Założenia budowy centrum badań i rozwoju obszaru monitoringu automatyki kolejowej

Building assumptions of a research and development center for the monitoring of railway automation

Radosław Zawierucha

Mgr

PKP Informatyka Sp. z o.o.

radoz72@gmail.com

Streszczenie: Artykuł zawiera wstępną analizę budowy Zespołu Badawczo-Rozwojowego (ZBR) w obszarze cyberbezpieczeństwa ze szczególnym uwzględnieniem analityki danych z systemów automatyki kolejowej. Opracowanie porusza zagadnienia organizacyjne, techniczne oraz biznesowe. Z racji doświadczenia własnego ostatnich lat pracy referat ten skonstruowany jest niejako z perspektywy operacyjnej i organizacyjnej spółki PKP Informatyka. Stąd wynika zakładany merytoryczny kontekst, otoczenie formalne, organizacyjne i legislacyjne przewidywanej domeny działania opracowywanego zespołu badawczo-rozwojowego. Praca opisuje zadania, metody badawcze, kompetencje i produkty zespołu badawczego. Samo przedsięwzięcie ma charakter projektowy – przewiduje więc pewne założenia, przyjmuje wybrane metodyki działania i zakłada osiągnięcie określonych wyników.

Słowa kluczowe: *Zespół Badawczy-Rozwojowy; Cyberbezpieczeństwo; Automatyka Kolejowa*

Abstract: The paper describes the initial analysis of the construction of the Research and Development Team (R&D) in the area of cyber security with particular emphasis on data analytics from railway automation systems. The study addresses organizational, technical and business issues. Due to the own experience of the last years of work, this paper is constructed from the operational and organizational perspective of PKP Informatyka. Hence the assumed substantive context, formal, organizational and legislative environment of the expected domain of operation of the research and development team under development. The work describes the tasks, research methods, competences and products of the research team. The project itself is of a project nature - it provides for certain assumptions, adopts selected methodologies and assumes the achievement of specific results.

Keywords: *Research and Development Team; Cybersecurity; Railway Automation Systems*

Definicje

Zespół Badawczo-Rozwojowy (ZBR): Zespół badawczo-rozwojowy w obszarze cyberbezpieczeństwa.

Badania podstawowe: Oryginalne prace badawcze eksperymentalne lub teoretyczne podejmowane przede wszystkim w celu zdobywania nowej wiedzy o podstawach zjawisk i obserwowalnych faktów bez nastawienia na bezpośrednie zastosowanie komercyjne.

Badania stosowane/przemysłowe: Badania mające na celu zdobycie nowej wiedzy oraz umiejętności w celu opracowywania nowych produktów, procesów i usług lub wprowadzania znaczących ulepszeń do istniejących produktów, procesów i usług; badania te uwzględniają tworzenie elementów składowych systemów złożonych, budowę prototypów w środowisku laboratoryjnym lub w środowisku symulującym istniejące systemy, szczególnie do oceny przydatności danych rodzajów technologii, a także budowę niezbędnych w tych badaniach linii pilotażowych, w tym do uzyskania dowodu w przypadku technologii generycznych.

CSIRT GOV: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego

CSIRT MON: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej, funkcjonujący w ramach Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni.

CSIRT NASK: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z

siedzibą w Warszawie.

Działalność badawczo-rozwojowa, B+R: Działalność badawcza i rozwojowa obejmuje pracę twórczą podejmowaną w sposób metodyczny w celu zwiększenia zasobów wiedzy. Termin obejmuje trzy rodzaje działalności: badania podstawowe, badania stosowane/przemysłowe i prace rozwojowe. Aby projekt dotyczący tworzenia oprogramowania został zaklasyfikowany jako B+R, warunkiem jego zakończenia musi być dokonanie postępu naukowego lub technicznego, a celem projektu musi być wyeliminowanie elementu naukowej lub technicznej niepewności w sposób metodyczny.

Innowacja: Wdrożenie nowego lub istotnie ulepszonego produktu (wyrobu lub usługi) lub procesu lub też nowej metody organizacyjnej, przy czym nowe procesy lub metody organizacyjne zostają wdrożone, kiedy rozpoczyna się ich faktyczne wykorzystywanie w działalności przedsiębiorstwa.

ISAC-Kolej: Centrum Wymiany i Analizy Informacji.

Laboratorium: Infrastruktura umożliwiająca uruchomienie środowiska testowego, dostosowanego do przeprowadzania najbardziej wymagających testów, badań i prac rozwojowych w dziedzinie bezpieczeństwa IT/OT.

PoC: Proof of Concept, prototypowa wersja docelowego rozwiązania, prezentująca jego możliwość zastosowania w organicznym zakresie lub z zawężonymi funkcjonalnościami.

Poziom gotowości technologicznej TRL: Metoda oceny zaawansowania projektów badawczo-rozwojowych. Wydziela ona dziewięć poziomów zaawansowania, przyporządkowanych odpowiednio do badań podstawowych (poziom I), badań przemysłowych (poziomy II-VI) i prac rozwojowych (poziomy VII-IX). Poziom IX projektu badawczo-rozwojowego oznacza wytworzenie gotowego, produkcyjnego rozwiązania innowacyjnego.

Prace rozwojowe: Nabywanie, łączenie, kształtowanie i wykorzystywanie dostępnej aktualnie wiedzy i umiejętności z dziedziny nauki, technologii i działalności gospodarczej oraz innej wiedzy i umiejętności do planowania produkcji oraz tworzenia i projektowania nowych, zmienionych lub ulepszonych produktów, procesów i usług, z wyłączeniem prac obejmujących rutynowe i okresowe zmiany wprowadzane do produktów, linii produkcyjnych, procesów wytwórczych, istniejących usług oraz innych operacji w toku, nawet, jeżeli takie zmiany mają charakter ulepszeń. Prace rozwojowe nie obejmują rutynowych i okresowych zmian wprowadzanych do produktów, linii produkcyjnych, procesów wytwórczych, istniejących usług oraz innych operacji w toku, nawet, jeżeli takie zmiany mają charakter ulepszeń.

Stan techniki: Najwyższy powszechnie i publicznie znany poziom zaawansowania prac techniki, typu urządzenia czy dziedziny.

Zespoły kompetencyjne: Zespoły doświadczonych pracowników o odpowiednich kompetencjach i kwalifikacjach wyspecjalizowany w określonej dziedzinie.

Charakterystyka odbiorców i interesariuszy

- Interesariusze projektu

o Podmioty działające na rynku kolejowym w Polsce – przewoźnicy, operatorzy infrastruktury, producenci.
o Właściciele biznesowi;
o Opiekunowie systemów;
o Klienci końcowi świadczonych usług – podmioty gospodarcze.

- Odbiorcy/użytkownicy projektu

o Sieci i instytuty naukowe;
o Zespoły badawczo-rozwojowe;
o Zespoły CSIRT;
o CERT PKP Informatyka;
o SOC PKP Informatyka;
o Zespoły bezpieczeństwa Grupy PKP;
o Zespoły kompetencyjne;
o Spółki grup PKP i PKP PLK;
o Administratorzy i użytkownicy systemów;
o Zespoły CERT i SOC innych podmiotów.

Cel utworzenia Zespołu Badawczo-Rozwojowego (ZBR)

Celem budowy Zespołu Badawczo-Rozwojowego jest wytworzenie potencjału badawczego do opracowywania i wdrażania innowacyjnych rozwiązań w obszarze cyberbezpieczeństwa. W pierwszej kolejności, zadaniem ZBR będzie gromadzenie wiedzy o najnowszych trendach i stanie nauki oraz reagowanie na pojawiające się nowe wyzwania i potrzeby klientów. Na ich podstawie, ZBR będzie dokonywać rozpoznania i proponować zastosowania innowacyjnych rozwiązań zabezpieczeń cyberprzestrzeni w infrastrukturze macierzystej organizacji oraz w infrastrukturze odbiorców usług.

W celu zwiększania zasobów wiedzy oraz jego wykorzystania do tworzenia nowych innowacyjnych zastosowań, do zadań ZBR należeć będzie między innymi:

- Przegląd i analiza dotychczas stosowanych rozwiązań;
- Testowanie i badanie innowacyjnych rozwiązań;
- Utworzenie laboratoriów cyberbezpieczeństwa;
- Opiniowanie rozwiązań innowacyjnych.

Jedną ze zidentyfikowanych inicjatyw dla ZBR jest utworzenie laboratoriów cyberbezpieczeństwa. Wykorzystywane one będą w celach badawczych, treningowych oraz jako narzędzie promocji badań i rozwoju

w dziedzinie bezpieczeństwa cybernetycznego.

Na podstawie prac badawczych Zespołu Badawczo-Rozwojowego, przeprowadzane będą:

- Planowania wdrożeń nowych rozwiązań;
- Implementacja nowych rozwiązań.

Zespół Badawczo-Rozwojowy prowadzić będzie również prace spełniającą formalne wymogi działalności B+R, docelowo dążące do budowy rozwiązań o poziomie gotowości technologicznej IX. Do działań o tym charakterze zaliczyć można:

- Badania innowacyjne;
- Budowa innowacyjnych narzędzi i rozwiązań;
- Opracowywanie innowacyjnych frameworków i metodyk badań.

Dodatkowo, Zespół Badawczo-Rozwojowy będzie zaangażowany w działania popularyzatorskie, proces budowania kompetencji, czy budowania sieci współpracy z instytucjami czy ośrodkami badawczymi.

Korzyści i ryzyka wynikające z powołania zespołu B + R

Zidentyfikowano następujące korzyści wynikające z budowy Zespołu Badawczo-Rozwojowego:

- Centralizacja wiedzy na temat rozwiązań cyberbezpieczeństwa;
- Poprawa jakości świadczonych usług w zakresie cyberbezpieczeństwa;
- Podniesienie poziomu cyberbezpieczeństwa;
- Ocena skuteczności dotychczasowych rozwiązań;
- Budowa zwinnego systemu reakcji na potrzeby klienckie;
- Opracowanie innowacyjnych rozwiązań;
- Wprowadzanie nowych produktów cyberbezpieczeństwa;
- Nawiązanie współpracy z jednostkami badawczo-rozwojowymi, naukowymi, uczelniami oraz zespołami badawczo–rozwojowymi podmiotów podsektora kolejowego oraz obszaru bezpieczeństwa IT;
- Możliwość świadczenia usług badawczych i analitycznych w zakresie cyberbezpieczeństwa w podsektorze kolejowym;
- Współfinansowanie prac zespołu ZBR na zasadach grantowych poprzez przeprowadzenie formalnego procesu B+R.

Zidentyfikowano następujące zagrożenia wynikające z budowy Zespołu Badawczo-Rozwojowego:

- Brak możliwości zapewnienia i pozyskania odpowiednich kompetencji w zespole;
- Nieodpowiednie przydzielenie ról w zespole ZBR;
- Niewypracowanie rozwiązań innowacyjnych;
- Nieopracowanie raportowalnych i przejrzystych KPI;
- Nieoptymalnie zaprojektowana współpraca wewnętrzna oraz podmiotami w otoczeniu.
- Zbyt wysokie koszty utrzymania zespołu, nieskompensowane przychodami z działalności

Zadania, usługi i produkty wytwarzane przez ZBR

W ramach określonych celów utworzenia Zespołu Badawczo-Rozwojowego zidentyfikowano
4 podstawowe obszary zadań i usług i realizowanych przez ZBR.

- Działania analityczne
  - o Działania analityczne dotyczyć mogą analizy systemów oraz analizy podatności. Analiza podatności ma na celu wytworzenie wiedzy na temat podatności, idących za nią zagrożeń, oraz opracowanie środków zaradczych.
  - o Prowadzone będą również przeglądy i testy dotychczas stosowanych rozwiązań.
  - o ZBR będzie prowadzić również analizy nowych rozwiązań informatycznych z domeny cyberbezpieczeństwa w celu oceny ich jakości i zastosowalności w podsektorze kolejowym.
  - o Przykładowe produkty i działania:
  - Raporty z analiz incydentów;
  - Raporty z testów penetracyjnych;
  - Opinie i zalecenia o zastosowaniach nowych rozwiązań w Spółce.

- Działania prototypowe i wdrożeniowe
  - o Po pozytywnym zaopiniowaniu rozwiązań, ZBR będzie opracowywać plany wdrożeniowe oraz wytwarzać PoC.
  - o Zaaprobowane przez Klientów systemy bezpieczeństwa będą implementowane i parametryzowane.
  - o W ramach działań wdrożeniowych uwzględnione są również testy bezpieczeństwa i konsultacje.
  - o Przykładowe produkty i działania:
  - Plany wdrożeniowe;
  - Wdrożenia systemów cyberbezpieczeństwa;
  - Konsultacje klienckie;
  - Dokumentacje projektowe.

- Działania o charakterze B+R
  - o Budowa laboratorium cyberbezpieczeństwa.
  - o ZBR będzie wykorzystać wiedzę, dane oraz doświadczenie zebrane w ramach pozostałych działań w celu prowadzenia kompleksowych prac badawczo-rozwojowych.
  - o Prowadzone analizy będą stanowić podstawę do badań podstawowych, pozwalających zidentyfikować innowacyjne rozwiązania wykrytych problemów badawczych.
  - o W ramach badań technologicznych przeprowadzane będą prace badawcze mające na celu doprowadzanie rozwiązań do IV poziomu gotowości technologicznej, tj. gotowości do testów laboratoryjnych.
  - o Docelowo innowacyjne rozwiązania opracowywane przez ZBR będą rozwijane do poziomu produkcyjnego a następnie wdraża-

ne u Klientów.
o Przykładowe produkty i działania:
- Laboratorium cyberbezpieczeństwa;
- Innowacyjne frameworki zarządzania incydentami bezpieczeństwa;
- Innowacyjne narzędzia, np. automatyzujące badania czy analizatory logów;
- Innowacyjne aplikacje.

• Działania popularyzatorskie i edukacyjne
o Zespół Badawczo-Rozwojowy powinien wspierać zespoły CERT i w SOC w zadaniach powiązanych z popularyzacją wiedzy dotyczącej cyberbezpieczeństwa w podmiotach kolejowych.
o Na podstawie wytworzonej wiedzy prowadzone będą warsztaty i szkolenia.
o Dodatkowym produktem prac B+R będą artykuły, publikacje i biuletyny, promujące usługi Spółki i rozwijające stan wiedzy.
o ZBR będzie również odpowiedzialne za współpracę z instytucjami naukowymi, innymi organizacjami B+R i sieciami badawczymi.
o Przykładowe produkty i działania:
- Publikacje z prac badawczych;
- Biuletyny informacyjne;
- Warsztaty i szkolenia promujące bezpieczeństwo w Spółce;
- Szkolenia z wykorzystania pozytywnie zaopiniowanych technologii u Klientów.

Role i kompetencje Zespołu Badawczo-Rozwojowego

Zadania realizowane przez Zespół Badawczo-Rozwojowy wymagają budowy zespołu o interdyscyplinarnych kompetencjach. Ze względu na charakter pracy badawczo-rozwojowych, niezbędne jest połączenie wieloletniej praktyki zawodowej, wiedzy teoretycznej, jak również zdolności analitycznych i doświadczenia w zakresie projektów B+R.

W odniesieniu do powyższych wymagań, określono następujące stanowiska wchodzące w skład ZBR:
• Koordynator zespołu badawczo-rozwojowego;
• Analityk bezpieczeństwa;
• Architekt IT;
• Inżynier wdrożeniowy;
• Tester bezpieczeństwa;

Dla poszczególnych ról w Zespole Badawczo-Rozwojowym zidentyfikowano następujące kompetencje:
• Koordynator zespołu badawczo-rozwojowego:
o Doświadczenie w planowaniu procesu B+R;
o Umiejętność pisania dokumentacji projektowej i technicznej oraz raportów;
o Doświadczenie w zakresie agregacji, analizy i wizualizacji danych;
o Znajomość metodyki PRINCE 2 lub PMI PMP (raportowanie na poziomie projektu i portfela projektów);
o Umiejętność pisania artykułów naukowych, raportów, recenzji i streszczeń;
o Umiejętność prowadzenia analiz przedwdrożeniowych i projektowania procesów biznesowych;
o Umiejętność przygotowywania wniosków badawczych i wniosków/ofert o dofinansowanie;
o Znajomość SQL;
o Umiejętnością wykorzystania narzędzi projektowych;
o Znajomość narzędzi JIRA, Confluence.

• Analityk bezpieczeństwa:
o Zaawansowana wiedza z dziedzin: technologii sieciowych, systemów operacyjnych, technologii i rozwiązań bezpieczeństwa, standardów, norm i metodologii informatycznych, wykonywania testów penetracyjnych;
o Wiedza i doświadczenie w konfiguracji i administracji systemów operacyjnych Windows oraz Linux/Unix;
o Praktyczna znajomość zagrożeń sieciowych oraz systemów i technologii bezpieczeństwa: IDS, IPS, Firewall, WAF, SIEM, EDR, DLP, oprogramowania antywirusowego, sandbox, skanerów podatności, systemów antyspamowych;
o Bardzo dobra znajomość protokołów: HTTP, HTTPS, SSH, FTP, SMTP, IMAP, POP, SNMP, WMI, syslog, NTP, DHCP, DNS, CIFS, NFS, itp.
o Znajomość zagadnień kryptograficznych;
o Umiejętność analizy złośliwego oprogramowania;
o Doświadczenie w przeprowadzaniu analizy powłamaniowej;
o Zaawansowana wiedza w zakresie wykonywania testów penetracyjnych.
o Minimum 2 lata w pracy na stanowiskach związanych z bezpieczeństwem IT;
o Praktyczna znajomość zabezpieczeń stosowanych w systemach informatycznych oraz metod przeprowadzania ataków na systemy IT, sposobów obrony oraz narzędzi do analizy zdarzeń i wykrywania incydentów bezpieczeństwa.

• Architekt IT:
o Znajomość notacji UML;
o Analityczne myślenie oraz rozwiązywanie złożonych problemów;
o Umiejętności modelowania architektury rozwiązań;
o Znajomość architektury oraz bezpieczeństwa IT/OT (m.in. tworzenie modelu bazy danych, podział na komponenty, zastosowanie frameworków);
o Doświadczenie w programowaniu interfejsów w m.in. C#, Python;
o Umiejętnością wykorzystania narzędzi projektowych;
o Znajomość narzędzi JIRA, Confluence;
o Znajomość wzorców architektonicznych na potrzeby budowania architektury rozwiązania;
o Wiedza praktyczna z zakresu sieci LAN/WAN.

- Inżynier wdrożeniowy:
  - Znajomość zagadnień konteneryzacji oraz CI/CD;
  - Wiedza oraz doświadczenie w pracy ze środowiskami zwirtualizowanymi;
  - Dobra znajomość rozwiązań IT (systemy operacyjne, systemy serwerowe, usługi teleinformatyczne);
  - Doświadczenie w zarządzaniu MS SQL Server, Sharepoint, Exchange;
  - Znajomość SQL;
  - Bardzo dobra znajomość języków skryptowych (m.in. Python, bash, Perl);
  - Minimum roczne doświadczenie we wdrożeniach systemów informatycznych.

- Tester bezpieczeństwa:
  - Bardzo dobra znajomość protokołów TCP/IP oraz protokołów : HTTP, HTTPS, SSH, FTP, SMTP, IMAP, POP, SNMP, WMI, syslog, NTP, DHCP, DNS, CIFS, NFS, itp.;
  - Minimum 2 lata w pracy na stanowiskach związanych z testowaniem bezpieczeństwa IT;
  - Znajomość metodologii testów penetracyjnych (OWASP, WASC-TC, PTES, OSSTMM);
  - Umiejętność pisania raportów technicznych;
  - Znajomość zagadnień kryptograficznych;
  - Znajomość testowania hardware technikami inżynierii wstecznej oprogramowania;
  - Umiejętność testowania pod kątem bezpieczeństwa aplikacji mobilnych oraz API;
  - Fizyczne testy bezpieczeństwa;
  - Dobra znajomość języka skryptowego (m.in. Python, bash, Perl);
  - Wiedza i doświadczenie w użytkowaniu systemów operacyjnych Windows oraz Linux/Unix.

Metodyka Zespołu Badawczo-Rozwojowego

Narzędzia badawcze

W ramach zadań i celów zidentyfikowanych dla ZBR, niezbędne będzie wykorzystanie odpowiednich narzędzi. Zgodnie z obecnym stanem techniki, w obszarze badań nad cyberbezpieczeństwem wykorzystywane są:

- Piaskownice: mechanizmy uruchamiania programów komputerowych w odizolowanych od reszty systemów środowiskach. Narzędzia te wykorzystywane są do uruchamiania programów potencjalnie niebezpiecznych lub pochodzących z niezaufanych źródeł.
- Wirtualne platformy sprzętowe: Wirtualizacja to sposób tworzenia odseparowanej warstwy sprzętu komputerowego za pomocą oprogramowania. Dzięki niej elementy sprzętowe jednego komputera — takie jak procesory, pamięć operacyjna, masowa i nie tylko — można podzielić na wiele urządzeń wirtualnych, powszechnie nazywanych maszynami wirtualnymi (VM). Wykorzystywane są one m.in. do uruchamiania piaskownic.
- Fizyczne platformy sprzętowe: Komputery PC, serwery, urządzenia sieciowe.
- Analizatory ruchu sieciowego: Oprogramowanie do analizy ruchu sieciowego.
- Narzędzia programistyczne i projektowe: Programy komputerowe służący do tworzenia, projektowania, modyfikowania i testowania oprogramowania (np. kompilatory, debuggery).
- Dziedzinowe systemy informatyczne i automatyki przemysłowej: Wyspecjalizowane systemy IT/OT wykorzystywane w sektorze kolejowego.
- Dostęp do baz wiedzy: Wykorzystywanie dostępnych źródeł informacji, know-how.

Jednocześnie, weryfikacja, aktualizacja i rozbudowa listy narzędzi będzie należeć do kluczowych zadań ZBR.

Proces badawczy

W ramach podstawowych zadań ZBR wykorzystywana będzie metodyka wypracowana przez SOC i CERT. Podstawą dla działań ZBR stanowić będą frameworki i metryki dla zespołów CSIRT takie, jak standardy FIRST CSIRT czy metryki ochrony informacji NIST.

Podstawą dla prowadzenia prac badawczo-rozwojowych w zespole ZBR jest kierowanie się kryteriami definiującymi działalność B+R, to jest:

- Kryterium nowatorskości: w sektorze przedsiębiorstw, projekty B+R mają prowadzić do wyników nowych dla przedsiębiorstwa i rozwiązań niewykorzystywanych w branży. Spełnia je również wytwarzanie wiedzy na potrzeby nowych produktów czy procesów.
- Kryterium twórczości: projekt B+R opiera się na oryginalnych, nieoczywistych koncepcjach i hipotezach.
- Kryterium nieprzewidywalności: na początkowych etapach prac badawczych niemożliwe jest dokładne określenie rezultatów i kosztów prac. Oznacza to, że prototypy wytwarzane w ramach prac B+R mają na celu weryfikację hipotez, a nie uzyskiwanie certyfikatów technicznych czy prawnych.
- Kryterium metodyczne: działalność badawczo rozwojowa prowadzona jest w sposób zaplanowany, z dokładną rejestracją przebiegu i wyników procesu.
- Kryterium odtwarzalności: wyniki projektu B+R powinny dawać potencjalną możliwość wykorzystania wytworzonej wiedzy czy rozwiązań innym zespołom badawczym.

W procesie badawczo-rozwojowym dodatkowo kluczowe jest dobranie odpowiednich metryk, pozwalających na precyzyjną ewaluację skuteczności opracowywanych rozwiązań.

Przykładowo, w zagadnieniu au-

tomatycznego wykrywania szkodliwego stosowane są metryki charakterystyczne dla problemów typu klasyfikacja w uczeniu maszynowym (jak precision, recall i F1 score). W zagadnieniu oceny skuteczności zestawów reguł w firewallach stosowane są metryki z domeny wytwarzania oprogramowania, takie, jak złożoność cyklomatyczna czy złożoność halstead, jak również unikalne metryki mierzące, np. poziom współzależności reguł.

Modele współpracy z Zespołem Badawczo-Rozwojowym

Model współpracy z zespołami SOC i CERT

Współpraca z SOC i CERT będzie odbywać się na zasadach wymiany informacji oraz doświadczeń z obszaru informatycznego oraz sieci. Model ten zakłada również przeprowadzanie badań zleconych przez w/w zespoły. Realizowane będą zadania z zakresu cyberbezpieczeństwa a jego wyniki przedstawiane będą na spotkaniach podsumowujących prace badawczo-rozwojowe.

Model współpracy z KPRM, MON, ABW, NASK PIB

Współpraca z organami właściwymi do spraw cyberbezpieczeństwa (CSIRT GOV, CSIRT MON, CSIRT NASK) i organami władzy publicznej w Rzeczypospolitej Polskiej przebiegać będzie na zasadach określonych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, jak również w myśl uchwały nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Polski na lata 2019-2024.

Model współpracy z Instytutem Kolejnictwa, NASK, ISAC-Kolej, sieciami i innymi podmiotami badawczymi

Współpraca z ISAC-Kolej opierać się będzie na zasadach ustalonych w porozumieniu o utworzeniu ISAC-Kolej zawartym przez Spółkę. Zespół Badawczo-Rozwojowy będzie przekazywał zidentyfikowane problemy zwiększające ryzyko wystąpienia incydentów cyberbezpieczeństwa, jak również wspomagał proces opracowywania polityk, procedur i standardów dostosowanych do potrzeb podsektora kolejowego.

W pracach B+R, Zespół Badawczo Rozwojowy może wykorzystywać ekspertyzę badawczą w zakresie cyberbezpieczeństwa i podsektora kolejowego Naukowej i Akademickiej Sieci Komputerowej Państwowego Instytutu Badawczego (NASK), Instytutu Kolejnictwa i sieci badawczych na mocy obecnie obwiązujących, lub zawartych w tym celu umów. Równocześnie, ZBR może świadczyć usługi dla wyżej wymienionych instytucji, na przykład poprzez wspólne uczestnictwo w programach grantowych.

Zakończenie

Dla utrzymania żywotnych funkcji społecznych, zapewnienia bezpieczeństwa i ochrony obywateli niezbędna jest infrastruktura krytyczna. Jej uszkodzenie, zniszczenie lub zakłócenie w wyniku klęsk żywiołowych, terroryzmu, awarii, działalności przestępczej lub złośliwych zachowań, może mieć znaczący i negatywny wpływ na bezpieczeństwo i dobrostan obywateli. Infrastruktury krytyczne (IK) są niezbędne do zagwarantowania obywatelom Unii Europejskiej (UE) podstawowych funkcji gospodarczych i społecznych. Świadczone przez nie usługi, w połączeniu z ich transgranicznym charakterem i współzależnościami, sprawiają że infrastruktury krytyczne stają się coraz bardziej narażone na różnego rodzaju zagrożenia, nie tylko naturalne i przypadkowe (losowe), ale także celowe. Wraz z postępem technologicznym i głębokimi wzajemnymi połączeniami, zmienia się i ewoluuje krajobraz potencjalnych zagrożeń na terytorium UE, torując drogę do większej podatności na nie. Jednym z rodzajów są cyberataki, które w przypadku wystąpienia zjawiska „awarii kaskadowej" dokonują sekwencyjnego uszkodzenia sieci. Awaria jednej (pojedynczej) części (elementu) danej infrastruktury krytycznej może doprowadzić do załamania się jej innych (kolejnych) części (ogniw, komponentów) a ostatecznie do poważnych uszkodzeń w całej sieci. Dodatkowo rosnąca zależność IK od zagranicznego postępu technologicznego (korzystanie i implementacja rozwiązań informatycznych spoza państw UE, głównie z Chin) stanowi kolejny czynnik złożoności oraz podatności na ataki i uszkodzenia z zewnątrz. Dotychczasowa ochrona infrastruktur krytycznych regulowana jest dyrektywą 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony1,(tzw. dyrektywą EIK), transponowaną do porządków prawnych poszczególnych państw członkowskich. Do polskiego porządku prawnego poprzez przyjęcie ustawy z dnia 29 października 2010 r. o zmianie ustawy o zarządzaniu kryzysowym. Natomiast obszar cyberbezpieczeństwa opracowuje dyrektywa UE NIS oraz NIS2.

Dyrektywa NIS została przyjęta 6 lipca 2016 r. Jest pierwszym europejskim prawem w zakresie cyberbezpieczeństwa. Dyrektywa nakłada na państwa członkowskie szereg obowiązków, obliguje je do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. W Polsce jej zapisy realizuje ustawa o krajowym systemie cyberbezpieczeństwa (KSC) z 28 sierpnia 2018 roku. Obecnie oczekiwana jest implementacja w polskim ustawodawstwie zapisów dyrektywy NIS2 poprzez nowelizację ustawy o KSC, zwiększająca obowiązki i zadania podmiotów w zakresie zabezpieczeń przed cyberzagrożeniami.

Realizacja omawianych zadań wymaga działań zainteresowanych instytucji zgodnych z przedstawionym modelem współpracy. ◄