bezpieczeństwa danych. Bezpieczeństwo sieci na poziomie portów zbudowane w oparciu o adresy MAC zapobiega dostępowi nieupoważnionych stacji do przełącznika - funkcja Port Security. Private VLAN izoluje porty przełącznika, zapewniając przepływ ruchu bezpośrednio od punktu wejściowego do urządzenia agregacyjnego przy użyciu ścieżki wirtualnej i uniemożliwiając skierowanie tego ruchu do innego portu. Wielopoziomowe bezpieczeństwo dostępu w konsoli przełącznika oraz w internetowym interfejsie zarządzania chroni przed dostępem nieupoważnionych użytkowników do sieci oraz przed zmianą konfiguracji i może być implementowane przy użyciu wewnętrznej bazy danych użytkowników dla każdego przełącznika lub za pomocą centralnie zarządzanego serwera (np. RADIUS).

Cisco PIX 515E jest dedykowanym rozwiązaniem sprzętowym spełniającym funkcję zapory sieciowej. Firewall Cisco PIX wyposażony jest w nowoczesny algorytm bezpieczeństwa Cisco ASA (*ang. Adaptive Security Algorithm*), który zapewnia obfity zestaw usług kontroli sesji, śledzących stan wszystkich autoryzowanych połączeń i zapobiegających nieuprawnionemu dostępowi do sieci. Dodatkową warstwę bezpieczeństwa tworzą specjalizowane moduły kontrolne, realizujące inspekcję ruchu w warstwach 4-7 dla popularnych aplikacji i protokołów. Własne założenia polityki bezpieczeństwa, można wdrożyć wykorzystując różne techniki kontroli dostępu np. grupy obiektów sieciowych/usługowych, akcelerowane listy kontroli dostępu (ACL), założenia bazujące na charakterze użytkownika/grupy oraz ponad 100 standardowo zdefiniowanych aplikacji i protokołów. Dzięki wielu funkcjom zabezpieczającym przed włamaniem, takim jak DNSGuard, FloodGuard, FragGuard, MailGuard, IP verify i przechwytywania sesji TCP, jak również wykrywaniu 55 innych sygnatur ataków, ściana ogniowa Cisco PIX

chroni przed atakami i może je opcjonalnie zablokować oraz powiadamiać o nich na bieżąco administratora. Cisco PIX 515E oferuje również wykorzystanie możliwości VPN, dzięki zastosowaniu standardów internetowej wymiany kluczy (IKE) oraz IPSec. Szyfrowanie może być zastosowane z wykorzystaniem algorytmów DES lub AES.

Seria Cisco 42xx IPS umożliwia wykrywanie i zatrzymywanie zagrożeń takich jak robaki, programy spyware/adware, wirusy, a także niedozwolone używanie dostępnych aplikacji. Oprogramowanie IPS 5.0 wspiera tryb hybrydowy tzn. jedna sprzętowa sonda może jednocześnie działać jako IDS sensor i IPS sensor obsługując kilka stref bezpieczeństwa. Daje to możliwość elastycznego stosowania oraz oszczędność kosztów. Moduły do przełączników posiadają tę samą funkcjonalność co sondy, różnica polega na tym, że nie posiadają fizycznych interfejsów, ale dołączone są do magistrali switcha.

Programy Host IDS instalowane są na chronionych komputerach i analizują komunikację między wybranymi procesami, sprawdzają integralność kluczowych plików systemowych, analizują logi. Ich zaletą jest możliwość wykrywania nietypowych zachowań niezależnie od pierwotnego źródła pochodzenia, najczęściej spotykaną wadą jest skomplikowany proces konfiguracji.

Głównym zadaniem koncentratorów firmy Cisco (VPN 3000 Concentrators) jest pełna obsługa zdalnego dostępu. Urządzenia te pozwalają w prosty sposób wdrożyć, skonfigurować i monitorować usługę zdalnego dostępu w wirtualnych sieci prywatnych. Istotną cechą jest skalowalność tych koncentratorów, a także współpraca różnymi typami klientów VPN. Wydajność urządzenia jest zwiększona dzięki karcie sprzętowego wsparcia szyfrowania (AES).

W celu zapewnienia ochrony sieci, zabezpieczenia powinny funkcjonować w kluczowych obszarach: tożsamości, stref bezpieczeństwa, bezpiecznych połączeń, monitorowania bezpieczeństwa i zarządzania zasadami bezpieczeństwa. Cisco wspiera proaktywne działanie umożliwiające kontrolę poziomu zabezpieczeń sieci i aplikacji. Architektura Cisco Self-Defending Network to wieloetapowa inicjatywa mająca na celu radykalną poprawę zdolności sieci do zapobiegania, wykrywania i ochrony przed potencjalnymi zagrożeniami. Architektura ta umożliwia samoadaptacje sieci do zmieniających się warunków brzegowych związanych z potencjalnymi zagrożeniami.

6. WNIOSKI

Systemy informatyczne mają strategiczne znaczenie dla działalności firmy i z tego powodu powinny być odpowiednio zabezpieczone. Każdy użytkownik powinien chronić własne zasoby przed niepowołanym dostępem z zewnątrz. Zagadnienia bezpieczeństwa na styku z Internetem nabierają innego wymiaru, jeśli firma decyduje się prowadzić przez sieć swoje interesy.

Wnikliwie przeprowadzona analiza ryzyka pozwala na wskazanie obszarów, w których należy zastosować zabezpieczenia. Nie wszystkie punkty infrastruktury sieciowej, wymagają wdrożenia skomplikowanych zabezpieczeń. W niektórych przypadkach dodatkowe elementy ochrony muszą realizować tylko podstawową funkcjonalność, a w innych nie jest wymagane wdrożenie mechanizmów zabezpieczających. Ważne jest zachowanie równowagi pomiędzy kosztem wdrożenia zabezpieczeń, a wartością chronionych zasobów oraz ewentualnymi następstwami ich utraty.

W artykule przedstawiono propozycję bezpiecznego połączenia sieci przedsiębiorstwa z Internetem. Dla mniejszej sieci rozwiązaniem optymalnym jest zastosowanie urządzenia

integrującego kilka funkcji, zaś dla bardziej rozbudowanej sieci należy rozważyć dystrybucję zadań pomiędzy różne urządzenia.

Mimo zwiększania poziomu bezpieczeństwa systemów teleinformatycznych, nie jest możliwe całkowite wyeliminowanie ryzyka. Stosując zabezpieczenia o różnym charakterze: fizycznym, organizacyjnym i technicznym, zmniejsza się tylko ryzyko do pewnego akceptowalnego poziomu.

7. BIBLIOGRAFIA

[1] Drzycimski Z.: *Możliwości technologiczne pozyskiwania i modyfikacji informacji w sieciach telekomunikacyjnych i teleinformatycznych* [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce* pod red. B. Lenta, Biblioteka „Bezpieczeństwa Narodowego", tom 3, Warszawa 2007.

[2] Dworakowski W.: *Najnowsze trendy w dziedzinie zabezpieczeń sieci informatycznych*, IX Konferencja PLOUG, Kościelisko, październik 2003

[3] Folga K.: *Jak uwierzytelnić bezprzewodowego użytkownika*, Networld nr 5/2006.

[4] *Info Guard: Risks and Dangers of Fiber Optic Cables*, 2004.

[5] Kula S.: *Systemy teletransmisyjne*, Wydawnictwo Komunikacji i Łączności, Warszawa 2005.

[6] Norscan Instruments Limited: Fiber Optic Intrusion Detection Systems,*2003*.