38

MONITORING MASZYN I URZĄDZEŃ – KONCEPCJA TECHNICZNEJ REALIZACJI PRZEPISÓW

38.1 WSTĘP

Świat IT (Information Technology) i OT (Operational Technology) we współczesnym przedsiębiorstwie działają niezależnie i obok siebie. W świecie IT powszechne jest dążenie do standaryzacji usług. Dużo wysiłku wkłada się w uzyskanie łatwego dostępu dla użytkowników do informacji, przy zachowaniu bezpieczeństwa systemów. Powszechne jest włączanie wszystkiego do Internetu. Zadomowił się tu na dobre protokół IP. Z kolei w świecie OT bywa z tym różnie [4]. Systemy informatyczne świata OT, tzw. systemy SCADA (Supervisory Control And Data Acquisition) są w większości przypadków systemami autorskimi producentów oprogramowania, w dokumentacji których brak jest informacji o sposobie dostępu do danych w nich zgromadzonych. Udostępnienie danych z tych systemów wiąże się zwykle z koniecznością udostępnienia takiego autorskiego oprogramowania, które te dane interpretuje i wizualizuje. Tym samym praktycznie niemożliwe jest udostępnienie samych danych bez umożliwienia dostępu do systemu informatycznego, przetwarzającego te dane. Z drugiej strony, liczne przepisy jak również rozsądek i doświadczenie projektantów systemów OT ograniczają powszechny dostęp do systemów „przemysłowych". Specjaliści OT mówią, że „gdy w IT coś nie działa, ludzie nie dostają maili. Gdy u nas coś nie działa ludzie tracą życie". W niniejszym artykule przedstawiono koncepcję rozwiązania bezpiecznego dostępu do danych zgromadzonych w systemach OT, umożliwiającą wymianę danych między tymi systemami, nie niosącego – zdaniem autorów – zagrożenia nieuprawnionej ingerencji w systemy monitorowania i sterowania procesami produkcji.

38.2 SPOSÓB OCHRONY SYSTEMÓW MONITOROWANIA I STEROWANIA PROCESAMI PRODUKCJI – STAN OBECNY

Dla potrzeb bezpieczeństwa systemów monitorowania i sterownia procesami produkcji w podziemnych zakładach górniczych, zostało stworzone w przepisach pojęcie sieci wydzielonych. Sposób ochrony tych systemów został określony w ust 2. § 636 Rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002 r. w sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego

zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych. Przepis ten ma następujące brzmienie:

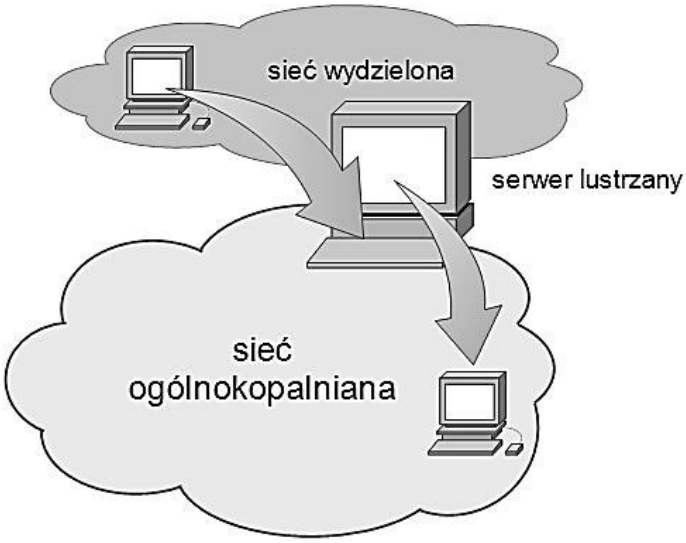
„2. Oprogramowanie i dane w systemach łączności, alarmowania, bezpieczeństwa i wspomagania pracy służb dyspozytorskich oraz innych układów funkcjonujących na podstawie technik informatycznych chroni się w następujący sposób:

1) systemy pracują w wydzielonych sieciach,
2) dostęp do danych z tych systemów jest możliwy wyłącznie w obrębie zakładu górniczego, przy czym:
   a. dane udostępnia się z wydzielonego serwera "lustrzanego", na który systemy te będą przesyłać informacje w układzie jednokierunkowym bez możliwości dostępu do systemów podstawowych,
   b. dostęp do oprogramowania systemów jest możliwy jedynie ze stanowisk zabudowanych wewnątrz sieci podstawowej, a system będzie zapisywał automatycznie wszystkie czynności dokonywane z tych stanowisk,
3) nadzór serwisowy producenta nad eksploatowanym w zakładach górniczych sprzętem (systemami komputerowymi) realizuje się bezpośrednio na terenie zakładu górniczego. W przypadku konieczności zdalnego nadzoru, kanał łączności konfigurują ręcznie pracownicy obsługi zakładu górniczego po telefonicznym uzgodnieniu przez serwis producenta, natomiast połączenie i dokonane czynności zostaną automatycznie odnotowane w systemie,
4) sposób zabezpieczenia, o którym mowa w pkt 3, zatwierdza kierownik ruchu zakładu górniczego”.

Wprawdzie Ustawodawca w żadnym akcie prawnym nie formułuje wprost listy sieci wydzielonych (ani też definicji takiej sieci), jednakże do takich sieci zalicza się co najmniej następujące sieci informatyczne i telekomunikacyjne: systemy teleinformatyczne eksploatowane w dyspozytorni kopalnianej, systemy łączności i alarmowania, systemy gazometrii, systemy informatyczne kopalnianej stacji geofizyki górniczej (sejsmologia i sejsmoakustyka), systemu rejestracji pracy urządzeń wyciągowych, systemu sterowania i nadzoru ZPMW. W związku z brakiem jednoznacznej definicji sieci wydzielonej, powyższa lista jest listą otwartą i uzależnioną od specyfiki danego zakładu górniczego [1, 6, 9].

Według przywołanego przepisu, istotnym i jedynym elementem zabezpieczającym sieć wydzieloną (podstawową) jest tzw. serwer lustrzany, o którym mowa w § 636 ust 2 pkt 2a ww. Rozporządzenia Ministra Gospodarki. Sieć ogólnodostępna (ogólnokopalniana) oraz wydzielona są ze sobą połączone za pomocą serwera lustrzanego, wyposażonego w dwa interfejsy sieciowe, który pełni funkcję serwera plików przesyłanych z sieci wydzielonej do sieci ogólnokopalnianej (rys. 38.1) [3].

Takie rozwiązanie tylko pozornie zabezpiecza sieć wydzieloną od ingerencji z sieci ogólnodostępnej. Serwer plików, pełniący funkcje serwera lustrzanego jest zabezpieczony przed ewentualną ingerencją osób nieupoważnionych jedynie za pomocą mechanizmów systemu operacyjnego na którym jest posadowiony, a które są niewystarczające do pełnej ochrony sieci wydzielonej.



Rys. 38.1 Idea serwera lustrzanego

Mechanizmy kontroli dostępu i kontroli uprawnień zaimplementowane w systemach operacyjnych Windows i Linux (stanowiących środowisko pracy dla serwera plików – tu serwera lustrzanego) nie weryfikują uprawnień użytkownika w zależności od interfejsu sieciowego, po którego stronie następuje logowanie. Ten sam użytkownik logując się na serwer lustrzany może przenieść dane z sieci ogólnodostępnej do sieci wydzielonej pomimo wyłączonego mechanizmu routingu miedzy sieciami [3].

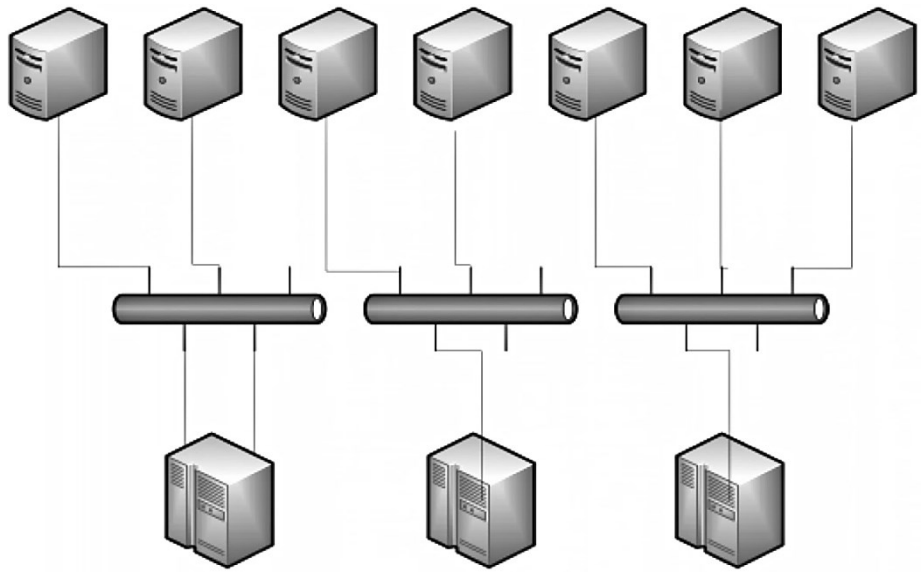
Ponadto sieci wydzielone wymagają dostosowania do zaleceń Wyższego Urzędu Górniczego w zakresie synchronizacji czasu we wszystkich urządzeniach informatycznych pracujących w sieciach wydzielonych. Tym samym w przypadku zdarzeń losowych, jakie mogą zajść w ruchu zakładu górniczego trudna lub wręcz niemożliwa jest korelacja tych zdarzeń i ustalenie ich kolejności i relacji przyczynowo-skutkowych. Pewną próbą rozwiązania tego problemu jest wykorzystanie urządzeń wykorzystujących sygnał czasu pozyskiwany z odbiornika GSM. Rozwiązanie takie jest jednak mało wygodne. Wymaga instalacji dodatkowego oprogramowania na urządzeniach, które mają mieć synchronizowany czas (nie na wszystkich urządzeniach instalacja dodatkowego oprogramowania jest dopuszczalna i możliwa). Ponadto w każdej z sieci wydzielonych, a jest takich sieci na kopalni co najmniej kilka, należałoby zainstalować takie zegary czasu. Osobnym tematem jest kwestia niezawodności rozwiązania z wieloma zegarami czasu – praktycznie niemożliwa jest ciągła kontrola pracy wszystkich zegarów w sieciach wydzielonych, a tym samym niemożliwe może być stwierdzenie, który zegar wskazuje czas poprawny w przypadku różnicy wskazań [3].

Kolejnym nierozwiązanym problemem jest dostęp serwisowy do systemów w sieciach wydzielonych, o którym mowa w ust 2 pkt 3 przywoływanego już wcześniej Rozporządzenia.

W większości przypadków odbywa się on poprzez połączenie modemowe pomiędzy siecią wydzieloną (komputerem w tej sieci) i siecią producenta serwisowanego systemu informatycznego. Tego typu rozwiązania uniemożliwiają automatyczne logowania sesji, o którym mowa w ww. przepisie. Alternatywą do

powyższego rozwiązania jest całkowity zakaz zdalnych połączeń serwisowych wydany przez niektórych Kierowników Ruchu Zakładu Górniczego [3].

Wreszcie ostatnim zidentyfikowanym przez autorów problemem, jest wymiana informacji między różnymi systemami teleinformatycznymi pracującymi w różnych sieciach wydzielonych (rys. 38. 2).



Rys. 38.2 Separacja sieci wydzielonych

W rozwiązaniu w którym istnieje wiele sieci wydzielonych, całkowicie (fizycznie) od siebie odseparowanych, niemożliwa jest jakakolwiek wymiana danych miedzy nimi. Jedynym rozwiązaniem takiego problemu jest zmiana definicji poszczególnych sieci wydzielonych i stworzenie sieci wydzielonej zawierającej kilka funkcjonalnie różnych systemów. Takie rozwiązanie stosuje się dziś powszechnie łącząc na przykład w jedną sieć wydzieloną (dyspozytorską) sieci bezpieczeństwa, alarmowania, łączności i systemy SCADA. Z punktu widzenia formalno-prawnego nie można zaprzeczyć poprawności takiego rozwiązania, jednak uwzględniając aspekt techniczny – takie rozwiązanie jest mało bezpieczne, gdyż awaria pojedynczego urządzenia może sparaliżować pracę całego układu.

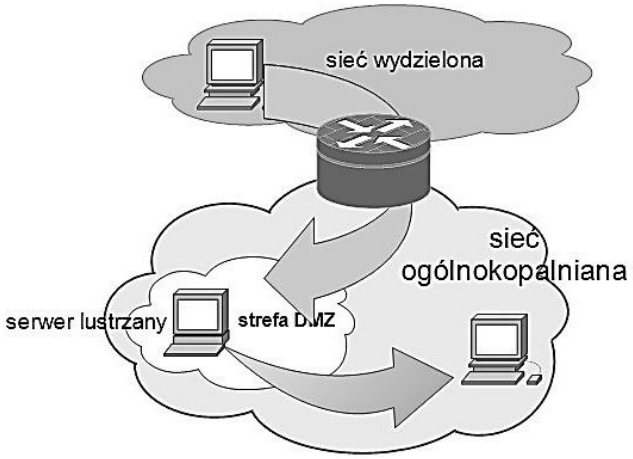
38.3 BEZPIECZEŃSTWO DANYCH I SYSTEMÓW W SIECIACH WYDZIELONYCH – PROPOZYCJA ROZWIĄZAŃ

Bezpieczeństwo definiowane jest jako brak zagrożeń, czasami jako możliwość niezakłóconego funkcjonowania i rozwoju. Według powszechnie znanej definicji, bezpieczny system teleinformatyczny to taki, który poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela. Bezpieczeństwo systemów teleinformatycznych wiąże się z dwoma obszarami zagrożeń: wewnętrznych (głównie niezawodność) i zewnętrznych (ingerencje z zewnątrz i zakłócenia) [2]. Często dla zapewnienia bezpieczeństwa danych i systemów trzeba się pogodzić z pewnymi

ograniczeniami w swobodzie konstruowania systemów teleinformatycznych. Rozwiązania mające służyć bezpieczeństwu opisane w poprzednim rozdziale a oparte na serwerze plików, który pełni funkcję tzw. serwera lustrzanego oparte są na stanie techniki komputerowej funkcjonującej w kopalniach w końcu ubiegłego wieku. Dynamiczny rozwój technik informatycznych w jakim uczestniczymy, pozwala na ominięcie ograniczeń i niedogodności związanych z archaicznymi rozwiązaniami opisanymi wyżej, przy zachowaniu pełnego bezpieczeństwa systemów podlegających ochronie.

38.4 REALIZACJA SERWERA LUSTRZANEGO I SIECI WYDZIELONYCH

W koncepcji opracowanej przez autorów rozwiązania i sukcesywnie wdrażanej przez Zakład Informatyki i Telekomunikacji w zakładach górniczych Kompanii Węglowej S.A. rozdzielono funkcje serwera plików i routera – jakie w dotychczasowym rozwiązaniu obecnie pełni serwer lustrzany – do oddzielnych urządzeń: sprzętowego firewall-a i serwera plików, co przedstawione zostało na rys. 38.3.



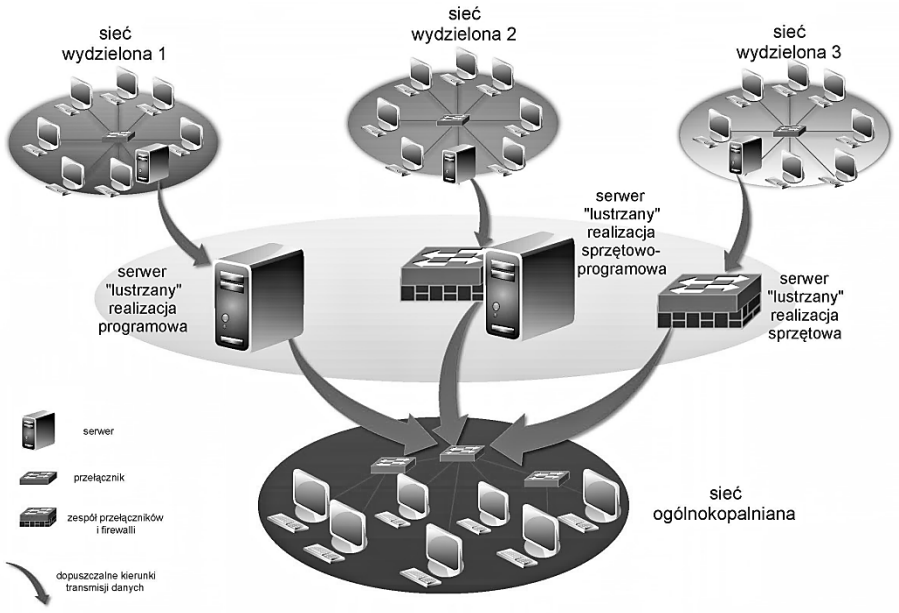
Rys. 38.3 Lokalizacja serwera lustrzanego w strefie DMZ

Serwer lustrzany przeniesiony zostaje ze styku sieci wydzielonej z ogólnokopalnianą do tzw. strefy DMZ (Demilitarized zone) w sieci ogólnokopalnianej, a na styku tych sieci wpięty zostaje sprzętowy firewall.

Zadaniem sprzętowego firewall-a jest zabezpieczenie sieci wydzielonej od ingerencji ze strony użytkowników sieci ogólnokopalnianej, przy jednoczesnym umożliwieniu jednostronnej transmisji danych z systemów znajdujących się w sieci wydzielonej do serwera „lustrzanego", pełniącego już tylko rolę serwera plików. Tym samym serwer „lustrzany" może być jeszcze bardziej „oddalony" od sieci wydzielonej i zlokalizowany w serwerowi obok innych serwerów usługowych, obsługujących systemy kopalniane w strefie DMZ. Komputer (serwer lustrzany) w strefie DMZ chroniony jest przed nieautoryzowanym dostępem użytkowników sieci ogólnokopalnianej nie tylko za pomocą mechanizmów systemu operacyjnego, ale również za pomocą mechanizmów sieciowych firewall'a. Ponadto sprzętowy firewall może rejestrować wszystkie zdarzenia zachodzące w punkcie styku sieci i zapewniać kontrolę transmisji danych

wyłącznie pomiędzy uprawnionymi komputerami z sieci wydzielonej do serwera lustrzanego. Przedstawione rozwiązanie zapewnia zwiększenie niezawodności oraz bezpieczeństwa systemu przy dodatkowej rejestracji i kontroli zdarzeń.

Postęp techniki informatycznej, jaki nastąpił po wydaniu Rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002r. w sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych umożliwia realizację rozwiązania „serwera lustrzanego" w różnoraki sposób. Serwer lustrzany może być realizowany sprzętowo (zespół przełączników i firewalli), programowo (oprogramowanie na komputerze pełniącym rolę serwera plików) lub sprzętowo-programowo (łącząc obydwa rozwiązania opisane wyżej). Rysunek 38.4 przedstawia różne realizacje serwera lustrzanego.



Rys. 38.4 Realizacja idei serwera lustrzanego

Dla systemów informatycznych zakwalifikowanych kategorii systemów objętych obowiązkiem szczególnej ochrony, o której mowa w §636 ust. 2, dla których producent nie dostarcza „autorskiego" serwera lustrzanego, autorzy rekomendują stosowanie opisanej wyżej sprzętowej realizacji serwera lustrzanego [5].

We wszystkich przedstawionych powyżej realizacjach serwerów lustrzanych udostępnienie danych zawsze odbywa się jednokierunkowo. Rozwiązanie jest zdaniem autorów zgodne z przepisem § 636 Rozporządzenia Ministra Gospodarki [8] z dnia 28 czerwca 2002 r. Potwierdzenie tej tezy można znaleźć w opinii technicznej Zespołu Atestacji Katedry Elektryfikacji Górnictwa Politechniki Śląskiej, zgodnie z którą: Istotą wymagań wyrażonych w § 636 Rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002 r. „w sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych". (Dz. U. Nr 139, poz. 1169) jest bowiem jednokierunkowa transmisja danych

realizowana z wykorzystaniem tzw. serwera „lustrzanego", a nie sam sposób wykonania „serwera lustrzanego", który może być zrealizowany sprzętowo (za pomocą zespołu przełączników i firewalli), programowo (oprogramowanie na komputerze pełniącym rolę serwera) lub sprzętowo-programowo (łącząc obydwa rozwiązania opisane wyżej). Realizowany przez Zakład Informatyki i Telekomunikacji KW S.A. sposób dostępu oraz ochrony danych z sieci wydzielonych kopalń jest prawidłowy i spełnia on wymogi § 636 Rozporządzenia Ministra Gospodarki z dnia 28.06.2002 r. [10].

38.5 AKTUALIZACJA SYSTEMÓW OPERACYJNYCH ORAZ WDROŻENIE OCHRONY ANTYWIRUSOWEJ W SIECIACH WYDZIELONYCH

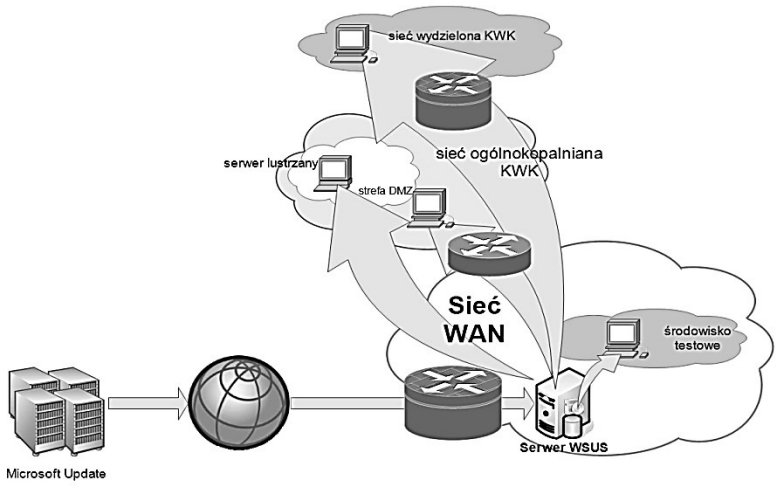
Szczególnym przypadkiem transmisji danych pomiędzy różnymi sieciami wydzielonymi jest implementacja aktualizacji systemów operacyjnych (Windows, Linux) oraz sygnatur dla systemu antywirusowego.

Producenci systemów operacyjnych stale udoskonalają swoje produkty poprzez udostępnianie poprawek mających na celu „załatanie dziur" w obszarze bezpieczeństwa systemów operacyjnych, oraz zwiększenie stabilności tych systemów. W Internecie, w specjalnie przygotowanych serwisach udostępniane są systemy dystrybucji takich poprawek. Niestety systemy pracujące w sieciach wydzielonych nie mają dostępu do tych serwisów. W praktyce okazuje się, że 95% ataków na systemy operacyjne oraz przypadki niestabilnej pracy systemów związane są z podatnością na znane i już rozwiązane przez producentów oprogramowania błędy, które nie zostały usunięte przez użytkowników w drodze implementacji poprawek. W systemach sieci wydzielonych należy wdrożyć aktualizowanie stosowanych systemów operacyjnych. Implementacja poprawek w systemach przemysłowych (monitorowania, sterowania, bezpieczeństwa łączności i alarmowania) będzie realizowana po sprawdzeniu celowości instalacji poszczególnych poprawek, przetestowaniu ich działania i wpływu na te systemy w środowisku testowym. Docelowo, ich wdrożenie w środowisku produkcyjnym uzależnione jest od pozytywnie zakończonych testów w ww. środowisku testowym lub uzyskaniu rekomendacji producenta systemu OT. Aktualizacja systemów w sieciach wydzielonych odbywać się będzie wyłącznie z „zaufanych" serwerów dystrybucji poprawek – znajdujących się w sieci wydzielonej z sieci ogólnokopalnianej, przeznaczonej dla serwerów dystrybucji poprawek i administrowanych przez uprawnione do tego osoby. Tego typu rozwiązanie stosowane jest już z powodzeniem w sieci ogólnokopalnianej KW S.A. w zakresie aktualizacji systemów operacyjnych „zwykłych" komputerów [3].

Rysunek 38.5 przedstawia sposób wdrożenia aktualizacji systemów operacyjnych na przykładzie rozwiązań firmy Microsoft Corp. – systemu WSUS (Windows Server Update Services).

Implementacja sygnatur systemu antywirusowego może przebiegać w sposób analogiczny do przedstawionego powyżej. Ze względu na fakt, iż systemy antywirusowe dość mocno ingerują w działanie systemu operacyjnego, należałoby jednak przed wdrożeniem ochrony antywirusowej systemów sterowania i bezpieczeństwa uzyskać

opinię i potwierdzenie producenta tych systemów co do poprawnego ich działania w środowisku z aktywnym systemem antywirusowym.



Rys. 38.5 Aktualizacja systemów operacyjnych

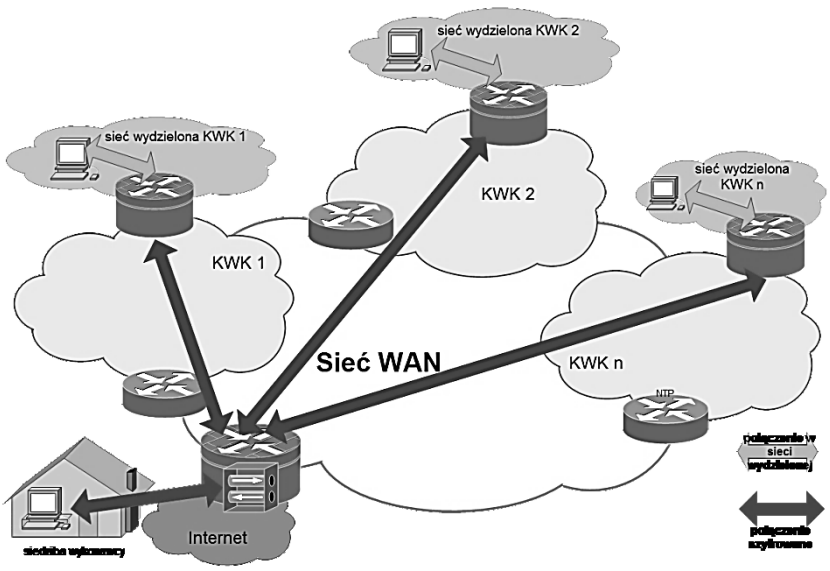
38.6 REALIZACJA ZDALNEGO DOSTĘPU SERWISOWEGO DO URZĄDZEŃ W SIECIACH WYDZIELONYCH

Ustawodawca definiując w §636 ust. 2 Rozporządzenia systemy podlegające szczególnej ochronie, obok systemów: łączności, alarmowania, bezpieczeństwa i wspomagania pracy służb dyspozytorskich, wymienia szeroko pojęte „inne układy funkcjonujące na podstawie technik informatycznych". Wskutek postępu technologicznego w zakresie technik informatycznych i telekomunikacyjnych w układach sterowania maszyn i urządzeń stosowanych w podziemnych zakładach górniczych, stosuje się sterowniki mikroprocesorowe, które umożliwiają między innymi zdalny nadzór nad pracą maszyn górniczych. W rozumieniu autorów, takie urządzenia mieszczą się w kategorii „innych układów funkcjonujących na podstawie technik informatycznych" i tym samym podlegają ochronie zgodnie z wymaganiami określonymi w ww. przepisie.

Wymagania serwisowe producentów maszyn górniczych, jak również warunki stawiane w umowach najmu czy leasingu przez właścicieli maszyn górniczych, obligują zakłady górnicze do udostępnienia zdalnego dozorowania pracy i parametrów eksploatacyjnych maszyn celem ich prawidłowej i bezpiecznej eksploatacji.

Zgodnie z §636 ust. 4 przytaczanego wcześniej Rozporządzenia Ministra Gospodarki, „kanał łączności konfigurują ręcznie pracownicy obsługi zakładu górniczego po telefonicznym uzgodnieniu przez serwis producenta, natomiast połączenie i dokonane czynności zostaną automatycznie odnotowane w systemie". Przepis ten odwzorowuje stan techniki z końca ubiegłego wieku, kiedy to jakakolwiek transmisja danych na odległość odbywała się za pomocą łącz modemowych. Stąd zapis o „ręcznej konfiguracji, po wcześniejszym uzgodnieniu telefonicznym". Dzisiaj, w erze powszechnego dostępu do Internetu oraz przy dostępności sprzętu i oprogramowania gwarantującego poufność i integralność zestawionego kanału łączności, dostęp

serwisowy może być zrealizowany w nowoczesny sposób, nie kolidujący jednak z obowiązującymi przepisami, z wykorzystaniem technologii Wirtualnych Sieci Prywatnych (VPN – Virtual Private Network) oraz systemu certyfikatów. Pomiędzy firewall'ami separującymi sieci wydzielone od sieci ogólnokopalnianych na poszczególnych kopalniach oraz firewall'em znajdującym się w punkcie styku z Internetem zostaną zestawione (na stałe) szyfrowane kanały VPN w sposób uniemożliwiający kontakt poszczególnych kanałów między sobą. Każdy z wykonawców zainteresowany zdalnym serwisowaniem systemów, zostanie wyposażony w odpowiedni login i hasło do poszczególnych systemów na zasadach uzgodnionych u Zamawiającego i zatwierdzonych przez KRZG poszczególnych kopalń. System zostanie skonfigurowany tak, by w danym czasie jeden Wykonawca mógł mieć dostęp tylko do jednej sieci wydzielonej. Do zdalnego dostępu do sieci zamawiającego zostanie wykorzystany mechanizm ssl/vpn. Na etapie inicjacji połączenia z siecią zamawiającego, komputer wykonawcy zostanie zweryfikowany pod względem podatności na zagrożenia (aktualność systemów antywirusowych, odpowiednie wersje systemu operacyjnego, itp.) oraz ważności certyfikatu dostępu. Każdorazowo dla dostępu serwisowego administrator systemu wystąpi do administratora bezpieczeństwa systemu o wydanie jednorazowego certyfikatu dostępu do sieci wydzielonej. Certyfikat ten zostanie wydany po akceptacji KRZG danej kopalni. Ważność certyfikatu określona będzie dla przedziału czasu, w którym KRZG oddziału zgadza się na prowadzenie zdalnych prac serwisowych w sieci wydzielonej. Poza okresem ważności certyfikatu, system kontroli zdalnego dostępu nie dopuści do połączenia zdalnego z siecią wydzieloną. Certyfikat zdalnego dostępu może być przesyłany do Wykonawcy z wykorzystaniem poczty e-mail. Przechwycenie przez osobę nieuprawnioną samego certyfikatu bez znajomości loginu i hasła, jak również znajomość loginu i hasła bez jednoczesnego posiadania ważnego certyfikatu nie umożliwia dostępu do chronionych zasobów sieci wydzielonej (chronionej) [3, 7]. Schemat połączeń przedstawia rys. 38.6.



Rys. 38.6 Zdalny dostęp serwisowy do sieci wydzielonych

Rozwiązanie jest zdaniem autorów zgodne z przepisem § 636 Rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002r. i jego wdrożenie nie wymaga uzyskania odstępstwa od stosowania ww. przepisu.

38.7 SYNCHRONIZACJA CZASU W URZĄDZENIACH ZNAJDUJĄCYCH SIĘ W SIECIACH WYDZIELONYCH

Potrzeba synchronizacji czasu w sieciach wydzielonych wynika z konieczności korelacji wielu zdarzeń, jakie zachodzą w ruchu zakładu górniczego i są rejestrowane przez urządzenia pracujące w różnych sieciach wydzielonych.

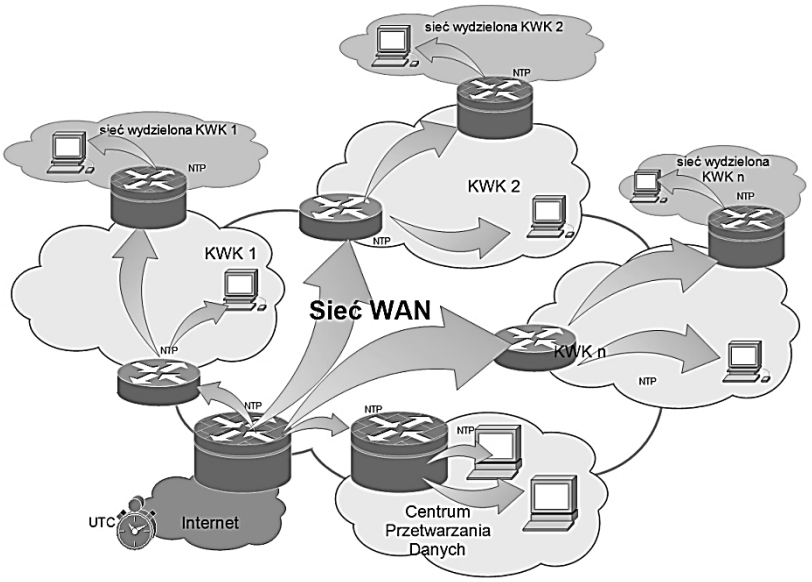
Ogólnokopalniana sieć teleinformatyczna Kompanii Węglowej S.A. jest synchronizowana ze źródłami czasu UTC (Universal Time Clock) klasy STRATUM-1, udostępnionymi w sieci INTERNET za pomocą mechanizmów NTP za pośrednictwem sieci WAN KW SA. Wszystkie urządzenia węzłowe sieci WAN Kompanii Węglowej SA są jednocześnie serwerami czasu NTP dla komputerów pracujących w sieci teleinformatycznej. Systemy operacyjne począwszy od MS Windows XP oraz UNIX i LINUX posiadają wbudowany w system mechanizm „klienta" NTP, co przy poprawnej konfiguracji pozwala założyć, że komputery te dysponują źródłem czasu bliskim czasowi UTC. Bardzo istotny jest również fakt, iż dla tych systemów operacyjnych dla obsługi mechanizmów NTP nie trzeba instalować dodatkowego oprogramowania [3, 7].

W związku z faktem, iż firewall, o którym mowa wyżej (rys. 38.3) zlokalizowany na granicy sieci wydzielonej i ogólnokopalnianej ma styk z obydwoma sieciami, może być zsynchronizowany ze źródłem czasu znajdującym się w sieci ogólnokopalnianej i być jednocześnie źródłem czasu dla sieci wydzielonej za pomocą protokołu NTP. Tym samym wszystkie urządzenia mogą być zsynchronizowane z tym samym źródłem czasu (niezależnie od tego „po której stronie lustra" się znajdują). Powielenie takiego rozwiązania we wszystkich kopalniach zapewnia również możliwość wykorzystania wskazań niektórych systemów kopalń sąsiadujących do identyfikacji i lokalizacji zdarzeń, jakie zaszły na granicy tych kopalń (np. wstrząsy sejsmiczne) [3]. Koncepcja rozwiązania przedstawiona jest na rys. 38.7.

Redundantne urządzenia stosowane zwykle w punkcie styku z Internetem, korzystanie z usług kilku niezależnych od siebie „dostawców Internetu", duża liczba serwerów będących źródłem czasu UTC w sieci Internet, jak również redundancja połączeń w sieci WAN Kompanii Węglowej S.A. powoduje że prawdopodobieństwo utraty synchronizacji czasu z czasem UTC jest pomijalnie małe.

Zakładając nawet całkowite zerwanie połączenia sieci KW S.A. z siecią Internet, nie powoduje to utraty synchronizacji czasu pomiędzy urządzeniami. Synchronizacja ta będzie dalej zachowana – w tej sytuacji już nie do źródła czasu UTC, lecz do głównego routera dostępowego [3].

Rozwiązanie powyższe jest zdaniem autorów zgodne z przepisem § 636 Rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002r. i jego wdrożenie nie wymaga uzyskania odstępstwa od stosowania ww. przepisu



Rys. 38.7 Synchronizacja czasu z wykorzystaniem mechanizmów NTP

38.8 UWAGI KOŃCOWE

Przedstawione w artykule rozwiązania z dziedziny bezpieczeństwa systemów teleinformatycznych nie są niczym nowym w dzisiejszym świecie IT. Wciąż jednak stanowią nowum w eksploatowanych systemach sieci wydzielonych zakładów górniczych. Wynika to nie tyle z ich sprzecznością z archaicznymi – jeśli chodzi o rozwiązania teleinformatyczne – przepisami Rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002 r. w sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych, lecz często wyłącznie z koniecznością wprowadzenia zmian w dokumentacji systemów eksploatowanych w sieciach wydzielonych. Przeważająca większość przedstawionych tu rozwiązań technicznych nie stoi w sprzeczności z przedmiotowym Rozporządzeniem. Natomiast w przypadku rozwiązań niezgodnych z obowiązującym przepisem §636 wspomnianego Rozporządzenia, należy wystąpić do Prezesa WUG z wnioskiem o zgodę na odstąpienie od obowiązku ich stosowania motywując swój wniosek obecnym stanem techniki, znacznie odbiegającym od stanu jaki był w momencie stanowienia tych przepisów. Dodatkowo warto wspomnieć, iż zastosowane w opisanych wyżej rozwiązaniach urządzenia IT są typowymi urządzeniami stosowanymi w informatyce. Gwarantuje to jednolitość systemów bezpieczeństwa, a co za tym idzie – łatwość zarządzania systemem, przejrzystość stosowanych procedur oraz niski koszt wdrożenia, utrzymania i eksploatacji.

LITERATURA

1. A. Dyczko, A. Wojaczek, (red): „Systemy telekomunikacyjne, monitoring i wizualizacja podziemnej eksploatacji złóż”, Wydawnictwo Fundacji dla AGH, Kraków 2011.
2. J. Korski, Z. Leks, A. Olszynka, Bezpieczeństwo systemów teleinformatycznych, [w:] Telekomunikacja i systemy bezpieczeństwa w górnictwie, Materiały z XXXVIII Konferencji Automatyka, Telekomunikacja, Informatyka ATI 2011, Wydawnictwo

Katedry Elektryfikacji i Automatyzacji Górnictwa Politechniki Śląskiej, Gliwice 2011.
3. Z. Leks, A. Olszynka, Bezpieczeństwo w sieciach wydzielonych, [w:] Materiały z XXXIX Konferencji Automatyka, Telekomunikacja, Informatyka ATI 2013, Wydawnictwo Katedry Elektryfikacji i Automatyzacji Górnictwa Politechniki Śląskiej, Gliwice 2013.
4. Z. Leks, A. Olszynka, Intranet rzeczy, czyli inne spojrzenie na systemy automatyki, monitorowania, bezpieczeństwa i łączności, [w:] Materiały z XL Konferencji Automatyka, Telekomunikacja, Informatyka ATI 2015, Wydawnictwo Katedry Elektryfikacji i Automatyzacji Górnictwa Politechniki Śląskiej, Gliwice 2015.
5. Z. Leks, A. Olszynka, Wyjaśnienia i informacje dodatkowe do wniosku o wyrażenie zgody na odstąpienie od wymagań § 636 ust 2 pkt 2 rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002r. „W sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych", Kompania Węglowa S.A. 2014r. (niepublikowane).
6. K. Miśkiewicz, A. Wojaczek, P. Wojtas, Systemy dyspozytorskie kopalń podziemnych i ich integracja, Wydawnictwo Politechniki Śląskiej, Gliwice 2011.
7. Regulamin Bezpieczeństwa Sieci Wydzielonych, Kompania Węglowa S.A., 2014r. (niepublikowane).
8. Rozporządzenie Ministra Gospodarki z dnia 28.06.2002r. „W sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych", Dz. U. z 2002r. nr 139 poz. 1169.
9. A. Wojaczek, A. Dyczko, (red): „Monitoring wybranych procesów technologicznych w kopalniach podziemnych", Wydawnictwo Katedry Elektryfikacji i Automatyzacji Górnictwa Politechniki Śląskiej, Gliwice 2015r.
10. Załącznik nr 2 z dnia 17.03.2014 r. do opinii technicznej nr 13/RG-1/2010 z dnia 16.06.2010 r. (wraz z Załącznikiem nr 1 do opinii z dnia 26.11.2012 r.) dotyczący: udostępniania danych z sieci wydzielonych podziemnych zakładów górniczych KW S.A. z wykorzystaniem tzw. serwera lustrzanego, Zespół Atestacji Katedry Elektryfikacji i Automatyzacji Górnictwa Politechniki Śląskiej, (niepublikowane).

Data przesłania artykułu do Redakcji: 03.2016
Data akceptacji artykułu przez Redakcję: 04.2016

mgr inż. Zenon Leks, inż. Adam Olszynka
Kompania Węglowa S.A.
Zakład Informatyki i Telekomunikacji
ul. Jastrzębska 10, 44-253 Rybnik, Polska
e-mail: z.leks@kwsa.pl |

MONITORING MASZYN I URZĄDZEŃ – KONCEPCJA TECHNICZNEJ REALIZACJI PRZEPISÓW

Streszczenie: *W artykule przedstawiono koncepcję ochrony systemów monitorowania i sterowania procesami przemysłowymi, przy jednoczesnym kontrolowanym dostępie do tych systemów oraz możliwość wymiany danych między nimi.*

Słowa kluczowe: *sieci wydzielone, bezpieczeństwo teleinformatyczne, serwer lustrzany, zdalny dostęp, systemy SCADA*

MONITORING OF MACHINES AND DEVICES – THE CONCEPT OF THE TECHNICAL IMPLEMENTATION OF THE REGULATIONS

Abstract: *We present the concept of protection Supervisory Control And Data Acquisition Systems both with unautorized access and posibility to data sharing betwen them.*

Key words: *dedicated IT networks, data security, data mirroring server, remote access, SCADA Systems*