Diagnostyka i utrzymanie systemów sterowania ruchem kolejowym na odległość - bezpieczny zdalny dostęp do systemów kluczowych

Remote maintenance and diagnostics of railway control systems- secure remote access to essential systems

Radosław Zawierucha

Mgr
Członek Zarządu ds. Rozwoju Infrastruktury IT i Bezpieczeństwa, PKP Informatyka Sp. z o.o.

radoz72@gmail.com

Grzegorz Kuta

Biuro Bezpieczeństwa Informacji i Spraw Obronnych,

PKP Polskie Linie Kolejowe S.A.

Streszczenie: W artykule przedstawiono opis prac nad projektem p*roof of concept* rozwiązania diagnostyki i utrzymania systemów sterowania ruchem kolejowym na odległość, przeprowadzonym przez PKP Polskie Linie Kolejowe S.A. oraz PKP Informatyka Sp. z o.o. wraz z firmą ALSTOM Polska S.A. Artykuł opisuje otoczenie prawne i wynikające z niego zapotrzebowanie na utworzenie podobnego projektu, proces określania wymagań dla docelowego rozwiązania na podstawie norm, standardów i zaleceń branżowych, oraz jego efekty, w formie opisu funkcjonalności i podstawowej architektury logicznej rozwiązania. W drodze *proof of concept* stwierdzono, że proponowane rozwiązanie realizuje określone wymagania funkcjonalne.

Słowa kluczowe: *Cyberbezpieczeństwo; Sterowanie Ruchem Kolejowym; Zdalny Dostęp; Cyberbezpieczeństwo OT*

Abstract: The article presents a description of the work on the proof of concept for the remote diagnostics and maintenance of railway traffic control systems solution, carried out by PKP Polskie Linie Kolejowe S.A., PKP Informatyka Sp. z o.o. and ALSTOM Polska S.A. The article describes the legal environment and the resulting needs for the creation of a similar project, the process of determining the requirements for the target solution and the underlying norms, industry standards and best practices, and a description of the functionality and basic logical architecture of the solution. Proof of concept has confirmed that the proposed solution meets the specified functional requirements.

Keywords: *Cybersecurity; Railway Signaling; Remote Access; OT Cybersecurity*

Otoczenie prawne dla prac nad diagnostyką nad bezpiecznym zdalnym dostępem do systemów kluczowych

W 2023 roku w Unii Europejskiej przyjęta została Dyrektywa Parlamentu Europejskiego i Rady 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (tzw. Dyrektywa NIS2) [1]. Dyrektywa NIS2 (ang. *Network and Information Systems Directive*) stanowi nowelizację obowiązującego od 2016 roku prawa europejskiego dotyczącego obszaru cyberbezpieczeństwa, które do polskiego systemu prawnego zaimplementowano przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.) [2]. Załączniki I Dyrektywy NIS2 podobnie jak obecnie obowiązujący załącznik do ustawy o krajowym systemie cyberbezpieczeństwa wskazuje sektory i podsektory kluczowe oraz rodzaje podmiotów objęte tymi regulacjami. Jeśli chodzi o transport kolejowy to Dyrektywa NIS2 pozycjonuje go jako podsektor kluczowy sektora transportu wymieniając w zakresie podmiotowym zarządców infrastruktury zgodnie z definicją zawartą w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE oraz przedsiębiorstwa kolejowe zgodnie z definicją zawartą w art. 3 pkt 1 dyrektywy 2012/34/UE [3], w tym operatorów infrastruktury kolejowej zdefiniowanej w art. 3 pkt 12 tej samej dyrektywy. W myśl Dyrektywy NIS2 „zarządca infrastruktury" to każdy podmiot lub przedsiębiorstwo, które jest odpowiedzialne w szczególności za założenie infrastruktury kolejowej, zarządzanie nią i jej utrzymanie, w tym za prowadzenie ruchu pociągów, urządzenia bezpiecznej kontroli jazdy i urządzenia sterowania ruchem kolejowym, a funkcje zarządcy infrastruktury na sieci lub części sieci mogą być przydzielane różnym podmiotom lub przedsiębiorstwom. Z kolei „przedsiębiorstwo kolejowe" w rozumieniu Dyrektywy NIS2 to każde

przedsiębiorstwo publiczne lub prywatne, posiadające licencję zgodnie z dyrektywą w sprawie utworzenia jednolitego europejskiego obszaru kolejowego, którego działalność podstawowa polega na świadczeniu usług w transporcie towarowym lub pasażerskim koleją, z zastrzeżeniem, że przedsiębiorstwo to zapewnia pojazdy trakcyjne, czyli obejmuje także przedsiębiorstwa, które tylko dostarczają pojazdy trakcyjne. „Operator obiektu infrastruktury usługowej" oznacza natomiast każdy podmiot publiczny lub prywatny odpowiedzialny za zarządzanie co najmniej jednym obiektem infrastruktury usługowej lub świadczący przedsiębiorstwom kolejowym jedną lub więcej usług (np. terminale towarowe, punkty zaplecza technicznego czy dostawę prądu trakcyjnego). W obecnie obowiązującym stanie prawnym, czyli bazując na przepisach aktualnie obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu go za operatora usługi kluczowej.

Dla sektora transportu i podsektora transportu kolejowego jest nim minister właściwy do spraw transportu. Stąd w obecnym stanie prawnym, aby zarządca infrastruktury kolejowej, przedsiębiorstwo kolejowe czy operator kolejowej infrastruktury usługowej zobowiązany był stosować przepisy ustawy o krajowym systemie cyberbezpieczeństwa musi otrzymać od organu właściwego do spraw cyberbezpieczeństwa decyzję administracyjną uznającą go za operatora usługi kluczowej. Dopiero na tej podstawie dana Spółka kolejowa w terminach wskazanych w ustawie (art. 16) wdrożyć musi obowiązki i wymagania z niej wynikające określone w art. 8 oraz art. 15. W decyzji administracyjnej wskazane są również wprost systemy informacyjne, które wspierają usługę kluczową. Zgodnie z Dyrektywą NIS2 znacznemu rozszerzeniu ulega katalog sektorów objętych działaniem tego przepisu. Mimo, że taki podział nie przesądza jeszcze o uznaniu danego podmiotu za kluczowy, odnosząc się do podsektora kolejowego zakres podmiotowy polskich Spółek kolejowych odjęty tą regulacją ulegnie znacznemu rozszerzeniu w stosunku do dziś obowiązujących przepisów. Obecnie, na bazie posiadanych informacji, pod przepisy ustawy o krajowym systemie cyberbezpieczeństwa w podsektorze kolejowym podlegają tylko cztery spółki kolejowe mające status operatora usługi kluczowej, świadczące usługi wskazane w rozporządzeniu Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych [4]. Ten akt prawny wskazuje, że w podsektorze transportu kolejowego podmiotem świadczącym usługi kluczowe jest zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym [5] z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, infrastruktury prywatnej oraz infrastruktury kolei wąskotorowej, a usługą kluczową jest „Konstrukcja rozkładu jazdy pociągów". Ponadto podmiotem świadczącym usługi kluczowe jest przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym. W przypadku przewoźników kolejowych usługą kluczową jest odpowiednio „transport kolejowy pasażerski" oraz „transport kolejowy towarów". W przypadku Dyrektywy NIS2 dla podsektora transportu kolejowego za podmioty kluczowe lub podmioty ważne uznane zostaną zarządcy infrastruktury, przedsiębiorstwa kolejowe oraz operatorzy infrastruktury kolejowej przekraczające pułapy określone dla średnich przedsiębiorstw (zatrudniające co najmniej 50 osób oraz których obroty roczne lub roczna suma bilansowa wynoszą od 10 mln euro do 50 mln euro). Za podmiot kluczowy lub ważny w podsektorze transportu kolejowego uznane mogą zostać również spółki kolejowe wskazane jako podmioty krytyczne na podstawie dyrektywy o odporności podmiotów krytycznych [6] (tzw. Dyrektywy CER), podmioty które państwo członkowie Unii Europejskiej wskazało przed wejściem w życie NIS2 jako operatorów usług kluczowych czy pomioty z sektorów wymienionych w załączniku I i II Dyrektywy NIS2, które nie kwalifikują się jako pomioty kluczowe (staną się one podmiotami ważnymi na gruncie Dyrektywy NIS2). W tym miejscu, odnosząc się do powyższego, należy również zwrócić uwagę na zapisy rozporządzenia Komisji Europejskiej 2023/2450 z dnia 25 lipca 2023 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 [7] (Dyrektywę CER o odporności podmiotów krytycznych) przez ustanowienie wykazu usług kluczowych. Dokument ten ustanawia niewyczerpujący wykaz usług kluczowych, w rozumieniu definicji zawartej w art. 2 pkt 5 Dyrektywy CER, świadczonych w poszczególnych sektorach i podsektorach.

Dla podsektora transportu kolejowego jako usługi kluczowe w/w rozporządzenie wskazuje:

- usługi w zakresie transportu kolejowego (pasażerskiego i towarowego) (przedsiębiorstwa kolejowe);
- eksploatację i utrzymanie infrastruktury kolejowej, w tym stacji pasażerskich, terminali to-

warowych, stacji rozrządowych i centrów sterowania ruchem, i zarządzanie nimi (zarządcy infrastruktury);
- eksploatację i utrzymanie obiektów kolejowej infrastruktury usługowej i zarządzanie nimi (operatorzy obiektów infrastruktury usługowej);
- eksploatację i utrzymanie instalacji i systemów związanych z zarządzaniem i sterowaniem ruchem kolejowym oraz telekomunikacją, które są wykorzystywane do sterowania ruchem, oraz zarządzanie tymi systemami i instalacjami (zarządcy infrastruktury).

Zapotrzebowanie dla prac nad diagnostyką nad bezpiecznym zdalnym dostępem do systemów kluczowych

Przygotowując się do wdrożenia zapisów Dyrektywy NIS2 oraz Dyrektywy CER, mając na względzie potrzebę zapewnienie odporności przed zagrożeniami nie tylko systemów informacyjnych (systemów IT), ale również technologii operacyjnych (systemów OT) do których zaliczyć należy urządzenia sterowania ruchem kolejowym, PKP Polskie Linie Kolejowe S.A. oraz PKP Informatyka Sp. z o.o. wraz z firmą ALSTOM Polska S.A. wykonały tzw. „proof of concept" w zakresie zdalnego dostępu i monitorowania komputerowych systemów sterowania ruchem kolejowym w PKP Polskie Linie Kolejowe S.A. w oparciu o infrastrukturę SIEM (Security Information and Event Management) oraz SOC (Security Operations Center). Utworzenie projektu motywowane było m.in. rosnącym zainteresowaniem podmiotów odpowiedzialnych za cyberbezpieczeństwo, w tym CSIRT-ów poziomu krajowego wskazanych w przepisach ustawy o krajowym systemie cyberbezpieczeństwa, kwestią zapewnienia bezpieczeństwa serwisu utrzymania i diagnostyki w systemach sterowania ruchem kolejowym oraz, jak wskazano powyżej, realizacji wymagań prawnych (Dyrektywy NIS2 oraz ustawy o krajowym systemie cyberbezpieczeństwa). Projekt został zrealizowany oraz nadal jest kontynuowany w ramach prac badawczo - rozwojowych zespołu CERT PKP Informatyka Sp. z o.o., we współpracy z dostawcami komputerowych systemów sterowania ruchem kolejowym, producentami rozwiązań z domeny cyberbezpieczeństwa oraz z PKP Polskie Linie Kolejowe S.A. Celem projektu jest wykazanie możliwości i słuszności zastosowania wybranych rozwiązań i technologii bezpieczeństwa w celu zwiększenia odporności cybernetycznej w komputerowych systemach sterowania ruchem kolejowym. Po raz pierwszy wyniki projektu zaprezentowano podczas VI Konferencji naukowo – technicznej „IT&OT w transporcie szynowym" zorganizowanej przez Stowarzyszenie Inżynierów i Techników Komunikacji RP.

Wymagania dla rozwiązania bezpiecznego zdalnego dostępu do systemów kluczowych

Kluczowym elementem związanym z diagnostyką i utrzymaniem systemów sterowania ruchem kolejowym z wykorzystaniem zdalnego dostępu było w pierwszej kolejności określenie zarówno środków proceduralnych jak i technicznych związanych projektowanym rozwiązaniem. W tym celu w pierwszej kolejności określono standardy obowiązujące zarówno w obszarze IT jak i OT biorąc pod uwagę zarówno elementy związane z bezpieczeństwem funkcjonalnym systemów sterowania ruchem kolejowym (m.in. normy RAMS serii EN 50120 [8]) jak również standardy związane z bezpieczeństwem systemów informacyjnych (normy serii ISO/IEC 27000 [9]), dotyczące zarządzania usługami (norma ISO 20000 [10]), związane z bezpieczeństwem systemów sterowania i automatyki przemysłowej (normy serii IEC 62443 [11]), powiązane z cyberbezpieczeństwem aplikacji kolejowych (norma CLC/TS 50701 [12]) oraz dotyczące zapewnienia ciągłości działania organizacji (norma ISO 22301 [13]). Zaznaczyć należy, że przesłanki związane z wdrożeniem określonych elementów systemu zarządzania cyberbezpieczeństwem dla komputerowych systemów sterowania ruchem kolejowym powinny wynikać z procesu zarządzania ryzykiem oraz uwzględniać obowiązujące u zarządcy infrastruktury kolejowej elementy zarządzania ruchem kolejowym, uwzględniać istniejącej polityki bezpieczeństwa w obszarze bezpieczeństwa ruchu kolejowego (SMS) [14], obszar bezpieczeństwa informacji (SZBI) a także być zgodne z wymaganiami prawnymi (np. ustawą o transporcie kolejowym, dyrektywami kolejowymi, Dyrektywą NIS2, ustawą o krajowym systemie cyberbezpieczeństwa). Wymagania dotyczące zapewnienia kontroli dostępu zarówno do systemów informacyjnych (IT) jak i operacyjnych (OT) określa odpowiednio standard ISO/IEC 27001:2022 (obszar IT) jak również standard IEC 62443 (obszar OT). W tym miejscu zwrócić uwagę należy na fakt, że kojarzony dotychczas tylko i wyłącznie z obszarem bezpieczeństwa informacji standard ISO/IEC 27001 został całkowicie zmieniony i w wersji normy z 2022 roku oprócz bezpieczeństwa informacji obejmuje on elementy związane z cyberbezpieczeństwem oraz ochroną prywatności. Koncepcje cyberbezpieczeństwa wskazane w normie ISO/IEC 27001:2022 umożliwiają postrzeganie zabezpieczeń w odniesieniu do tych określonych chociażby w standardzie ISO/IEC TS 27110 (informatyka, cyberbezpieczeństwo i ochrona prywatności – wytyczne dotyczące rozwoju ram cyberbezpieczeństwa), czyli m.in. odnosić się do celów biznesowych

***1**. Funkcjonalności rozwiązania*

organizacji, aktywów, procesów biznesowych oraz praw i regulacji, którym dany podmiot podlega. Mając na względzie powyższe w realizowanym projekcie uwzględniono wymagania normy ISO/IEC 27001:2022 w następującym zakresie:

- kontrola dostępu (pkt 5.15 normy),
- zarządzanie tożsamością (pkt 5.16 normy),
- informacje uwierzytelniające (pkt 5.17 normy),
- prawa dostępu (pkt 5.18 normy),
- monitorowanie, przegląd i zarządzanie zmianą usług dostawców (pkt 5.22 normy),
- praca zdalna (pkt 6.7 normy),
- uprzywilejowane prawa dostępu (pkt 8.2 normy),
- bezpieczne uwierzytelnianie (pkt 8.5 normy),

Natomiast stosując zapisy standardu IEC 62443 uwzględniono takie wymagania jak:

- uwierzytelnianie wszystkich zdalnych użytkowników na odpowiednim poziomie (pkt 4.3.3.6.5 normy),
- kontrola dostępu: administracja kontami (pkt 4.3.3.5 normy),
- kontrola dostępu: uwierzytelnienie (pkt 4.3.3.6 normy),
- kontrola dostępu: autoryzacja (pkt 4.3.3.7 normy),

Wymagania kontroli dostępu jakie uwzględniono w realizowanym projekcie zdalnego dostępu i monitorowania komputerowych systemów sterowania ruchem kolejowym to:

- zapewnienie gwarancji, że cecha tożsamości użytkownika logującego się do systemów sterowania ruchem kolejowym czy to lokalnie np. w Lokalnym Centrum Sterowania, czy w sposób zdalny (np. z siedziby usługodawcy) jest prawidłowa, gdyż uwierzytelnianie użytkownika jest warunkiem niezbędnym do przyznania dostępu do wszystkich zasobów w systemie sterowania ruchem kolejowym,
- zapewnienie, że środki użyte do potwierdzenia tożsamości użytkownika (np. hasło) są bezpieczne oraz umożliwiają zapewnienie autentyczności, czyli atrybutu bezpieczeństwa polegającego na tym, że użytkownik jest tym, za kogo się podaje,
- umożliwienie szybkiego i niezawodnego dostępu do korzystania z informacji oraz z funkcjonalności systemu sterowania ruchem kolejowym,
- wdrożenie zasady najmniejszego uprzywilejowania, czyli mechanizmów które zapewnią, że użytkownicy będą posiadali jak najmniejsze przywileje w systemie zgodne z przydzielonymi obowiązkami, funkcjami i rolami.

Dodatkowo w realizowanym projekcie dokonano analizy możliwości wdrożenia w komputerowych systemach sterowania poszczególnych elementów kontroli bezpieczeństwa CIS (Critical Security Controls) wydanych przez instytut SANS [15]. Standard CIS Controls w wersji 8 zawiera konkretne rekomendacje podzielone na 18 grup środków bezpieczeństwa (rozwiniętych na 153 szczegółowe wymagania) dotyczące działań oraz najlepszych praktyk poprawiających cyberbezpieczeństwo. Dla realizowanego projektu ze standardu CIS Controls v8 wybrano następujące środki kontroli bezpieczeństwa:

- kontrola 04: bezpieczna konfiguracja zasobów i oprogramowania, kontrola 12: zarządzanie infrastrukturą sieciową oraz kontrola 13: monitorowanie i ochrona sieci – system sterowania ruchem kolejowym, oprócz segmentacji i separacji sieci będzie chroniony systemem klasy firewall w sposób zapewniający ochronę przed niepożądanymi połączeniami do Lokalnego Centrum Sterowania, a bezpośrednia komunikacja możliwa będzie poprzez tunele VPN (ang. Virtual Private Network),
- kontrola 05: zarządzanie kontami oraz kontrola 06: zarządzanie kontrolą dostępu – dostęp administratorów i serwisantów zewnętrznych do systemu sterowania ruchem kolejowym zapewniony będzie za pomocą narzędzia klasy PAM (Privileged Access Management), czyli rozwiązania dotyczącego zarządzana dostępem uprzywilejowanym, który zapewni bezpieczeństwo w zakresie tożsamości użytkowników oraz ochronę przed cyberzagrożeniami poprzez monitorowanie, wykrywanie i zapobieganie nieautoryzowanemu, uprzywilejowanemu dostępowi do zasobów systemu sterowania ruchem kolejowym.

W ramach zarządzania kontami zakładane jest wdrożenie serwera dostępowego i przesiadkowego, dwuskładniowe uwierzytelnianie użytkownika, rejestracja i audyt sesji zdalnych zarówno aktualnych jak i archiwalnych, nagrywanie wszystkich trwających sesji oraz możliwość ich odtworzenia, śledzenie aktywności użytkowników, budowanie indywidualnych profili behawioralnych użytkowników co pozwoli wykryć anomalie w sesji użytkownika i na ich podstawie raportować do SOC sesję jako podejrzaną oraz automatycznie wstrzymać lub zablokować podejrzaną sesję oraz użytkownika,

- kontrola 08: zarządzanie dziennikiem audytu – dostęp do dzienników systemowych zapewni kontrolę aktywności użytkowników i serwisantów w systemach srk poprzez dostęp i zarządzanie logami systemowymi, co w przypadku incydentu cyberbezpieczeństwa zapewni wiedzę na temat danego zdarzenia. Kontrola ta zapewniona zostanie poprzez system klasy SIEM służący do zbierania i przetwarzania logów oraz agregowania i korelowania zdarzeń dla zespołu SOC (Security Operations Center). W ten sposób będzie można monitorować i wykrywać naruszenia bezpieczeństwa np. nieautoryzowane próby połączeń do systemów,
- kontrola 15: zarządzanie dostawcami usług – dostęp serwisantów zewnętrznych będących dostawcami usług w systemie sterowania ruchem kolejowym zapewniony będzie za pomocą narzędzia klasy PAM oraz monitorowany za pomocą systemu klasy SIEM,
- kontrola 17: zarządzanie i reagowanie na incydenty – kontrola zapewniona zostanie przez zespół SOC i wdrożone narzędzia klasy PAM oraz SIEM, a także opracowane w tym celu procedury reagowania, co umożliwi m.in. wyznaczenie osób po stronie SOC, zarządcy infrastruktury kolejowej jak i dostawcy systemów sterowania ruchem kolejowy do procesu zarządzania obsługą wykrytych incydentów oraz ustanowienie procesu reagowania na nie.

Na podstawie powyższych kontroli i otoczenia prawnego określono wymagania funkcjonalne dla projektowanego i opisywanego rozwiązania. Rozwiązanie bezpiecznego zdalnego dostępu do systemów kluczowych ma zapewnić:

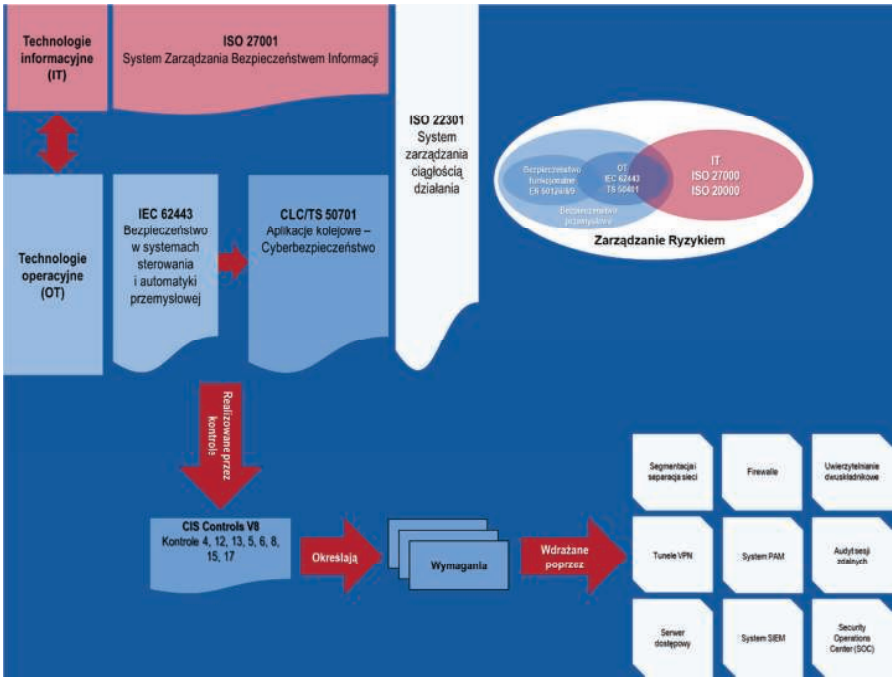
- szybki zdalny dostęp do logów oraz narzędzi diagnostycznych w systemach sterowania ruchem kolejowym w celu identyfikacji przyczyny zaistniałego problemu lub awarii,
- zdalne zarządzania sesjami serwisantów zewnętrznych oraz użytkowników z poziomu zarządcy infrastruktury (gestora systemu) oraz zespołu SOC,
- rozliczalność serwisantów zewnętrznych systemów sterowania ruchem kolejowym przez zarządcę infrastruktury kolejowej,
- integrację z systemem klasy SIEM, a przez to umożliwienie zarządzania i reagowania na incydenty cybernetyczne.

Proces określania komponentów rozwiązania bezpiecznego zdalnego dostępu do systemów przedstawiony został na ilustracji **2**.

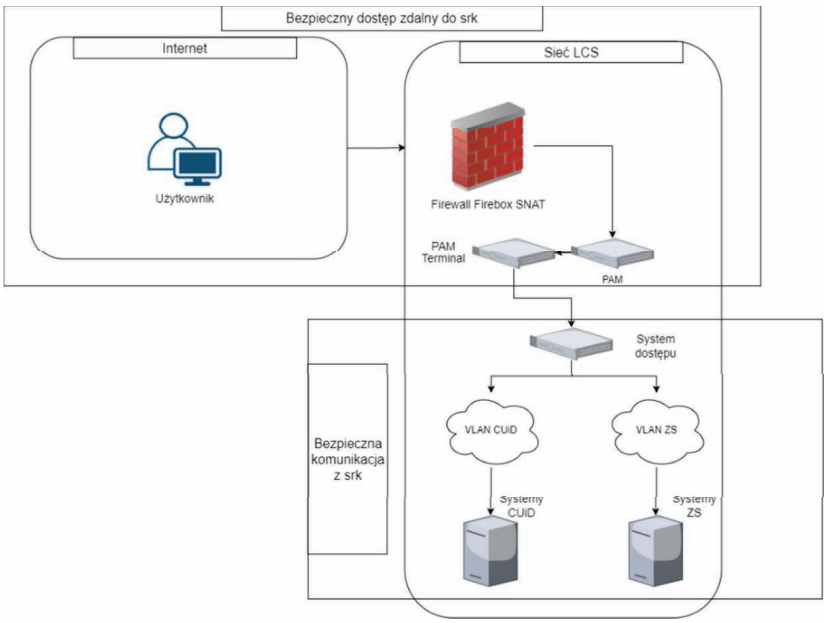
Rozwiązanie bezpiecznego zdalnego dostępu do systemów kluczowych i etapy przedsięwzięcia

Realizacja przedsięwzięcia podzielona została na następujące fazy:

1. opracowanie architektury rozwiązania (koncepcje, studium wykonalności),
2. wdrożenie laboratoryjne rozwiązania u dostawcy systemu,
3. testy opracowanego rozwiązania (raport techniczny z przeprowadzonych testów wraz z wnioskami, przeprowadzenie oceny znaczenia zmiany zgodnie z procedurami SMS),
4. akceptacja interesariuszy (zarządca infrastruktury, dostawca systemu sterowania ruchem kolejowym, SOC),
5. wdrożenie rozwiązania w środo-



***2**. Wpływ otoczenia prawnego i wymagań technicznych na komponenty rozwiązania. Opracowanie własne*



***3**. Architektura logiczna systemu. Opracowanie własne*

wisku produkcyjnym, w Lokalnym Centrum Sterowania.

Wymagania dla rozwiązania bezpiecznego zdalnego dostępu do systemów kluczowych stanowiły podstawę do opracowania podstawowej architektury logicznej rozwiązania, przedstawionej na ilustracji **3**.

Podsumowanie i wnioski

Aktualnie realizowany projekt zakończony został w fazie 2 (wdrożenia laboratoryjnego), a wdrożenie potwierdziło poprawność wszystkich założonych funkcji projektowanego rozwiązania oraz prawidłowe działanie systemu klasy PAM w zakresie zarządzania uprawnieniami oraz kontroli i rejestracji zdalnych sesji oraz zarządzania dziennikami zdarzeń w systemie klasy SIEM. Z tego punktu widzenia nie ma przeszkód technicznych do realizacji zdalnego dostępu zarówno do systemów diagnostycznych jak i systemów sterowania ruchem kolejowym. ◄

Materiały źródłowe

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

[3] Dyrektywa Parlamentu Europejskiego i Rady 2012/34/UE z dnia 21 listopada 2012 r. w sprawie utworzenia jednolitego europejskiego obszaru kolejowego (przekształcenie). https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32012L0034

[4] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001806

[5] Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20030860789

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32022L2557

[7] Rozporządzenie delegowane Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R2450

[8] EN 50126 (IEC 62278) – Reliability, Availability, Maintainability, and Safety (RAMS)

[9] ISO/IEC 27000:2018

[10] ISO/IEC 20000-1:2018 Service Management System (SMS) Standard

[11] IEC 62443-1-1, Industrial communication networks – Network and system security

[12] CLC/TS 50701:2023 Railway applications – Cybersecurity

[13] ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements

[14] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/798 z dnia 11 maja 2016 r. w sprawie bezpieczeństwa kolei. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:02016L0798-20200528

[15] Center for Internet Security CIS, Critical Security Controls Version 8, 2021. https://www.cisecurity.org/controls/v8