ZENON LEKS

Zasady bezpieczeństwa informatycznego w świetle nowych przepisów

Nowe przepisy w sprawie szczegółowych wymagań dotyczących prowadzenia ruchu podziemnych zakładów górniczych, wprowadzone Rozporządzeniem Ministra Energii z dnia 23 listopada 2016 r. [1], w wielu miejscach obligują Kierownika Ruchu Zakładu Górniczego (KRZG) do określenia szczegółowych zasad realizacji zawartych w nich zaleceń. Tak jest również w części tego dokumentu dotyczącej bezpieczeństwa systemów informatyki przemysłowej eksploatowanych w kopalniach. Taka regulacja pozwala na ciągłe doskonalenie stosowanych rozwiązań z zakresu bezpieczeństwa teleinformatycznego. Artykuł jest przeglądem dostępnych rozwiązań bezpieczeństwa IT rekomendowanych przez autora do technicznej realizacji ochrony systemów informatycznych w przemyśle wydobywczym. Omówione tu rozwiązania mogą zostać przyjęte jako ogólne zasady bezpieczeństwa informatycznego w kopalniach, będąc podstawą do realizacji obowiązku nałożonego na KRZG w tym rozporządzeniu.

Słowa kluczowe: *bezpieczeństwo teleinformatyczne, systemy sterowania i nadzoru, SCADA, sieci wydzielone*

1. WPROWADZENIE I STAN PRAWNY

W dniu 1 lipca 2017 r. weszło w życie *Rozporządzenie Ministra Energii (RME) z dnia 23 listopada 2016 r. w sprawie szczegółowych wymagań dotyczących prowadzenia ruchu podziemnych zakładów górniczych* [1]. Rozporządzenie to w obszarze bezpieczeństwa systemów informatycznych wykorzystywanych w zakładach górniczych zastąpiło dotychczasowe *Rozporządzenie Ministra Gospodarki (RMG) z dnia 28 czerwca 2002 r. w sprawie bezpieczeństwa i higieny pracy*, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych [2]. W związku z faktem, że od opracowania poprzednich przepisów upłynęło kilkanaście lat, co w przypadku techniki informatycznej jest bardzo dużym okresem czasu, nowe przepisy stały się okazją do dostosowania mechanizmów bezpieczeństwa do obecnego stanu wiedzy i techniki w celu obrony przed nowymi zagrożeniami zewnętrznymi dla systemów informatycznych.

W aktualnym stanie prawnym wymagania dotyczące zabezpieczeń systemów informatycznych zostały zdefiniowane w § 750 rozporządzenia ministra energii [1]:

§ 750. 1. Oprogramowanie wykorzystywane do funkcjonowania systemów:

1) ogólnozakładowej łączności telefonicznej,
2) alarmowania,
3) gazometrycznych,
4) lokalizacji pracowników,
5) monitorowania zagrożenia tąpaniami

– zabezpiecza się.

2. Zabezpieczenie oprogramowania i danych systemów, o których mowa w ust. 1, spełnia następujące minimalne wymagania:
   1) dostęp do danych i oprogramowania spoza wyznaczonych punktów dostępu i bez zalogowania się z użyciem unikatowego hasła jest niemożliwy;
   2) dostęp do danych i oprogramowania jest zhierarchizowany;
   3) informacje dotyczące logowań i prób logowań oraz ingerencji i prób ingerencji w dane i oprogramowanie są automatycznie archiwizowane przez okres nie krótszy niż jeden rok, przy czym dla systemów, o których mowa w:
      a) ust. 1 pkt 1 i 2, automatycznie archiwizowane przez okres nie krótszy niż jeden rok są także bilingi połączeń i prób połączeń,

b) ust. 1 pkt 3–5, automatycznie archiwizowane przez okres nie krótszy niż jeden rok są także wyniki pomiarów wykonywanych przez urządzenia wchodzące w skład danego systemu;
4) wykonuje się kopie bezpieczeństwa bilingów połączeń i prób połączeń oraz wyników pomiarów;
5) oprogramowanie i dane chroni się przed złośliwym oprogramowaniem.

3. Czasy systemowe systemów, o których mowa w ust. 1, oraz systemu łączności kierownika akcji ratowniczej synchronizuje się z dokładnością do 0,1 s.
4. Szczegółowe zasady bezpieczeństwa informatycznego obowiązujące w przypadku systemów funkcjonujących na podstawie technik informatycznych w zakładzie górniczym są określane przez kierownika ruchu zakładu górniczego.

W odniesieniu do dotychczasowych przepisów zakres obligatoryjnego stosowania zasad bezpieczeństwa został ograniczony do następujących systemów: łączności, alarmowania, gazometrii, lokalizacji pracowników i monitorowania zagrożenia tąpaniami, w miejsce dotychczasowego, bardzo ogólnego stwierdzenia: innych układów funkcjonujących na podstawie technik informatycznych, co w dzisiejszym stanie techniki sprowadzałoby się do praktycznie wszystkich aspektów działalności kopalni, w tym do systemów ERP włącznie. W odróżnieniu od poprzednich przepisów [2], w obecnych [1] nie narzucono konkretnych rozwiązań bezpieczeństwa, pozostawiając KRZG opracowanie szczegółowych zasad bezpieczeństwa informatycznego, które mogą być sukcesywnie uaktualniane w miarę postępu technik informatycznych oraz pojawianiem się nowych zagrożeń dla systemów informatycznych. Rzecz jasna, bezpieczeństwo innych systemów może być chronione w identyczny sposób, jak systemów wymienionych w RME [1, 3].

W artykule zostaną omówione rozwiązania dotychczas stosowane w ochronie danych i systemów informatycznych działających w sieciach wydzielonych oraz rekomendowane przez autora rozwiązania bezpieczeństwa informatycznego do zastosowania w ochronie systemów informatyki przemysłowej.

Wraz ze wzrostem znaczenia systemów informatyki przemysłowej w literaturze przyjęło się nazywanie tych systemów systemami OT, w odróżnieniu od systemów informatyki ogólnej (IT). Dla potrzeb tego artykułu autor przyjął następującą definicję:

Systemy OT (Operational Technology) – przeznaczone do sterowania i/lub monitorowania procesów technologicznych, lub też bezpośredniego wpływania na działanie maszyn i urządzeń. Do systemów OT zalicza się systemy SCADA (Supervisory Control and Data Acquisition), CNC (Computer Numerical Control), PLC (Programmable Logic Controller) itp.

2. PRZEGLĄD DOTYCHCZAS STOSOWANYCH ROZWIĄZAŃ

Kopalnie eksploatują systemy OT, w tym wymienione w § 750 rozporządzenia [1] w stanie technicznym dostosowanym do wymagań stawianych przez dotychczasowe prawo. Wobec ograniczonych środków finansowych, jakie mogą one przeznaczyć na ich modernizację, należy przeprowadzić analizę dotychczasowych rozwiązań pod względem ich zgodności z nowym rozporządzeniem oraz dostosować dotychczasowe rozwiązania do współczesnego stanu techniki w dziedzinie bezpieczeństwa systemów informatycznych, a więc do zgodności z cytowanymi wyżej przepisami RME [1].

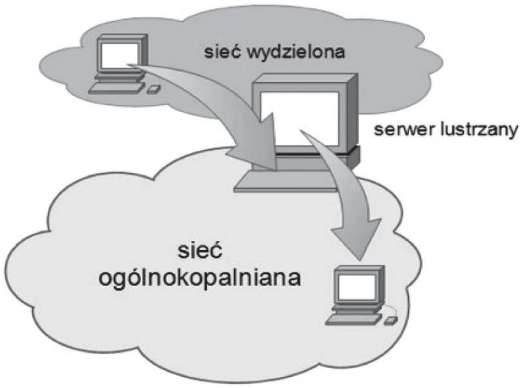
2.1. Bezpieczeństwo środowiska przetwarzania

Wprawdzie w obecnie obowiązującym rozporządzeniu nie używa się pojęć „sieć wydzielona” ani „serwer lustrzany”, jednak ze względu na powszechność ich stosowania w środowisku informatycznym górnictwa w artykule te pojęcia będą wykorzystane.

Praktycznie jedynym elementem zabezpieczającym sieć wydzieloną od sieci zewnętrznej (ogólnokopalnianej) jest tzw. serwer lustrzany [4]. 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. 1).

Idea serwera lustrzanego oraz separacji sieci wydzielonej od ogólnodostępnej jest powszechnie wykorzystywana we współczesnych rozwiązaniach bezpieczeństwa teleinformatycznego. Jednak realizacja separacji sieci za pomocą serwera plików budzi wątpliwości co do bezpieczeństwa takiego rozwiązania [5, 6]. Wśród możliwych metod ochrony systemów SCADA rozwiązanie takie zostało najgorzej ocenione przez brytyjskie Centre for Protection of National Infrastructure (CPNI) [5]. W skali piętnastopunktowej serwer z dwoma interfejsami sieciowymi przezna-

czonymi do separacji sieci uzyskał cztery punkty. Omawiane rozwiązanie zostało zaprojektowane w drugiej połowie ubiegłego wieku i w żaden sposób nie zabezpiecza urządzeń przed atakiem z udziałem exploitu o działaniu takim jak EternalBlue wykorzystanym do rozpowszechnienia w ostatnim czasie ramsonware WannaCry czy Petya.



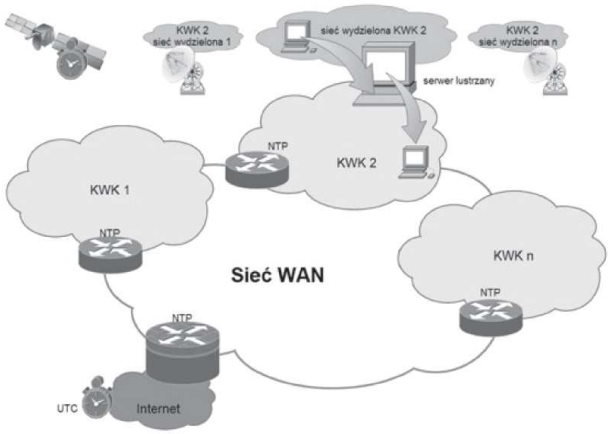
Rys. 1. Idea serwera lustrzanego [4]

Analizując rozwiązanie separacji sieci za pomocą „serwera lustrzanego", należy podkreślić wrażliwość takiego rozwiązania na czynnik ludzki, co jest związane z tym, że systemy operacyjne MS Windows, czy Linux stosowane w „serwerach lustrzanych" nie mają zaimplementowanej w swoich mechanizmach kontroli dostępu weryfikacji uprawnień użytkownika w zależności od interfejsu sieciowego, po którego stronie następuje logowanie. Tym samym użytkownik, logując się na serwer lustrzany, może przenieść dane z sieci ogólnodostępnej do sieci wydzielonej pomimo wyłączonego mechanizmu routingu między sieciami.

Mając na uwadze powyższe, zdaniem autora, należy zmienić sposób zabezpieczenia urządzeń w sieciach wydzielonych na nowocześniejszy, opisany w dalszej części artykułu.

2.2. Synchronizacja czasu

Bezdyskusyjny jest wymóg, by wszystkie urządzenia w sieci informatycznej miały zsynchronizowany czas z jednym wzorcem. Pozwoli to dokonać korelacji zdarzeń losowych, jakie mogą zajść w kopalni, w celu ustalenia ich kolejności i relacji przyczynowo-skutkowych. Pewną próbą rozwiązania tego problemu jest zastosowanie urządzeń wykorzystujących sygnał czasu pozyskiwany z odbiornika GSM. Rozwiązanie takie jest jednak mało wygodne. Wymaga instalacji dodatkowego oprogramowania na urządzeniach, które mają mieć zsyn-chronizowany czas (nie na wszystkich urządzeniach instalacja dodatkowego oprogramowania jest dopuszczalna i możliwa). Ponadto w każdej z sieci „wydzielonych", a jest takich sieci w kopalni co najmniej kilka, należałoby zainstalować zegary czasu. Z kolei sieci informatyczne ogólnokopalniane mają czas synchronizowany do źródeł czasu dostępnych w internecie z zegarów atomowych, co jest realizowane za pomocą protokołu NTP. Wobec wielu systemów będących dla urządzeń informatycznych źródłem czasu powstaje kwestia niezawodności takiego rozwiązania – praktycznie niemożliwa jest ciągła kontrola pracy wszystkich zegarów w sieciach informatycznych, a tym samym niemożliwe może być stwierdzenie, który zegar wskazuje czas poprawny w przypadku różnicy wskazań.



Rys. 2. Synchronizacja czasu – rozwiązanie dotychczasowe

Mając powyższe na uwadze, zdaniem autora, należy zmienić sposób synchronizacji czasu we wszystkich urządzeniach informatycznych funkcjonujących w kopalni na opisany w dalszej części artykułu.

2.3. Oprogramowanie stosowane w systemach sterowania i nadzoru

Stosowane oprogramowanie w kopalnianych systemach sterowania i nadzoru nie jest rozwiązaniem typowym, „pudełkowym", lecz zostało napisane z myślą o docelowym odbiorcy. Oprogramowanie to według opinii użytkowników oraz zapewnieniom producentów spełnia wszystkie wymagania bezpieczeństwa stawiane zarówno przez dotychczasowe, jak i obecne przepisy.

2.4. Ochrona przed złośliwym oprogramowaniem

Ze względu na obowiązujące dotychczas przepisy zakazujące przesyłania jakichkolwiek danych z sieci ogólnodostępnej do sieci wydzielonych nie stosowano ochrony antywirusowej oraz nie aktualizowano na bieżąco systemów operacyjnych. W niektórych przypadkach czynności takie były dokonywane doraźnie przez obsługę systemów lub firmy serwisujące.

2.5. Dostęp serwisowy do urządzeń w sieciach wydzielonych

Ze względu na ograniczenia w dotychczasowych przepisach nie stosowano zdalnego dostępu serwisowego do urządzeń znajdujących się w sieciach wydzielonych lub dostęp taki miał charakter incydentalny.

3. REKOMENDOWANE ROZWIĄZANIA BEZPIECZEŃSTWA SYSTEMÓW OT

Obligatoryjne wymagania co do bezpieczeństwa przemysłowych systemów informatycznych (systemów OT), zdefiniowane w § 750 RME, należy rozpatrywać w trzech sferach związanych z realizacją systemu bezpieczeństwa:

- wynikające z architektury środowiska przetwarzania, w tym dostępu do tych systemów;
- dotyczące zastosowanego oprogramowania;
- czynności administracyjnych w systemach OT.

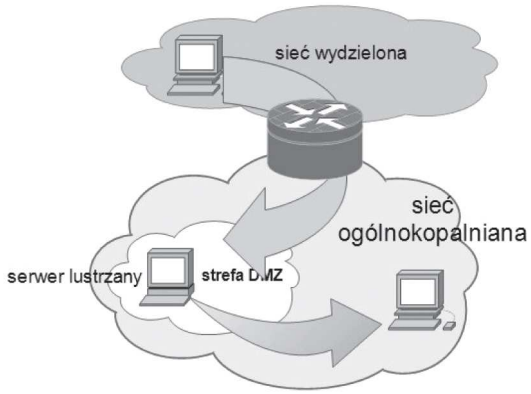
Patrząc z tej perspektywy na przepisy § 750 RME, wymagania co do stosowanego w tych systemach oprogramowania dotyczą konieczności utworzenia indywidualnych kont dla użytkowników i hierarchizacji uprawnień do systemu oraz rejestracji udanych i nieudanych prób logowań. W dużej części wymagania dotyczące archiwizacji danych również powinny być realizowane przez aplikację.

Z kolei wymagania ograniczenia lokalizacji, z których będą dostępne chronione systemy OT (ust. 2 pkt 1) oraz synchronizacji czasu w tych systemach (ust. 3), są wymaganiami co do architektury środowiska przetwarzania i sieci informatycznej wykorzystywanej do udostępnienia użytkownikom danych z tych systemów. W celu praktycznej realizacji tych wymagań należy odpowiednio skonfigurować sieć informatyczną. Wreszcie wymóg wykonywania kopii bezpieczeństwa danych (ust. 2 pkt 4) oraz ochrony przed szkodliwym oprogramowaniem (ust. 2 pkt 5) dotyczy wykonywania czynności administracyjnych przez obsługę informatyczną zabezpieczanych systemów.

3.1. Wymagania dotyczące architektury środowiska

3.1.1. Ograniczenie dostępu do danych

Rekomenduje się zachowanie idei „serwerów lustrzanych" przeznaczonych do udostępnienia danych przy dużej liczbie odbiorców danych w sieci ogólnodostępnej oraz w sytuacji, gdy dane przed ich udostępnieniem wymagają przetworzenia wymagającego dużej ilości operacji obciążających serwer. Wtedy serwer lustrzany dodatkowo zwiększa bezpieczeństwo sieci przemysłowych przez odciążenie infrastruktury od obsługi żądań osób niebiorących bezpośredniego udziału w procesie nadzoru produkcji. Serwer taki nie będzie jednak pełnił funkcji urządzenia separującego środowisko sieci ogólnodostępnej od sieci chronionej (wydzielonej). To będzie realizowane przez sprzętowy firewall, którego zadaniem jest zabezpieczenie urządzeń znajdujących się w sieci wydzielonej od ingerencji ze strony użytkowników, przy jednoczesnym umożliwieniu transmisji danych z sieci wydzielonej do „serwera lustrzanego" i z „serwera lustrzanego" do sieci ogólnokopalnianej. Dla „serwera lustrzanego" w konfiguracji firewalla zostanie zdefiniowana odrębna sieć – tzw. strefa DMZ (demilitarized zone). W strefie tej serwer jest chroniony przed ewentualną ingerencją czynników zewnętrznych (użytkownicy, szkodliwe oprogramowanie) nie tylko za pomocą mechanizmów systemu operacyjnego, ale również mechanizmów sieciowych firewalla (rys. 3) [7, 8].



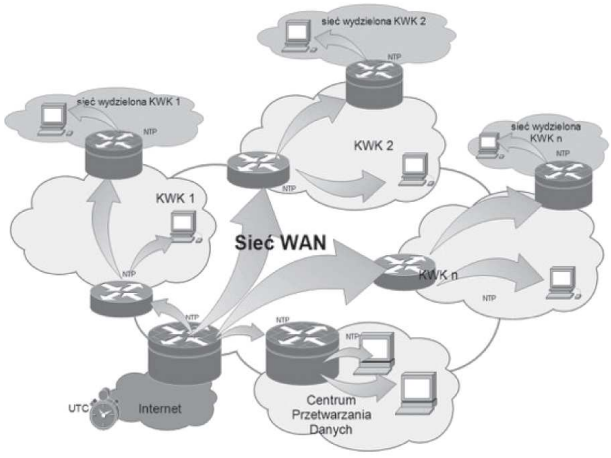
Rys. 3. Lokalizacja serwerów lustrzanych w strefie DMZ [4]

Takie rozwiązanie zabezpieczenia sieci wydzielonej we wspomnianym wyżej opracowaniu Centre for Protection of National Infrastructure (CPNI) [5] zostało ocenione na 12,5 punktów (w piętnastostopniowej skali).

Ograniczenie dostępu do danych z wyznaczonych punktów, o czym mowa w § 750 ust. 2 pkt 1 będzie realizowane z wykorzystaniem mechanizmów sieciowych: sieci VLAN lub poszczególnych adresów IP, które zostaną przyporządkowane do stref zdefiniowanych urządzeniu firewall.

3.1.2. Synchronizacja czasu

Zastosowanie firewalla do zabezpieczenia sieci wydzielonej umożliwia również łatwe spełnienie wymagań synchronizacji czasu w urządzeniach, o których mowa w § 750 ust. 1 RME [1]. Ogólnokopalniana sieć teleinformatyczna Polskiej Grupy Górniczej (PGG) jest zsynchronizowana ze źródłami czasu UTC (Universal Time Clock, Coordinated Universal Time) klasy STRATUM-1, udostępnionymi w sieci INTERNET za pomocą mechanizmów protokołu NTP, za pośrednictwem sieci WAN. Wszystkie urządzenia węzłowe sieci WAN skonfigurowano w taki sposób, że są jednocześnie serwerami czasu NTP dla komputerów pracujących w sieci teleinformatycznej (rys. 4). Z kolei 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.



Rys. 4. Synchronizacja czasu z wykorzystaniem mechanizmów NTP [4]

W związku z tym, że firewall zabezpieczający sieć wydzieloną (rys. 3, rys. 4) 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 w sieci PGG mogą być zsynchronizowane z tym samym źródłem czasu. 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) [4].

Redundantne urządzenia stosowane zwykle w punkcie styku z internetem, korzystanie z usług kilku niezależnych od siebie dostawców sieci internetowych, duża liczba serwerów będących źródłem czasu UTC w sieci, jak również redundancja połączeń w sieci WAN PGG gwarantuje, że prawdopodobieństwo utraty synchronizacji czasu z czasem UTC jest pomijalnie małe. Zakładając nawet całkowite zerwanie połączenia sieci PGG z internetem, 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 [4].

Takie rozwiązanie jest już stosowane w PGG dla sieci ogólnodostępnej. Uzyskana dokładność synchronizacji czasu jest o rząd lepsza od wymaganej przepisem § 750 ust. 3 RME.

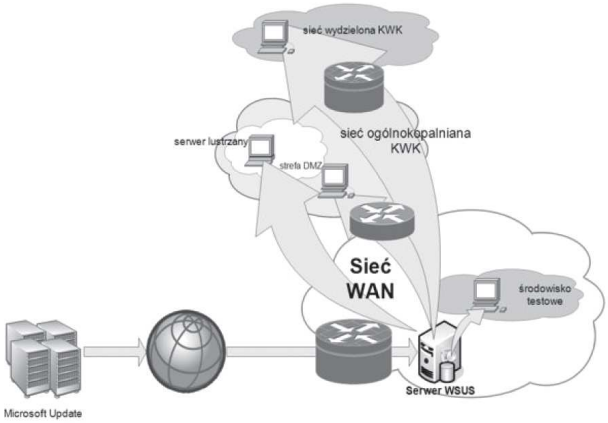
3.1.3. Zabezpieczenie przed złośliwym oprogramowaniem

Powszechnie uważa się, że wystarczającym zabezpieczeniem przed złośliwym oprogramowaniem jest zapewnienie aktualizacji systemów operacyjnych dzięki bieżącemu wgrywaniu poprawek publikowanych przez producenta oraz zainstalowaniu w komputerze systemu antywirusowego. Takie postępowanie w większości przypadków jest wystarczające dla systemów informatycznych wykorzystywanych w domu i do prac biurowych. W systemach sterowania i nadzoru może się okazać niewykonalne lub niebezpieczne. Aktualizacja systemu operacyjnego lub system antywirusowy mogą w taki sposób wpływać na pracę komputera, że zakłócają działanie systemu produkcyjnego. Oczywiście dobrą praktyką jest przed implementacją takich zmian w systemie produkcyjnym sprawdzenie poprawności ich działania w środowisku

testowym, co jednak ze względów technicznych i organizacyjnych może być niewykonalne. Kopalnia nie posiada drugiego, testowego systemu gazometrycznego, łączności, alarmowania itp. Zdaniem autora, rolą producenta ww. systemów powinno być informowanie o konieczności i celowości instalowania w nich poprawek lub systemów antywirusowych. Producenci oprogramowania systemów przemysłowych powinni być zobowiązani w ramach umów serwisowych do przesyłania na bieżąco informacji o konieczności aktualizacji systemów ich autorstwa lub o zagrożeniach wynikających z aktualizacji dla poprawnego działania systemów. Inaczej jest z systemami przeznaczonymi do prezentacji danych, które to systemy można odtworzyć w środowisku testowym i wypróbować ich pracę po implementacji poprawek systemu operacyjnego lub zbadać wpływ systemów antywirusowych na ich działanie.

Aktualizacja systemów w sieciach wydzielonych odbywać się będzie z serwerów dystrybucji poprawek i sygnatur antywirusowych znajdujących się w sieci PGG (a nie bezpośrednio z internetu), administrowanych przez uprawnione do tego osoby według polityki ustalonej dla poszczególnych urządzeń. Takie rozwiązanie jest z powodzeniem stosowane w ogólnokopalnianej sieci IT PGG.

Rysunek 5 [4] przedstawia przykład wdrożenia aktualizacji systemów operacyjnych firmy Microsoft za pomocą systemu WSUS (Windows Server Update Services).



Rys. 5. Aktualizacja systemów operacyjnych [4]

Odrębnym tematem jest zapewnienie bezpieczeństwa systemów, na które z różnych względów nie można aplikować poprawek i/lub systemów antywirusowych. Takie systemy powinny być wyodrębnione do oddzielnych sieci (mechanizm VLAN) i stref bezpieczeństwa (mechanizmy firewalla), a ich komunikacja z innymi systemami zlokalizowanymi w innych strefach bezpieczeństwa powinna być ograniczona co do kierunku przesyłania informacji oraz urządzeń, które mogą się ze sobą komunikować. Taka konfiguracja zostanie utworzona na urządzeniu firewall separującym sieci [7, 8].

Dalszym zabezpieczeniem dla takich systemów jest ograniczenie praw administracyjnych użytkowników i zablokowanie im dostępu do portów USB w celu podłączenia nośników pamięci oraz wdrożenie mechanizmów ochrony sieci typu NAC (Network Admission Control) [9]. Takie rozwiązanie pozwoli na ograniczenia źródła zagrożeń. Utrudni to jednak czynności serwisowe, gdyż dla ich wykonania każdorazowo będzie konieczne nadanie serwisantowi uprawnień do włączenia do chronionego systemu nośnika pamięci lub podłączenia komputera do chronionej sieci (w przypadku stosowania systemu typu NAC).

Istotą działania systemu NAC jest uniemożliwienie dopuszczenia do pracy w sieci jakichkolwiek obcych (nieznanych systemowi) urządzeń przed ich weryfikacją pod względem aktualności systemów zabezpieczeń (aktualność oprogramowania antywirusowego, systemu operacyjnego itp.). Komputer niespełniający wymagań bezpieczeństwa zostanie przekierowany do podsieci (VLAN-u) sieci ogólnokopalnianej, w której będzie mógł pobrać aktualizacje sygnatur oprogramowania antywirusowego czy poprawek do systemu operacyjnego. Dopiero po zainstalowaniu takich aktualizacji będzie mógł podjąć pracę w sieci wydzielonej.

3.2. Wymagania dotyczące oprogramowania

Przepisy § 750 RME stawiają nowe wymagania co do oprogramowania wykorzystywanego w systemach informatycznych OT tam wymienionych. Realizacja wymagań dotyczących stosowania unikatowych kont użytkowników i hierarchii uprawnień dla użytkowników jest uzależniona od konfiguracji systemu przez administratora, a nie samego oprogramowania. Według zapewnień autorów systemów, w oprogramowaniu spełnione są również wymagania dotyczące rejestracji logowań i prób logowań oraz automatyzacji wykonywania archiwizacji danych. Według obserwacji autora, systemy sterowania i nadzoru nie posiadają dokumentacji pozwalającej na skorzystanie ze zgromadzonych w nich danych przez służby kopalni, dla potrzeb budowy innych systemów nadzoru lub zobrazowania danych w innych systemach. Niesie to za

sobą dodatkowe koszty, jakie kopalnia musi ponieść przy wdrażaniu nowych systemów typu SCADA. Zdaniem autora, przed planowanym zakupem nowych rozwiązań należy zażądać dostarczenia szczegółowej dokumentacji w tym zakresie. Ponadto, obecnie eksploatowane systemy są tak skonstruowane, że bez technicznego uzasadnienia, do swojego działania wymagają uprawnień administratora komputera, na którym są uruchomione. Tu również w przyszłych postępowaniach przetargowych należy postawić wymagania możliwości eksploatacji zamawianego systemu bez konieczności nadania użytkownikowi uprawnień administratora komputera.

3.3. Wymagania dotyczące administrowania systemami OT

Przepisy § 750 RME wprost definiują minimalny zakres czynności związanych z użytkowaniem systemów wymienionych w ww. przepisie, które polegają na właściwym administrowaniu kontami użytkowników (imienne konta i hierarchiczne uprawnienia) oraz wykonywaniu codziennych rutynowych czynności polegających na archiwizacji danych i wykonywaniu kopii bezpieczeństwa.

Zdaniem autora, przy organizacji pracy służb odpowiedzialnych za prawidłowe funkcjonowanie systemów OT, w szczególności systemów wymienionych w § 750 RME, należy rozdzielić odpowiedzialność za bieżącą eksploatację systemów od administrowania i konfiguracji systemami bezpieczeństwa. Zwiększy to poziom bezpieczeństwa dzięki uniemożliwieniu użytkownikom nadużywania uprawnień administracyjnych przy bieżącej eksploatacji systemów.

4. UWAGI KOŃCOWE

Nowe przepisy RME [1], obowiązujące od 1 lipca 2017 r., pozwalają na wdrożenie nowoczesnych rozwiązań bezpieczeństwa, pozostawiając dużą swobodę w ich wyborze. Rekomendowane tu rozwiązania mają na celu zwiększenie bezpieczeństwa danych oraz zwiększenie niezawodności systemów pracujących w sieciach wydzielonych. Zastosowane w opisanych wyżej rozwiązaniach urządzenia i systemy są typowymi urządzeniami stosowanymi w informatyce. Gwarantuje to jednolitość systemów bezpieczeństwa, a co za tym idzie – łatwość zarządzania systemem, przejrzystość stosowanych procedur i niski koszt wdrożenia.

Literatura

[1] *Rozporządzenie Ministra Energii z dnia 23 listopada 2016 r. w sprawie szczegółowych wymagań dotyczących prowadzenia ruchu podziemnych zakładów górniczych*, Dz.U. z 2017 r., poz. 1118.

[2] *Rozporządzenie 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. z 2002 r., poz. 1169.

[3] PN-EN 61508-1: *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne*.

[4] Leks Z., Olszynka A.: *Bezpieczeństwo w sieciach wydzielonych*, w: *Materiały XXXIX Konferencji Sekcji Cybernetyki w Górnictwie KG PAN „Automatyka Telekomunikacja Informatyka ATI'2013"*, Wydawnictwo Katedry Elektryfikacji i Automatyzacji Górnictwa Politechniki Śląskiej, Gliwice 2013.

[5] Byres E., Karsch J., Carter J.: *Firewall Deployment for SCADA and Process Control Networks*, Centre for Protection of National Infrastructure, Government Digital Service, 2005.

[6] Homeland Security: *Control Systems Cyber Security Defense in Depth Strategies*, Control Systems Security Center 2006.

[7] Stawowski M., Karaś S., Wal R.: *Sieci VLAN i bezpieczeństwo*, ArsKOM, Warszawa 2009.

[8] Stawowski M.: *Zapory sieciowe firewall. Projektowanie i praktyczne implementacje na bazie zabezpieczeń Check Point NGX*, ArsKOM, Warszawa 2006.

[9] Jazib Frahim, David Ehite Jr: *Cisco Network Admission Control, Volume II: NAC Framework Deployment and Trouble-shooting*, Networking Technology Series, Cisco Press, 2006.

mgr inż. ZENON LEKS
Polska Grupa Górnicza S.A.
Oddział Zakład Informatyki i Telekomunikacji
ul. Jastrzębska 10, 44-253 Rybnik
z.leks@pgg.pl