PRZEGLĄD ELEKTROTECHNICZNY

Ukazuje się od 1919 roku 3'14

Organ Stowarzyszenia Elektryków Polskich • Wydawnictwo SIGMA-NOT Sp. z o.o.

Michał SZEWCZYK

Politechnika Śląska, Instytut Elektroenergetyki i Sterowania Układów

Wybrane analizy pracy struktur teletransmisyjnych i teleinformatycznych w elektroenergetyce

Streszczenie. *W artykule zostaną zaprezentowane wybrane analizy problemowe funkcjonowania struktur teletransmisyjnych i teleinformatycznych we współczesnej infrastrukturze elektroenergetyki. W sposób szczególny zwrócono uwagę na elementy bezpieczeństwa pracy takich sieci i ich podatności na ataki wynikające z konwergencji usług teleinformatycznych.*

Abstract*. The paper will present selected analyses of issues related to the functioning of the teletransmission and teleinformatic structures in today's electric power infrastructure. In particular, special attention is paid to the safety of such networks and their vulnerability to the attacks resulting from the convergence of ICT services. (**Selected analyses of teletransmission and teleinformatic structures in electrical power**).*

Słowa kluczowe: sieci teletransmisyjne, systemy teleinformatyczne, system elektroenergetyczny, bezpieczeństwo pracy systemów teleinformatycznych.
Keywords: teletransmission, teleinformatics, electrical power system, safety of teleinformatics systems

doi:10.12915/pe.2014.03.01

Wstęp

Komputery i sieci teletransmisyjne pełnią w systemie elektroenergetycznym różne zadania. Znalazły zastosowanie w automatyce zabezpieczeniowej, w systemach sterowania i nadzoru, systemach sterowania pracą elektrowni. Przesyłają informacje związane z obrotem energią oraz administracyjne. Przez długi czas systemy te działały jako systemy odosobnione. Jednakże w ostatnim czasie następuje silna ich integracja – tak, by zdarzenia w jednym systemie oddziaływały na drugi system. Te same dane mogą być wykorzystane do różnych celów i są dostępne dla różnych części systemu. Złożoność systemu powoduje jednak, że wzrasta liczba słabych punktów w sieci, a tym samym podatność systemów informatycznych energetyki na działania włamywaczy komputerowych, czy wirusy. Dopuszczając do sieci coraz więcej użytkowników (pracowników, klientów, poddostawców), powiększa się obszar zagrożeń spowodowany faktem, iż autentyczność danych lub osób nie może być zagwarantowana. Ponadto wykorzystanie sieci teleinformatycznej do przesyłania danych niezwiązanych z potrzebami energetyki, dodatkowo zwiększa potrzebę zapewnienia bezpiecznej wymiany danych. Stosując odpowiednie techniki bezpieczeństwa, należy zapewnić niezbędną ochronę dla informacji technologicznych i administracyjnych. Konieczne staje się również oddzielenie tych informacji od danych przesyłanych na potrzeby zewnętrznych użytkowników. W przeszłości istotną rolę pełniły fizyczne aspekty polityki bezpieczeństwa sieci teleinformatycznych. Wynikało to z faktu większościowego wykorzystania łączy szeregowych, modemów telefonicznych i protokołów transmisyjnych, które najczęściej były chronione patentami producenta danego rozwiązania. W takich przypadkach stosowano powszechnie proste metody autoryzacji w postaci pary uwierzytelniającej użytkownik-hasło (najczęściej przy braku jakiegokolwiek szyfrowania). Problemy dotyczące współdzielenia infrastruktury teleinformatycznej i/lub mediów pojawiają się z coraz większym nasileniem wraz z wykorzystaniem rozwiązań opartych na Ethernecie. Tego typu homogeniczne rozwiązania transportowo-usługowe w dziedzinie transmisji danych są obecnie coraz częściej spotykane w zastosowaniach przemysłowych, w tym również w infrastrukturze teleinformatycznej elektroenergetyki. Wynika to m.in. z dużej elastyczności tego rozwiązania. Jednocześnie jest on najlepiej dopasowany do protokołu TCP/IP co daje możliwość realizacji transmisji danych w sieciach rozległych. Nowoczesne przełączniki sieciowe (switche) zastosowane na wszystkich poziomach systemu dają szansę budowy sieci w pełni zarządzalnej i przewidywalnych parametrach jakościowych transmisji. W szczególności jest to bardzo istotne dla aplikacji czasu rzeczywistego. Sukcesywnie wprowadza się nowe funkcjonalności i rozwiązania, podwyższające wydajność i niezawodność pracy takich sieci. Możliwa jest więc na przykład praca w trybie tzw. pełnego dupleksu. W takim trybie eliminuje się zjawisko kolizji, a połączenie nawiązywane jest tylko pomiędzy dwoma urządzeniami. Nie ma tutaj ograniczeń co do odległości pomiędzy urządzeniami, a transmisja jest uzależniona przez wymagania tzw. zbieżności innych protokołów (np. reagujących na zmianę topologii struktury sieciowej).

Bezpieczny system, według standardów ISO/IEC 17799 powinien zapewniać pięć podstawowych elementów [1, 2, 4, 5]:

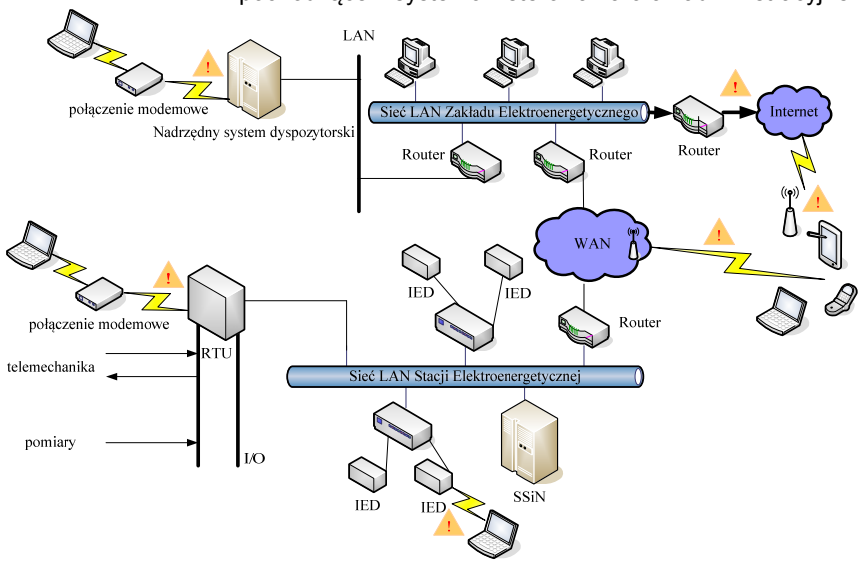
- uwierzytelnianie, obejmujące dwie formy: uwierzytelnianie tożsamości oraz uwierzytelnianie źródła pochodzenia danych;
- kontrolę dostępu, służącą do ochrony zasobów przed nieupoważnionym wykorzystaniem;

- poufność danych, zapewniająca ochronę przed nieupoważnionym ujawnianiem informacji;
- integralność danych, chroniąca przed zagrożeniami wiarygodności danych;
- niezaprzeczalność, uniemożliwiająca zaprzeczenie wysyłania lub odbioru danych.

Struktura systemów teleinformatycznych energetyki

Powiększająca się sieć teletransmisyjna energetyki jest coraz bardziej podatna na działania, które mogą spowodować zakłócenia w jej pracy. Możliwe jest zarówno przechwycenie ważnych informacji, zwłaszcza tych o charakterze administracyjnym związanych z handlem energią, jak i atak powodujący zablokowanie funkcjonowania danego fragmentu sieci lub danej usługi (np. dostępu do serwera z bazą danych). Szczególnie niebezpieczne może być zablokowanie działania sieci przesyłającej informacje czasu rzeczywistego, związane z zabezpieczeniami, telesterowaniem i telekontrolą. Włamania do sieci mogą dokonać również uprawnieni użytkownicy od wewnątrz systemu. Rysunek 1 przedstawia kilka punktów w sieci technologicznej energetyki, z których możliwy jest nieautoryzowany dostęp do zasobów.

Udostępnienie teleinformatycznej sieci energetyki na potrzeby zewnętrznych użytkowników, to kolejne źródło zagrożenia. Niezbędne jest oddzielenie informacji przesyłanych na potrzeby energetyki od zewnętrznego ruchu. Ponadto ruch administracyjno-biurowy powinien być również odseparowany od ruchu związanego ze zdalnym prowadzeniem nadzoru nad obiektami energetyki. Brak wyraźnego rozdzielenia tych sieci może przykładowo spowodować potencjalne włamanie do systemu sterowania pracą elektrowni, dzięki dostępowi przez sieć administracyjną, czy spowodować zablokowanie działania i skasowanie danych z systemu SCADA [1, 2, 4, 5]. Logicznego rozdzielenia sieci można dokonać wykorzystując sieci prywatne VPN z wyznaczaniem tras za pomocą protokołu MPLS. Przykładem może być wykorzystanie tej techniki do ustalenia bezpiecznej i wydzielonej trasy dla przepływających pakietów pomiędzy oddziałami spółki dystrybucyjnej. Dostęp do sieci administracyjnej będzie oddzielony od podobnej sieci innej spółki, mimo iż sieć przesyłająca dane technologiczne może być współdzielona.



Rys. 1. Potencjalne miejsca ataku na sieć przesyłająca dane do systemów dyspozytorskich

W celu poprawy bezpieczeństwa niezbędne jest również zainstalowanie zapór ogniowych filtrujących ruch i blokujących dostęp do intranetów energetyki dla nieuprawnionych komputerów. Firewall jest uzupełnieniem dla sieci VPN. Powinien być umieszczany m.in. w punktach styku z siecią Internet, czy w punktach styków dwóch sieci różnych oddziałów spółek. Wszelkie serwery oferujące usługi na potrzeby przedsiębiorstwa (obsługujące pocztę elektroniczną, przechowujące bazy danych, klucze szyfrujące lub hasła), powinny być umieszczone w strefie zdemilitaryzowanej. Obecnie firewall'e są w stanie analizować ruch pod kątem konkretnej usługi, czy protokołu wymiany danych. Dzięki temu mogą blokować dostęp do sieci technologicznej dla pakietów, które korzystają z protokołów innych niż powszechnie używane w energetyce (IEC 61850, DNP3.0, Modbus). Uzupełnieniem urządzeń filtrujących ruch są systemy wykrywania włamań do sieci IDS (ang. *Intrusion Detection System*) [4 5 8]. System IDS analizuje ruch pod kątem oznak znanych ataków i rejestruje przepływające dane w dzienniku zdarzeń, pozwalając na późniejszą ich analizę. W momencie wykrycia podejrzanych pakietów generowany jest alarm oraz modyfikowane są reguły filtrowania w zaporze ogniowej, aby jak najszybciej zablokować potencjalne zagrożenie. Dzięki możliwościom tych systemów, każdemu użytkownikowi (np. w sieci administracyjnej) można przypisać określony wzorzec użytkowania sieci. Nieuzasadnione odchylenie się od tego wzorca może być uznane za potencjalną próbę ataku. Systemy IDS pomagają więc w zapobieganiu ataków pochodzących z wewnątrz sieci.

Logiczne oddzielenie sieci energetyki za pomocą VPN można uzupełnić przez fizyczną separację sieci technologicznej i administracyjnej od sieci publicznej. Fizyczny podział sieci polega na zastosowaniu dedykowanych włókien światłowodowych lub połączeń kablowych, do łączenia telezabezpieczeń lub systemów sterowania i nadzoru. W krajowym systemie obowiązuje podział włókien światłowodowych, będących w posiadaniu PSE, według którego pewien procent włókien (zarezerwowanych przepływności) jest przeznaczonych na potrzeby technologiczne i administracyjne, a reszta może zostać udostępniona dla zewnętrznego operatora. Do oddzielenia poszczególnych sieci można wykorzystać również technikę zwielokrotniania falowego WDM. Dzięki całkowitej niezależności kanałów optycznych, w jednym włóknie mogą być przesyłane przykładowo informacje pochodzące z systemów sterowania oraz administracyjne.

Zapewnienie bezpieczeństwa systemów teleinformatycznych energetyki wymaga zarówno zastosowania wspomnianych technik, jak i stworzenia odpowiedniej polityki bezpieczeństwa. Powinna ona zawierać definicję bezpieczeństwa oraz określać zasady dostępu do określonych zasobów. Należy uwzględnić fakt, iż wiele systemów energetyki (np. telezabezpieczeń, telesterowania) wymaga wysokiego poziomu dostępności i wysokiego priorytetu w działaniu, gdyż przesyłają krytyczne dane. W zależności od topologii sieci i ważności danych zasobów można określić dodatkowe uwarunkowania. Proponowanym przez CIGRE podejściem do klasyfikacji informacji w systemie pod względem bezpieczeństwa i dostępu do poszczególnych usług jest koncepcja domen bezpieczeństwa [1, 2, 4, 5]. Przykładowo można wyróżnić następujące domeny, w których będą obowiązywać różne poziomy bezpieczeństwa:

- utrzymania ruchu;
- sterowania pracą elektrowni;
- sterowania pracą stacji elektroenergetycznej;
- telekomunikacyjna;
- aplikacji czasu rzeczywistego;
- administracyjna;
- publiczna.

Domeny bezpieczeństwa są ze sobą powiązane, gdyż współdzielą medium transmisyjne. Różnią się jednak co do wymagań względem bezpieczeństwa, gdyż różne jest ich przeznaczenie. Energetyka może również określić poziomy bezpieczeństwa na danym szczeblu (np. regionalnym). Lokalne zasady mogą określać, czy wszystkie elektrownie, stacje i lokalne centra nadzoru i sterowania, znajdujące się na danym terenie, podlegają tym samym zasadom, czy zasady zostaną podzielone. Za pomocą domen można również ustalić odrębne zasady bezpieczeństwa dla udostępnianych zasobów sieci teleinformatycznej energetyki zewnętrznym użytkownikom (domena publiczna). Zastosowanie wcześniej wymienionych technik separuje ruch pomiędzy domenami oraz zapobiega konfliktom w wymianie danych między nimi.

Podstawowe algorytmy kryptograficzne

Szyfrowanie informacji ma na celu eliminację zagrożeń związanych z naruszeniem poufności informacji, gdyż zaszyfrowana informacja może być odczytana tylko przez osoby upoważnione. Metody kryptograficzne zapewniają też usługę uwierzytelniania. Mogą zostać zastosowane również do sprawdzania integralności wiadomości (razem z sumami kontrolnymi) oraz mogą uniemożliwić, zarówno nadawcy, jak i odbiorcy, zaprzeczenie faktowi wysłania lub odebrania wiadomości. Współczesne systemy kryptograficzne opierają się na pojęciu klucza, elementu, bez którego nawet znajomość samego algorytmu szyfrowania nie pozwala na odczytanie zaszyfrowanej informacji. Skuteczność kryptografii zależy od długości klucza (np. 256 bitowego) i czasu potrzebnego na złamanie szyfru. Istnieją dwa podstawowe algorytmy kryptograficzne [4, 5, 6]:

- algorytmy symetryczne (np. AES, ang. *Advanced Encryption Standard*) – wymagające znajomości klucza przez obydwie strony przekazu informacji. Stąd wynika ich wada, mianowicie konieczność przekazania klucza odbiorcy oraz używania tylu kluczy, ilu jest odbiorców;
- algorytmy asymetryczne (np. RSA – nazwa pochodzi od nazwisk twórców: *Rivest*, *Shamir*, *Adelman*) – posługujące się parą kluczy: publicznym i prywatnym. Klucz publiczny jest znany wszystkim zainteresowanym, natomiast prywatny – tylko jego właścicielowi. W dużych sieciach szyfrowanie asymetryczne wymaga użycia mniejszej liczby kluczy niż przy szyfrowaniu symetrycznym. Ponadto algorytmy te pozwalają na oddzielenie autentyczności i poufności oraz umożliwiają sprawdzenie integralności wiadomości za pomocą podpisu cyfrowego. Szyfrowanie kluczami asymetrycznymi jest wolniejsze (dłuższe klucze), jednak dzięki temu bardziej bezpieczne.

Aby wymienione metody mogły działać, klucze publiczne muszą być udostępniane. Wymieniając między sobą klucze publiczne i kojarząc je z kluczami prywatnymi, obie strony mogą wymieniać między sobą informacje poufne bez konieczności przekazywania klucza do deszyfrowania informacji. Mechanizm ten nosi nazwę kryptografii klucza publicznego PKC (ang. *Public Key Cryptography*). Idea kluczy publicznych może być rozszerzona o certyfikaty cyfrowe [4 5 6], wiążące klucze publiczne z osobą lub organizacją i potwierdzane podpisem zaufanych wydawców certyfikatów. W kryptografii ważną rolę spełnia również sposób administrowania kluczami. Zarządzanie kluczami oraz certyfikatami, stosowanymi w kryptografii klucza publicznego, zapewnia infrastruktura kluczy publicznych PKI (ang. *Public Key Infrastructure*) [4, 5, 6]. Określa ona sposoby tworzenia, dystrybucji, śledzenia i odwoływania kluczy i certyfikatów.

Kryptografia jest również stosowana przetworzeniu podpisów cyfrowych [4, 5, 7]. Polega on na dodaniu unikatowych danych (skrótu wiadomości) do dokumentu w taki sposób, że generować je może jedynie właściciel klucza prywatnego. Natomiast każdy, kto posiada odpowiedni klucz publiczny, może weryfikować autentyczność takiego podpisu. Skrót wiadomości (abstrakt) tworzony jest za pomocą funkcji haszującej (np. SHA-256). Następnie jest szyfrowany kluczem prywatnym, stając się podpisem cyfrowym. Prawdopodobieństwo wystąpienia takiego samego abstraktu wiadomości w dwóch różnych dokumentach jest bliskie zeru i dlatego nawet najmniejsza zmiana w treści dokumentu spowoduje zmiany w abstrakcie. Dzięki temu podpisy cyfrowe zapewniają najwyższy poziom integralności danych oraz gwarantują niezaprzeczalność. Nie gwarantują jednak prywatności – szyfrowanie samej wiadomości musi być wykonane oddzielnie. Podpisy mogą być wykorzystane również w procesie uwierzytelniania.

Klucze publiczne stosowane są również w protokołach bezpieczeństwa [4, 5, 7]: SSL (ang. *Secure Socket Layer*), TLS (ang. *Transport Layer Security*), czy S/MIME (ang. *Secure Multipurpose Internet Messaging Extension*). SSL to protokół warstwy transportowej modelu OSI, pozwalający zapewnić uwierzytelnianie oraz poufność i integralność przesyłanych danych. Nie zapewnia natomiast niezaprzeczalności. SSL stał się standardem bezpiecznej komunikacji (w protokole HTTP) użytkownika z serwerem WWW. Zabezpiecza przesyłanie informacji, dzięki szyfrowaniu danych opuszczających przeglądarkę i deszyfrowaniu ich po dotarciu do serwera. Podobnie szyfruje się dane przed wysłaniem ich do użytkownika. SSL stosuje szyfrowanie kluczem publicznym, wymieniając klucze sesyjne pomiędzy przeglądarką i serwerem webowym. Klucz sesyjny używany jest do szyfrowania zarówno dyspozycji jak i odpowiedzi, zachowując w tajemnicy prywatne klucze użytkownika i serwera. Negocjowanie połączenia z serwerem przez protokół SSL wygląda następująco [4, 5, 6]:

- użytkownik łączy się za pomocą przeglądarki internetowej z serwerem;
- serwer wysyła swój certyfikat;
- komputer użytkownika weryfikuje autentyczność certyfikatu serwera;
- opcjonalnie może być dokonana weryfikacja certyfikatu użytkownika. Serwer sprawdza, czy jest on na komputerze klienta, i pobiera jego dane. Informacje te porównywane są z zawartością bazy danych. Z parametrów certyfikatu serwera wynika, jakie szyfrowanie może być użyte;
- po ustaleniu preferowanej długości klucza sesyjnego przeglądarka użytkownika generuje go, a następnie szyfruje z wykorzystaniem klucza publicznego zawartego w certyfikacie serwera algorytmem asymetrycznym. Zaszyfrowany klucz sesyjny jest wysyłany do serwera wraz z informacją o wybranym algorytmie szyfrowania;
- serwer wykorzystuje swój klucz prywatny do odszyfrowania klucza sesyjnego. Dalsza transmisja jest zabezpieczona uzyskanym w ten sposób kluczem symetrycznym.

Wiele problemów związanych z bezpieczeństwem danych można rozwiązać za pomocą kryptografii. Konieczne jest jednak zastosowanie innych technik

zabezpieczających sieć przed wykonywanymi przez Internet niepożądanymi próbami dostępu bądź atakami na jej działanie. Jednym ze sposobów jest zapora ogniowa (ang. *Firewall*). Zapora umieszczana jest najczęściej w punkcie styku intranetu przedsiębiorstwa z siecią Internet lub inną zewnętrzną siecią. Stanowi ona fizyczne odseparowanie wszystkich komputerów wspomagających realizację istotnych zadań i przechowujących strategiczne informacje. Aby mogła ona spełniać swoją funkcję, cały ruch wchodzący i wychodzący z wewnętrznej sieci musi przechodzić przez zaporę. Firewall sprawdza każdy przepływający przez niego pakiet i przepuszcza lub blokuje go, zgodnie z regułami bezpieczeństwa ustalonymi przez administratora. Z jego pomocą można chronić sieć przed nieautoryzowanym dostępem, podszywaniem się, czy atakami typu *DoS* (w tym odmiana *Smurf*). Nie zapewnia natomiast ochrony przed podsłuchiwaniem i błędami w oprogramowaniu. Zapory ogniowe możemy podzielić na trzy kategorie [4, 5, 6]:

- aplikacyjne (ang. *application gateway*) – umożliwiające kontrolowany dostęp do określonych usług;
- połączeniowe (ang. *circuit gateway*) – zestawiający według określonych zasad połączenia TCP pomiędzy komputerami z sieci wewnętrznej, a Internetem;
- filtrujące (ang. *packet filtering gateway*) – sprawdzające pakiety przychodzące i wychodzące z sieci pakiety.

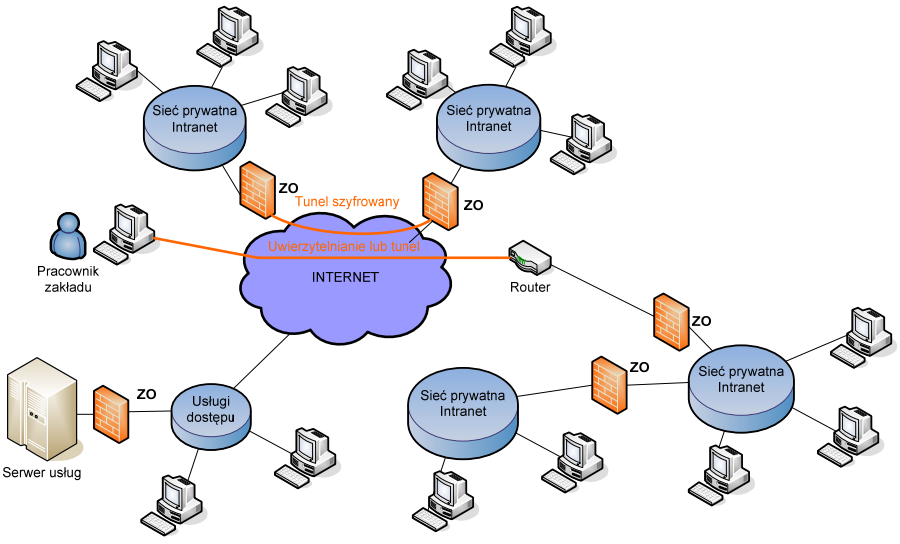
Blokadę dostępu, za pomocą zapory ogniowej, na poziomie aplikacji umożliwia mechanizm filtrowania sesji [4, 5, 6]. Polega on na rejestracji przetransportowanych pakietów dzięki czemu staje się możliwe ustalenie związków między pakietami tego samego połączenia. To rozwiązanie jest w stanie zagwarantować, że po ustaleniu połączenia, żaden niepowołany pakiet nie przyłączy się do strumienia i nie przekształci zawartości serwera lub stacji klienta. Może też nie dopuszczać pakietów, które przykładowo mają za krótkie ramki. Dzięki możliwości rozpoznania natury każdego z protokołów, zapora jest w stanie precyzyjnie ustalić reguły kontroli. Bramy poziomu aplikacji mogą również modyfikować lub nawet usuwać niektóre fragmenty z treści wiadomości i wprowadzać usługę uwierzytelniania w protokołach bezpołączeniowych. Innym sposobem na filtrowanie ruchu w warstwie aplikacji jest zastosowanie serwera *proxy*, jako zapory pośredniczącej. Jego zadaniem jest przejmowanie żądań pochodzących z zewnątrz sieci i po sprawdzeniu uprawnień, utworzenie połączenia z komputerem w sieci wewnętrznej, lecz za pośrednictwem nowego połączenia w warstwie aplikacji. Mechanizm ten działa również w odwrotną stronę – zestawiając połączenia pomiędzy użytkownikiem wewnątrz, a serwerem na zewnątrz. Jako przykład można podać zestawienie połączenia w protokole FTP. Zamiast bezpośredniego uruchamiania sesji FTP do systemu zdalnego, sesja uruchamiana jest na zaporze i dopiero oprogramowanie firewall'a uruchamia połączenie z systemem zdalnym. Zabezpieczające działanie *proxy* polega w tym wypadku na blokowaniu wszelkich pakietów niepoprawnych z punktu widzenia protokołu FTP, które przy bezpośrednim połączeniu mogłyby być obsłużone przez lokalny system. Serwer *proxy* umożliwia też w tym przypadku kontrolę kto, kiedy oraz w jaki sposób korzysta z usługi FTP. Firewall w postaci serwera *Proxy* pozwala na maskowanie struktury sieci, gdyż cała sieć może być widoczna na zewnątrz za pomocą jednego adresu IP (dzięki procedurom translacji adresów). Połączenie mechanizmów filtrujących z translacją adresów praktycznie uniemożliwia bezpośredni atak, na którykolwiek z komputerów chronionych zaporą.

Zapory ogniowe z filtrowaniem pakietów działają w warstwie sieciowej [3, 4, 5]. Mechanizm filtrowania realizowany jest przez odpowiednie oprogramowanie, które potrafi uniemożliwić przedostanie się pakietów z jednej sieci do drugiej. Program ten może znajdować się w ruterze lub przełączniku LAN, jak na rysunku 1. Administrator musi skonfigurować filtr, określając, które pakiety mogą przechodzić przez ruter, a które powinny być zatrzymane. Filtr pakietów przegląda pola adresowe w nagłówku każdego pakietu. Jest konfigurowany w ten sposób, że podawane są pola, które mają być sprawdzane oraz sposób interpretacji wartości tych pól.

Jak wspomniano wcześniej, zapora ogniowa umieszczana jest na styku dwóch sieci i ma zapewniać ochronę zasobów przed niepożądanym dostępem. Za działanie zapory odpowiada dedykowane oprogramowanie znajdujące się na serwerze, ruterze, przełączniku bądź komputerze użytkownika (zapory aplikacyjne). Zapory ogniowe mogą działać w kilku różnych układach, przedstawionych na rysunku 2.

Zapory ogniowe mogą rozdzielać dwie prywatne sieci, chronić osobiste komputery użytkowników, filtrować ruch w połączeniach odległych oddziałów przedsiębiorstw, czy chronić serwer udostępniający usługi (np. przechowujący bazy danych lub klucze szyfrujące oraz hasła). Wzmocnienie ochrony może zapewnić zastosowanie dwóch zapór ogniowych (wewnętrznej i zewnętrznej) poprzez utworzenie strefy zdemilitaryzowanej DMZ [4, 5, 7]. Utworzony w ten sposób pomocniczy system ochrony zapewnia wysoki poziom bezpieczeństwa, nie obniżając wydajności pracy firewall'a.

Zewnętrzna zapora (zaimplementowana na przykład w przełączniku sieciowym) ma za zadanie wstępnie filtrować pakiety i realizować ewentualną translację adresów. Pierwsza linia odrzuca pakiety odbiegające od zadanej normy – z niewłaściwa długością ramki, identycznymi adresami źródłowymi i odbiorczymi, z adresami źródłowymi używanymi wewnątrz sieci, itp. Wewnętrzna zapora realizuje pełniejszy zakres ochrony, czyli może prowadzić analizę protokołów lub kojarzyć pakiety z aplikacjami.



Rys. 2. Najczęściej stosowane miejsca instalacji „zapór ogniowych" **ZO** (*ang. firewalls*)

Dodatkowo w celu rozładowania ruchu, przełączniki pierwszej linii mogą rozpraszać ruch na szereg wewnętrznych zapór, zwiększając w ten sposób przepustowość.

Należy również zaznaczyć, że zapory ogniowe mogą być przenikane za pomocą tuneli kryptograficznych. Jeżeli dwa komputery po różnych stronach zapory ustanowią połączenie szyfrowane w ramach VPN lub SSL, znaczna część reguł analizy pakietów straci sens. Nie będzie można stosować reguł, które odnoszą się do warstw sieciowych wyższych niż warstwa, na której odbywa się szyfrowanie. Zapory stanowią więc ochronę przed atakami z zewnątrz, a nie z uwierzytelnionych sieci prywatnych.

Podsumowanie

Obecnie powszechnie rozważana jest unifikacja polityki dostępu, bezpieczeństwa i sposobu zarządzania sieciami najbardziej wymagających i krytycznych systemów teleinformatycznych. W elektroenergetyce opracowuje się różne tego typu koncepcje. Ciekawym rozwiązaniem jest NERC-CIP. Opisuje ona wymagania odnośnie bezpieczeństwa systemów np. pod kątem możliwości przeprowadzania ataków terrorystycznych. Wspomniany wcześniej standard pozwala na zidentyfikowanie najbardziej krytycznych zasobów co pozwala na odpowiednie zabezpieczenie sieci i szkolenie personelu. Wprowadzanie do energetyki tzw. inteligentnych sieci elektroenergetycznych („*smart grid*") powoduje konwergencję różnych technologii informatycznych i komunikacyjnych. Znaczenie analiz bezpieczeństwa pracy takich systemów znacząco wzrasta. Niestety opracowywane standardy są najczęściej w wersjach rozwojowych i nie nadążają za dynamiką zmian funkcjonalności i powszechności dostępności pewnych obszarów systemów teleinformatycznych infrastruktury elektroenergetyki dla ogółu ludności. Należy podkreślić, że każdy możliwy punkt styku sieci teleinformatycznych ogólnodostępnych z sieciami o znaczeniu krytycznym jest potencjalnym punktem możliwego ataku na tego typu sieć. Doświadczenia ostatnich lat wskazują, że dla tego typu sieci zagadnienia bezpieczeństwa nie są traktowane z należytą uwagą. Wielokrotnie dochodziło np. do ataków na teoretycznie dobrze zabezpieczone sieci banków lub wielkich korporacji (również na strony rządowe). Odczytywane były również „zaszyfrowane" depesze przesyłane w sieciach o znaczeniu militarnym. Wprowadzanie nowych funkcjonalności do systemów teleinformatycznych elektroenergetyki powinno więc być poprzedzone starannymi analizami wpływu tychże funkcjonalności na bezpieczeństwo pracy takich systemów. Przy obecnym poziomie informatyzacji procesów wytwarzania, przesyłu i odbioru energii elektrycznej jakakolwiek możliwość nieautoryzowanego oddziaływania na system elektroenergetyczny, jego obiekty i urządzenia elementarne może mieć katastrofalne skutki.

LITERATURA

[1] CIGRE, JWG D2-B3-C2.01: Cyber security considerations in power system operations. *Electra 218/2005*

[2] CIGRE, JWG D2-B3-C2.01 Managing information security in an electric utility. *Electra 216/2004*

[3] Comer D.E.: Sieci komputerowe i intersieci. Warszawa, *WNT* 2003

[4] Szewczyk M., Halinka A.: Media transmisyjne w automatyce elektroenergetycznej, *Materiały Sympozjum Naukowo-Technicznego pod patronatem honorowym Komitetu Automatyki Elektroenergetycznej SEP "Zabezpieczenia elektroenergetyczne w zakładach górniczych*", ISBN 978-83-60837-04-7, Gliwice, 3 kwietnia 2007, s. 43 - 61

[5] Halinka A., Szewczyk M.: Bezpieczeństwo przesyłu informacji oraz algorytmy szyfrujące możliwe do wykorzystania w infrastrukturze teleinformatycznej energetyki, *Wiadomości Elektrotechniczne*, ISSN 0043-5112, 6/2008, s. 3-8

[6] *Vademecum teleinformatyka Tom 1*. Warszawa, IDG Poland 1999

[7] *Vademecum teleinformatyka Tom 2*. Warszawa, IDG Poland 2002

[8] *Vademecum teleinformatyka Tom 3*. Warszawa, IDG Poland 2004

***Autor**: dr inż. Michał Szewczyk, Politechnika Śląska w Gliwicach, Instytut Elektroenergetyki i Sterowania Układów, ul. B. Krzywoustego 2, 44-100 Gliwice, E-Mail: Michal.Szewczyk@polsl.pl*.