http://dx.doi.org/10.7494/miag.2017.4.532.49

ZENON LEKS

Principles of IT security in light of new regulations

In many places, the new regulations on the detailed requirements of underground mining operations introduced by the Minister of Energy on November 23, 2016, obligate the head of a coal mine to specify the detailed rules of implementation of the recommendations contained therein. This article is a review of the available IT security solutions recommended by the author for the technical implementation of the protection of SCADA systems. The solutions described here may be adopted as IT security regulations in coal mines.

Key words: *IT safety, SCADA systems, separated networks*

1. INTRODUCTION AND LEGAL STATUS

On July 1, 2017, the ordinance of the Minister of Energy (RME) from November 23, 2016, regarding the detailed requirements of underground mining operations published in (Dz.U. 2017, 1118) entered into force [1].

This regulation in the area of IT systems used in the technical aspect of mining industry operations has replaced the current regulation of the Minister of Economy (RMG) from June 28, 2002, about Health and Safety, mining operations, and specialized fire protection in underground mining [2].

Due to the fact that it had been over a dozen years since the preparation of the previous regulations (which is a very long period of time in the case of IT), the new provisions have become an opportunity to adapt security mechanisms to the current state of the art in order to defend against new external threats to IT systems.

In the current state of law, an IT system's security requirements are defined in §750 of the Regulation of the Minister of Energy [1]:

§ 750. 1. Software used in following systems:
1) company-wide telephone communications,
2) alarm systems,
3) gasometrical,
4) employee localization,
5) rock burst-threat monitoring

– is secured.

2. The protection of software and system data referred to in Par. 1 meets the following minimum requirements:
   1) Access to data and software outside designated access points and without having to log in with a unique password is not possible;
   2) Access to data and software is hierarchical;
   3) Information on login and login attempts as well as interference and tampering of data and software are automatically archived for a period of not less than one year, with the systems referred to in:
      a) Par. 1, Pts. 1 and 2 automatically archived for a period of not less than one year are also call logs and connection attempts,
      b) Par. 1, Pts. 3–5 automatically archived for a period not shorter than one year, are also the results of measurements performed by devices included in the particular system;
   4) Backups of connection, connection attempt logs and measurement results are also performed;
   5) Software and data are protected against malware.
3. System times of the systems referred to in Par. 1, and the rescue manager communication system synchronizes with an accuracy of 0.1 s;
4. Detailed IT security rules applicable to systems operating on the basis of information technology in a mining plant are determined by the mining plant operations manager.

With regard to the existing regulations, the scope of the mandatory application of the principles of safety is limited to these systems: communication, alarming, gasometrical, employee localization, and rock burst-threat monitoring (in place of the previous very general statement): Other systems operating on the basis of information technology (as in the present state of the art) would be reduced to practically all aspects of mine operations, including ERP systems. Unlike previous regulations [2], the author of the Regulation from November 23, 2016 [1], does not impose specific security solutions, leaving the Mining Plant Manager to develop detailed IT security rules that can be updated on a continuous basis as information technology advances and new threats to information systems emerge. Of course, the security of other systems can be protected in the same way as the systems mentioned in the RME [1, 3].

This article will discuss the solutions used to protect data and information systems operating in separated networks as well as the author's recommended IT security solutions for use in the protection of industrial computer systems.

With the rise of the importance of industrial information systems, the term OT systems was used in the literature to refer to these systems (as opposed to IT systems). For the purposes of this article, the author has adopted the following definition:

OT systems (Operational Technology) – an information system designed to control and/or monitor technological processes or directly affect the operation of machinery and equipment. OT systems include SCADA (Supervisory Control and Data Acquisition), CNC (Computer Numerical Control), PLC (Programmable Logic Controller) etc.

2. OVERVIEW OF THE CURRNET SOLUTIONS

Mines are currently operating OT systems, including those listed in §750 of the ordinance from November 23, 2016 [1], in a state of art adapted to the requirements of the current law. Due to the limited financial resources that mines can spend on modernization of these systems, it is necessary to analyze existing solutions in terms of their compliance with the new regulation and adapt existing solutions to the current state of the art in the field of information system security to comply with the above-mentioned RME regulations [1].

2.1. Security of computing environment

Although the terms "separate network" and "mirror server" are not used in the current regulation, these terms will be used in this article because of their widespread application in the mining IT environment.

Virtually, the only security feature of a "separated network" from an external network (a general-purpose network) is the so-called "mirror server" [4]. The "general" and "separated" networks are connected by means of a "mirror server" equipped with two network interfaces, which act as a file server between a separated and public networks (Fig. 1).

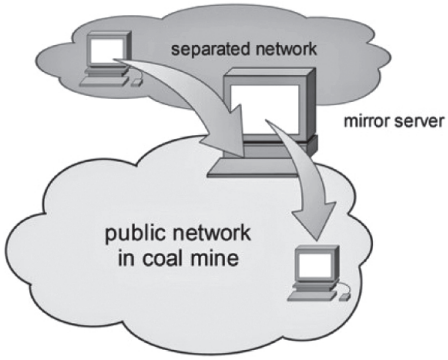


Fig. 1. Mirror server concept [4]

The idea of a "mirror server" and the separation of "separated networks" from public networks is widely used in today's ICT security solutions. However, the separation of the network with the file server raises doubts about the security of such a solution [5, 6]. Among the possible ways to protect SCADA systems, such a solution has been rated worst by the UK Centre for the Protection of National Infrastructure (CPNI) [5]. On a 15-point scale, a server with two network interfaces destined for network separation scored 4 points. The solution was designed in the second half of the last century and does not in any way protect against exploits such as EternalBlue, which has recently been used to distribute WannaCry or Petya ransomware.

When analyzing a network-separation solution, the sensitivity of such a solution to the human factor should be emphasized, because the MS Windows or Linux operating systems used in "mirror servers" do not have ability to verify access rights implemented in their access control mechanisms depending on the network interface used to log in. Thus, the user logging on to the mirror server can move data from

the public network to the separated network despite the routing mechanism being switched off between the networks.

Bearing in mind the above, it is necessary in the author's opinion to change the way of securing devices in networks separated into the more-advanced way described in the following article.

2.2. Time synchronization

It is unquestionable that all devices in a computer network should have a synchronized time with one pattern. This will allow us to correlate events to determine their order and causal relationships in the event of random events that may occur in the mining plant. One way to solve this problem is to use devices that use the time signal from a GSM receiver. Such a solution, however, is inconvenient, because it requires the installation of additional software on devices that have a synchronized time (the installation of additional software is not possible or allowed on some devices). Also, in each of the "separated" networks (and there are such networks at the mine facility at least a few), it would be necessary to install such time clocks. On the other hand, the general-purpose computer networks have time synchronized to the time sources available on the Internet from atomic clocks, which is accomplished via NTP protocol. It is virtually impossible to continually control the operation of all clocks in IT networks; therefore, it is impossible to determine which clock points to the correct time when there is difference in indications.

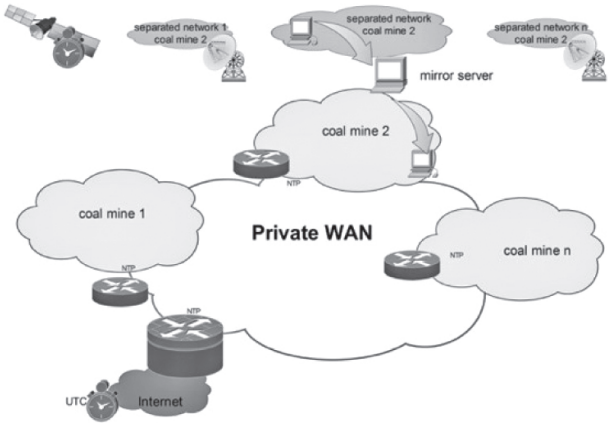


Fig. 2. Time synchronization – present solution

Bearing in mind the above, the author believes that the time synchronization should be changed in all IT devices operating in the mine as described in the following article.

2.3. Software used in control and monitoring systems

The software used in mine control and surveillance systems is not a typical commercial solution but was written for the target audience. According to users and manufacturers assurances, this software meets all the safety requirements of the previous and current regulations.

2.4. Protection against malware

Due to the existing regulations prohibiting the transmission of any data from a public network to the separated networks, no anti-virus protection was applied, and the operating systems were not updated on an ongoing basis. In some cases, such operations were performed on an ad hoc basis by system support or service companies.

2.5. Service access for devices in separated networks

Due to limitations in the current regulations, remote service access to devices located in separated networks was not used (or the access was incidental).

3. RECOMMENDED SAFETY SOLUTIONS OF OT SYSTEMS

Obligatory requirements for the safety of industrial information systems (OT systems) as defined in §750 RME [1] are to be considered in three aspects in terms of the implementation of a security system:

- resulting from the architecture of the processing environment, including access to these systems;
- about the software used;
- administrative tasks in OT systems.

Looking from this perspective on the provisions of §750 of the RME, the requirements for the software used in these systems are set out in Par. 2, Points 1, 2, and 3 and concern the need to create individual accounts for users and system hierarchies and record successful and failed login attempts. Much of the requirements for data archiving should also be realized by the application. On the other hand, the requirements for restricting locations from the protected OT systems can be accessed (Par. 2, Pt. 1), and the time synchronization in these systems (Par. 3) are requirements for the architecture of the processing environment and computer network used to provide users

with data from these systems. The practical implementation of these requirements requires the proper configuration of the IT network. Finally, the requirement to back up data (Par. 2, Pt. 4) and protection against malware (Par. 2, Pt. 5) should be handled by the IT services of the secured systems.

3.1. Requirements for the architecture of the environment

3.1.1. Data access restriction

It is recommended to maintain the concept of "mirror servers" when shared data is intended to be available to a large number of data receivers on a public network and where the data prior to use requirs to be processed (requiring a large amount of server load). In this way, the "mirror server" further enhances the security of industrial networks by relieving the infrastructure from handling requests from people not directly involved in the production process. However, this server will not be the role of the device separating the public network environment from the protected (separated) network. This feature will be implemented by a hardware firewall, which is designed to protect the devices located on the separated network (separated from user interference) while also allowing the transmission of data from the separated network to the "mirror server" and from the "mirror server" to the public network. For the "mirror server" in the firewall configuration, a separate network will be defined – the so-called demilitarized zone (DMZ). In this zone, the server is protected against possible interference by external factors (users, malicious software) not only by operating system mechanisms but also by the network mechanisms of the firewall (Fig. 3) [7, 8].

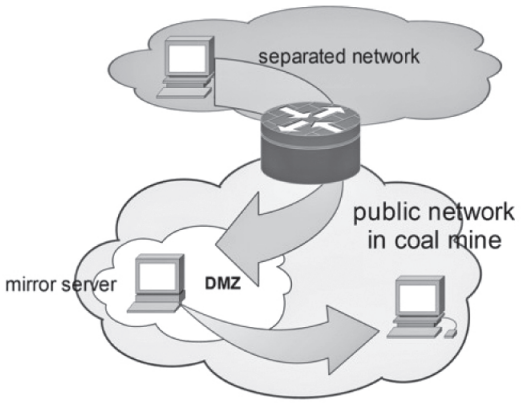


Fig. 3. Mirror server localized in demilitarized zone [4]

This solution of securing the separated network was in the above-mentioned study from the Centre for the Protection of National Infrastructure (CPNI) [5] was rated at 12.5 points (on the 15-point scale).

Limitation of access to the designated access points, as referred to in §750, Sec. 2, Point 1 will be implemented using network mechanisms: VLANs or individual IP addresses that will be assigned to the zones defined by the firewall device.

3.1.2. Time synchronization

The use of a firewall to secure a dedicated network also makes it easy to meet time synchronization requirements in devices, referred to in §750 (1) of the RME [1]. A mine-wide IT network in PGG is synchronized with the STRATUM-1 class Universal Time Clock (Coordinated Universal Time) server, which is available on the INTERNET via NTP over the WAN. All WAN node devices are configured in such a way that they are both NTP time servers for computers operating in a teleinformatic network (Fig. 4). On the other hand, operating systems starting from MS Windows XP, UNIX, and LINUX have a built-in NTP "client" mechanism that, when correctly configured, assumes that these machines have a source of time close to the UTC time. It is also important that no additional software is required for these operating systems to support NTP.

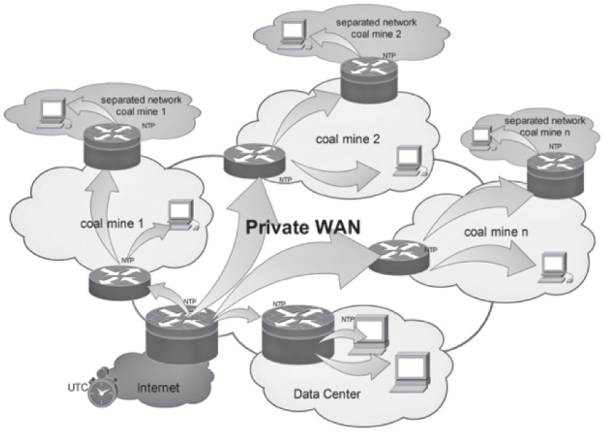


Fig. 4. Time synchronization using NTP protocol [4]

Due to the fact that the firewall protecting the "separated network" (Figs. 3 and 4) is located on the boundary of the separated and general networks, it has contact with both networks and can be synchronized with the time source located in the public network and, simultaneously, a source of time for the separated network using NTP protocol. Thus, all

devices in the PGG network can be synchronized with the same time source. The replication of such a solution in all mines also provides the possibility of using the indications of some neighboring mine systems for identifying and locating events at mine boundaries (e.g., seismic waves) [4].

Redundant devices usually used at the point of contact with the Internet enable the use of several independent "ISPs," a large number of UTC time servers on the Internet, and WAN PGG redundancy guarantees that the probability of losing time synchronization with UTC time is negligible. Even if PGG is completely disconnected from the Internet, this will not cause devices to lose time synchronization. In this case, the synchronization will continue not with the UTC source but with the main access router [4].

This solution is already used in PGG for public access networks. The accuracy of time synchronization is better than that provided by §750, Sec. 3 RME [1].

3.1.3. Protection against malware

It is generally believed that sufficient protection against malware is to provide an update to operating systems by running the up-to-date fixes published by the manufacturer and having an anti-virus system installed on the computer. This is the case for most home and office IT systems. In control and surveillance systems, this may be unrealistic or dangerous. It may be that updating operating system or installing antivirus system in such way affects the operation of the computer so it may interfere with the operation of the production system. Of course, a good practice is checking the correctness of the operation in a test environment before implementing such changes in the production system; however, it may not be feasible for technical and organizational reasons. Mines may not have second gasometrical systems, communications, alarms, etc. that can be used for testing purposes. According to the author, the role of the manufacturer of the above-mentioned systems should be to inform about the necessity and purpose of installing patches or anti-virus systems in them. Manufacturers of industrial system software should be obligated under maintenance contracts to keep up-to--date on the need to update their systems or the risks of updating for the correct functioning of the systems. This is not the case for systems that are designed to present data that can be reproduced in a test environment and tested for performance after the operating system patch is implemented or to investigate the impact of antivirus systems on their performance.

System upgrades in separated networks will be made from patch distribution servers and anti-virus signatures located in the PGG network (rather than directly from the Internet), administered by authorized individuals according to individual policies set for each device. This solution is successfully used in the IT network of PGG.

Figure 5 [4] shows an example of deploying Microsoft operating system updates using Windows Server Update Services (WSUS).

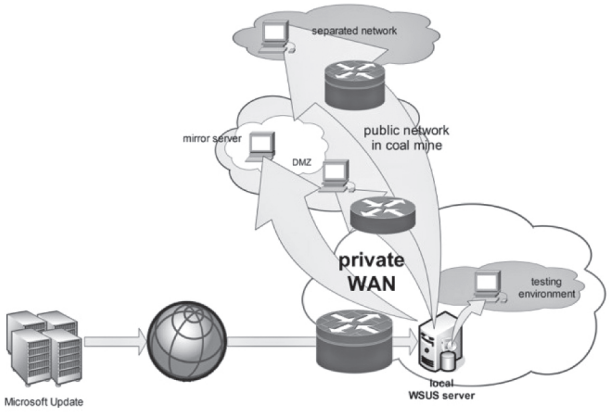


Fig. 5. Updating Operating Systems [4]

A separate topic is the security of systems that cannot be patched and/or anti-virus systems installed for various reasons. Such systems should be separated into separate networks (VLANs) and security zones (firewalls), and their communication with other systems located in other security zones should be limited to the direction of the transmission of information and devices that can communicate with one another. This configuration will be created on the network isolation firewall device [7, 8].

Further protection for such systems is to limit user administrative rights and block access to USB ports for connecting storage media and implementing Network Admission Control (NAC) [9]. Such solutions will reduce the source of threats. This will make it difficult to service because it will be necessary to assign rights to the service technician to connect storage media to a protected PC or to connect the computer to a protected network (for NAC systems).

The essence of the NAC system is to prevent any unauthorized (unknowable) system from being allowed to work on the network before they are verified in terms of security systems (antivirus software, operating system, etc.). A non-compliant computer will be

redirected to a subnet (VLAN) of the mine-wide network in which it will be able to download antivirus software signature updates or patches to the operating system. Only after installing such updates will the computer be able to work on a separate network.

3.2. Software requirements

The provisions of §750 of the RME put new requirements on the software used in the OT IT systems mentioned there. Implementing the requirements for using unique user accounts and user permission hierarchies depends on the system configuration of the administrator rather than the software itself. According to the author's assurances, the software also meets the requirements for logon registration, logon attempts, and the automation of data archiving. According to the author's observation, the control and surveillance systems do not have the documentation that allow the data collected by this system to be used by mines for the purpose of constructing other surveillance systems or displaying data in other systems. This adds to the additional costs that the mine must incur when implementing new SCADA systems. According to the author, before the planned purchase of new solutions, it is necessary to request delivery of detailed documentation in this regard. In addition, the systems currently in use are designed in such a way that, without technical justification, they require administrator privileges on the computer where they are running. Also in future tendering procedures, you should set requirements for the operation of the ordered system without having to give the user the authority of the computer administrator.

3.3. Requirements for administration of OT systems

The provisions of §750 of the RME explicitly define the minimum scope of activities related to the use of the systems mentioned in the afore-mentioned provision, which consists of the proper administration of user accounts (registered accounts and hierarchical permissions) and daily routine activities of data archiving and backup.

According to the author, when organizing the work of the services responsible for the proper functioning of the OT systems (the systems listed in §750 RM in particular), the responsibility for the day-to-day operation of the systems should be separated from the administration and configuration of security systems. This will increase the level of security by preventing users from misusing administrative privileges in the current system.

4. FINAL REMARKS

The new RME regulations [1], which came into force on July 1, 2017, allow for the implementation of modern security solutions, leaving a great deal of freedom in their choice. The solutions recommended here are to increase data security and increase the reliability of systems running on separated networks. The devices and systems used in the solutions described above are typical devices used in computer science. This guarantees the uniformity of security systems and, therefore, the ease of system management, transparency of procedures, and low implementation cost.

References

[1] *Rozporządzenie Ministra Energii z dnia 23 listopada 2016 r. w sprawie szczegółowych wymagań dotyczących prowadzenia ruchu podziemnych zakładów górniczych*, Dz.U. 2017, 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. 2002, 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*, in: *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] Frahim J., Ehite D. Jr: *Cisco Network Admission Control, Volume II: NAC Framework Deployment and Troubleshooting*, Networking Technology Series, Cisco Press, 2006.

ZENON LEKS, M.Sc., Eng.
Polska Grupa Górnicza
Oddział Zakład Informatyki i Telekomunikacji
ul. Jastrzębska 10, 44-253 Rybnik, Poland
z.leks@pgg.pl

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].

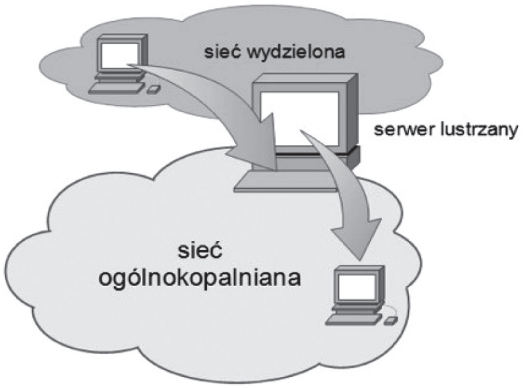
2.1. Bezpieczeństwo środowiska przetwarzania

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.



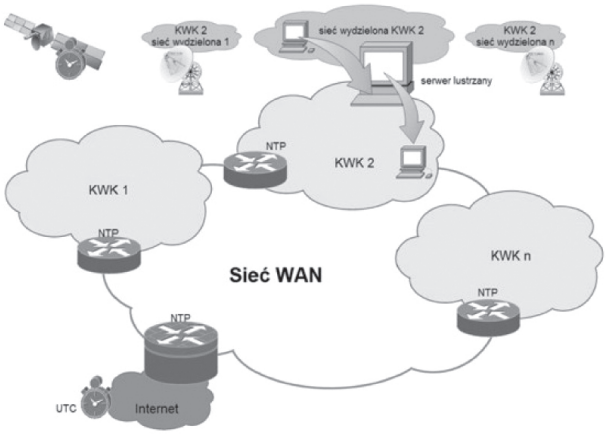
Rys. 1. Idea serwera lustrzanego [4]

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 zsynchronizowany 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.

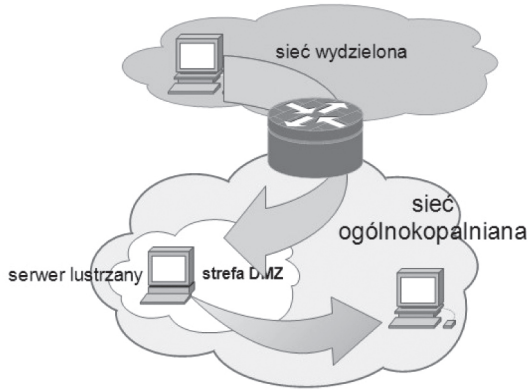
Patrząc z tej perspektywy na przepisy § 750 RME, wymagania co do stosowanego w tych systemach oprogramowania dotyczą konieczności utworzenia indywidualnych kont dla użytkowników i hierarchizacji uprawnień do systemu oraz rejestracji udanych i nieudanych prób logowań. W dużej części wymagania dotyczące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



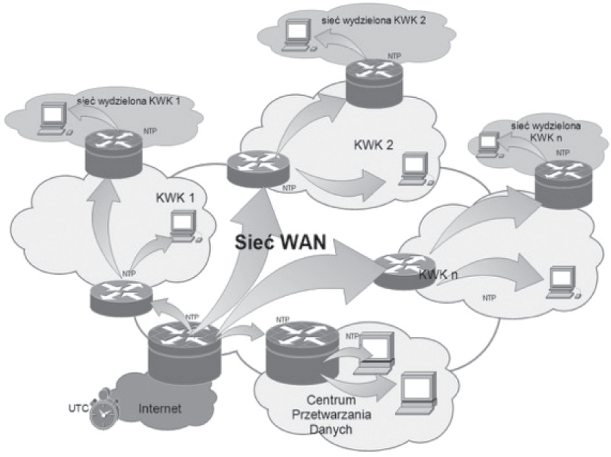
Rys. 3. Lokalizacja serwerów lustrzanych w strefie DMZ [4]

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.

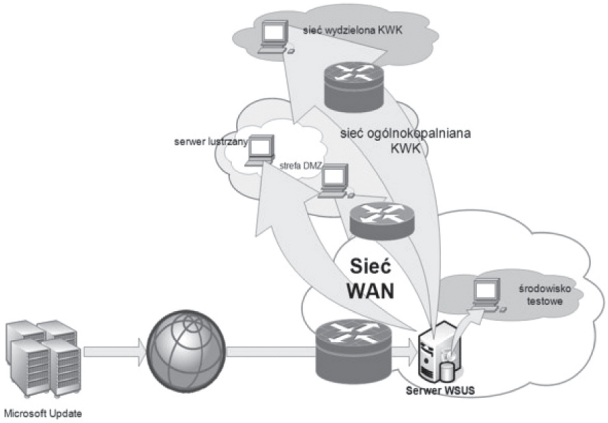
3.1.3. Zabezpieczenie przed złośliwym oprogramowaniem

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 Il: 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