PREZES
NAJWYŻSZEJ IZBY KONTROLI
Departament Infrastruktury

KIN.410.6.2.2023

Pan
Tadeusz Turzyński
Prezes PKP Informatyka Sp. z o. o.
al. Jerozolimskie 142A
02-305 Warszawa

WYSTĄPIENIE POKONTROLNE

P/23/017 Funkcjonowanie systemów zarządzania kryzysowego na kolei.

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 50 00, F +48 22 444 57 93
nik@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa

I. Dane identyfikacyjne

Jednostka kontrolowana	PKP Informatyka Sp. z o. o. (dalej: PKP IK) 02-305 Warszawa, al. Jerozolimskie 142A
Kierownik jednostki kontrolowanej	Tadeusz Turzyński – Prezes Zarządu PKP Informatyka Sp. z o. o. (dalej: Prezes)[1] [Dowód: akta kontroli str. 18-20]
Zakres przedmiotowy kontroli	Świadczenie na rzecz zarządcy infrastruktury i przewoźników kolejowych oraz zarządcy dworców kolejowych usług informatycznych lub telekomunikacyjnych i utrzymaniowych niezbędnych do realizacji przewozów kolejowych, funkcjonowania dworców kolejowych i obsługi pasażerów, w sytuacjach o charakterze kryzysowym występujących na kolei.
Okres objęty kontrolą	Lata 2020 – 2023 (I półrocze)
Podstawa prawna podjęcia kontroli	Kontrola została przeprowadzona na podstawie art. 2 ust. 1 ustawy o Najwyższej Izbie Kontroli[2].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Infrastruktury
Kontrolerzy	Maria Rainczuk, specjalista kontroli państwowej, upoważnienie do kontroli nr KIN/46/2023 z dnia 28 czerwca 2023 r. [Dowód: akta kontroli str. 1]

[1] W okresie objętym kontrolą funkcję kierownika jednostki kontrolowanej pełnił: Tadeusz Turzyński na podstawie Uchwały Wspólnika Spółki PKP Informatyka sp. z o. o. z dnia 26 marca 2019 r. i Uchwały nr 8 Zwyczajnego Zgromadzenia Wspólników PKP Informatyka Sp. z o. o. z dnia 10 czerwca 2022 r.

[2] Dz. U. z 2022 r. poz. 623 ze zm., dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

PKP Informatyka sp. z o.o. posiadała organizację i procedury pozwalające zapewnić bezpieczeństwo usług informatycznych świadczonych na rzecz kontrahentów tej spółki.

PKP IK, jako sygnatariusz porozumienia w sprawie organizacji kolejowego systemu zarządzania kryzysowego[4] rzetelnie współpracowała ze spółkami kolejowymi, organami lub innymi podmiotami w zakresie wymiany informacji i doświadczeń dotyczących cyberbezpieczeństwa infrastruktury oraz transportu kolejowego. PKP IK przyjęła do stosowania, uregulowane w tym Porozumieniu, zasady i procedury dotyczące postępowania w sytuacjach o charakterze kryzysowym na kolei.

Ponadto PKP IK prowadziła skuteczny monitoring bezpieczeństwa usług kluczowych PKP Polskich Linii Kolejowych S.A.[5] tj. Systemu ewidencji pracy eksploatacyjnej[6] i Internetowego systemu zamawiania trasy pociągu[7].

PKP IK wdrażając dedykowane oprogramowanie na rzecz kontrahentów, jednocześnie rzetelnie dbała o jego utrzymanie i zapewniała użytkownikom wsparcie IT.

Spółka skutecznie zarządzała bezpieczeństwem i zapewniała ciągłość działania tworzonego oprogramowania i świadczonych usług IT w zakresie umów, które objęto szczegółowym badaniem.

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[4] Porozumienie z dnia 30 października 2017 r. w sprawie organizacji kolejowego systemu zarządzania kryzysowego oraz monitorowania bieżącej pracy eksploatacyjno–przewozowej na liniach kolejowych zarządzanych przez PKP Polskie Linie Kolejowe S.A. oraz budynkach i budowlach przeznaczonych do obsługi osób i rzeczy, zawarte pomiędzy PKP Polskie Linie Kolejowe S.A., a PKP Informatyka sp. z o.o., PKP S.A., PKP Energetyka S.A., PKP Telekom sp. z o.o. oraz PKP Utrzymanie sp. z o.o., dalej: Porozumienie.

[5] Dalej: PKP PLK S.A.

[6] Dalej: SEPE.

[7] Dalej: ISZTP.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

Świadczenie na rzecz zarządcy infrastruktury i przewoźników kolejowych oraz zarządcy dworców kolejowych usług informatycznych lub telekomunikacyjnych i utrzymaniowych niezbędnych do realizacji przewozów kolejowych, funkcjonowania dworców kolejowych i obsługi pasażerów, w sytuacjach o charakterze kryzysowym występujących na kolei.

Opis stanu faktycznego

PKP Informatyka sp. z o.o. działała na podstawie umowy spółki, statutu[9] i Kodeksu Spółek Handlowych[10]. Do podstawowych zadań Spółki w okresie objętym kontrolą należało w szczególności:

- świadczenie i sprzedaż usług w zakresie opracowywania, wdrażania, eksploatacji, utrzymania i rozwoju systemów informatycznych,
- świadczenie i sprzedaż usług w zakresie wdrażania, eksploatacji i utrzymania systemów informatycznych niebędących produktami Spółki,
- budowa i zarządzanie systemami telekomunikacyjnymi oraz świadczenie usług telekomunikacyjnych,
- świadczenie i sprzedaż usług w zakresie administrowania serwerami i bazami danych, siecią informatyczną, obsługi integracyjnej systemów i wspomagania użytkownika,
- świadczenie i sprzedaż usług w zakresie informatycznej obsługi technicznej i technologicznej.

Ponadto PKP IK zapewniała ciągłość działania systemów i aplikacji kluczowych dla funkcjonowania kolei w Polsce – m.in. systemu rezerwacji i sprzedaży biletów kolejowych, systemu obsługi przesyłek towarowych, a także monitorowała krytyczne dla kolei systemy, aplikacje i infrastrukturę IT operacyjnego centrum bezpieczeństwa.

Spółka świadcząc powyższe usługi - nie była właścicielem oraz posiadaczem samoistnym i zależnym obiektów, instalacji lub urządzeń infrastruktury krytycznej. Zarządcy infrastruktury krytycznej mieli obowiązek jej ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia.

Szczegółową organizację wewnętrzną i zakres zadań komórek organizacyjnych określał Regulamin organizacyjny PKP IK z dnia 28 listopada 2001 r. ze zmianami[11].

---

[8] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[9] Akt Notarialny Repertorium A nr 16913/2018, Protokół Nadzwyczajnego Zgromadzenia Wspólników z dnia 21.11.2018r., Akt Notarialny Rep A nr 1838/2021, Protokół Nadzwyczajnego Zgromadzenia Wspólników z dnia 01.02.2021r., Akt Notarialny Rep A nr 13890/2021, Protokół NZW z dnia 16.06.2021r., Akt Notarialny Rep A nr 4737/2022, Protokół NZW z dnia 09.03.2022r., Akt Notarialny Rep A nr 8663/2022, Protokół NZW z dnia 09.05.2022r., Akt Notarialny Rep A nr 27241/2022, Protokół NZW z dnia 22.12.2022r., Akt Notarialny Rep A nr 3323/2023, Protokół NZW z dnia 03.03.2023r.

[10] Ustawa z dnia 15 września 2000 r. Kodeks Spółek Handlowych (Dz.U. z 2022 r. poz. 1467 ze zm.).

[11] Regulamin organizacyjny PKP Informatyka spółka z o.o. uchwalony Uchwałą nr 60/2019 Zarządu PKP Informatyka spółka z o.o. z dnia 15.05.2019 r. i zatwierdzony uchwała Rady Nadzorczej nr 18/VII/2019 r. z 27.05.2019 r., Uchwałą nr 3/2020 Zarządu PKP Informatyka spółka z o.o. z dnia 20.01.2020 r. i zatwierdzony uchwała Rady Nadzorczej 2/VII/2020 z 27.01.2020 r., Uchwałą nr 129/2020 Zarządu PKP Informatyka spółka z o.o. z dnia 21.12.2020 r. i zatwierdzony Uchwałą Rady Nadzorczej 33/VII/2020 z 28.12.2020 r., Uchwałą nr 152/2021Zarządu PKP Informatyka spółka z o.o. z dnia 08.12.2021 r. i zatwierdzony Uchwałą Rady Nadzorczej

W Regulaminie organizacyjnym nie określono bezpośrednio, która komórka organizacyjna Spółki była właściwa w sprawach zarządzania kryzysowego (zarządzania sytuacjami kryzysowymi).

W Regulaminie określono, że Biuro Centrum Kompetencyjne Bezpieczeństwa IT było odpowiedzialne za zapewnienie m.in.:

- warunków do bezpiecznego funkcjonowania Spółki w obszarach bezpieczeństwa teleinformatycznego,
- bezpieczeństwa danych i informacji,
- bezpieczeństwa fizycznego,
- monitorowania zasobów krytycznych,
- zarządzania bezpieczeństwem ciągłości działania,
- zapewnienia bezpieczeństwa teleinformatycznego.

Do kompetencji kolejnego Biura - Centrum Kompetencyjnego Obsługi Technicznej IT należały m.in.:

- obsługa techniczna i utrzymanie rozwiązań dedykowanych dla obsługi podróżnych i bezpieczeństwa dworców kolejowych zarówno w obszarze systemów teleinformatycznych jak i urządzeń IT,
- obsługa i rozwiązywanie incydentów/problemów związanych z teleinformatyczną infrastrukturą dworcową.

Zgodnie z Regulaminem za komunikację kryzysową (zarządzanie informacją w sytuacjach nadzwyczajnych) odpowiedzialne było Wieloosobowe Stanowisko ds. Marketingu Strategicznego w Biurze Strategii i Architektury Spółki.

[Dowód: akta kontroli str. 2-8, 12-42]

PKP IK była jednym z sygnatariuszy porozumienia zawartego 30 października 2017 r. z PKP PLK S.A. w sprawie organizacji kolejowego systemu zarządzania kryzysowego oraz monitorowania bieżącej pracy eksploatacyjno-przewozowej na liniach kolejowych zarządzanych przez PKP Polskie Linie Kolejowe S.A. oraz w budynkach i budowlach przeznaczonych do obsługi osób i rzeczy. Zgodnie z postanowieniem § 2 ust. 2 Porozumienia Zarząd PKP IK delegował swoich przedstawicieli, którzy wchodzili w skład zespołów zarzadzania kryzysowego w PKP PLK S.A. Delegowanymi przedstawicielami PKP IK byli - Członek Zarządu odpowiedzialny za sprawy bezpieczeństwa oraz Dyrektor Biura Centrum Kompetencyjnego odpowiedzialnego za Infrastrukturę IT. Przedstawiciele PKP IK uczestniczyli w spotkaniach zespołów zwoływanych przez koordynującego pracę Kolejowego Centrum Zarządzania Kryzysowego w PKP PLK S.A. (dalej: KCZK). Na każdorazowe wezwanie ze strony PKP PLK S.A. - PKP IK przekazywała aktualny wykaz osób delegowanych do udziału w KCZK.

PKP IK jako sygnatariusz Porozumienia przyjęła do stosowania następujące regulacje:

- „Zasady organizacji kolejowego systemu zarzadzania kryzysowego w czasie wystąpienia zagrożeń oraz sytuacji kryzysowych na liniach kolejowych zarządzanych przez PKP Polskie Linie Kolejowe SA oraz w budynkach

34/VIII/2021 z 29.12.2021 r., Uchwałą nr 36/2022 Zarządu PKP Informatyka spółka z o.o. z dnia 22.03.2022 r. i zatwierdzony Uchwałą Rady Nadzorczej 4/VIII/2022 z 30.03.2022., Uchwałą nr 167/2022 Zarządu PKP Informatyka spółka z o.o. z dnia 20.12.2022 r. i zatwierdzony Uchwałą Rady Nadzorczej 38/VIII/2022 z 29.12.2022 r.

Uchwałą nr 77/2022 Zarządu PKP Informatyka spółka z o.o. z dnia 13.06.2022 r. i zatwierdzony Uchwałą Rady Nadzorczej 20/VIII/2022 z 29.06.2022 r.

i budowlach przeznaczonych do obsługi osób i rzeczy", dalej: „Zasady organizacji",

- „Zasady monitorowania bieżącej pracy ekspolatacyjno-przewozowej i postepowania w czasie wystąpienia zagrożeń, sytuacji kryzysowych, innych wydarzeń na liniach kolejowych zarządzanych przez PKP Polskie Linie Kolejowe SA oraz budynkach i budowlach przeznaczonych do obsług osób i rzeczy", dalej: „Zasady monitorowania"

Nadzór i koordynację w zakresie organizacji i funkcjonowania kolejowego systemu zarządzania kryzysowego sprawowała PKP PLK S.A. Zarząd PKP IK natomiast był odpowiedzialny w szczególności za podejmowanie, w zakresie swoich kompetencji, działań mających na celu ograniczenie negatywnych skutków zagrożeń i sytuacji kryzysowych.

[Dowód: akta kontroli str. 50-193]

W okresie objętym kontrolą w obszarze działalności prowadzonej przez PKP IK zaistniały zagrożenia, które spełniały przesłanki do uznania je za sytuacje kryzysowe w rozumieniu § 1 ust. 2 „Zasad organizacji". Były to:

- zagrożenie chorobą szczególnie niebezpieczną i wysoce zakaźną COVID-19,
- wprowadzenie trzeciego stopnia alarmowego Charlie-CRP,
- sytuacja polityczno-militarna na Ukrainie.

W celu zapewnienia sprawnej realizacji procesu eksploatacyjno-przewozowego w związku z zagrożeniem chorobą szczególnie niebezpieczną i wysoce zakaźną COVID-19 Przewodniczący Zespołu Zarządzania Kryzysowego w PKP PLK S.A. Decyzją nr 7/2020 z dnia 10 marca 2020 r. powołał KZZK. Natomiast Decyzją nr 8/2020 z 10 marca 2020 r. Przewodniczący imiennie określił skład i czas rozpoczęcia pracy KCZK.

W związku z wprowadzeniem trzeciego stopnia alarmowego Charlie-CRP Przewodniczący KZZK Decyzją nr 5 z dnia 22 lutego 2022 r. imiennie określił skład i rozpoczęcie pracy KCZK. Na posiedzeniu KCZK 22 lutego 2022 r. ustalono, że w PKP IK zespół monitorowania (funkcjonujący w ramach Centrum Operacji Bezpieczeństwa - SOC) prowadził działalność w trybie całodobowym, ustalone zostały grafiki dyżurów jego poszczególnych członków, przeglądano i testowano ciągłość działania świadczonych usług i dostępność wymaganych backupów danych.

W dniu 28 lutego 2022 r. odbyła się telekonferencja[12] dotycząca sytuacji na wschodniej granicy Polski oraz możliwości uruchomienia dodatkowych pociągów. 10 maja 2022 r. odbyła się telekonferencja[13] dotycząca planowanego strajku generalnego pracowników Polregio S.A.

Sporządzane notatki ze spotkań KZZK służyły utrwaleniu ustaleń i koordynacji działań podmiotów kolejowych współpracujących w ramach tego Zespołu.

Decyzją nr 23 i Decyzją nr 24 z dnia 29.06.2023 r. Przewodniczący KZZK zakończył pracę Kolejowego Centrum Zarządzania Kryzysowego w powyższych sprawach.

[Dowód: akta kontroli str. 147-193]

Niezależnie od obowiązującego porozumienia z PKP PLK S.A. - PKP IK w okresie objętym kontrolą podjęła działania w związku z wprowadzeniem na obszarze kraju stanu epidemii wirusa SARS-CoV-2. Decyzją Prezesa PKP IK z 19 marca 2020 r. na posiedzeniu sztabu kryzysowego w Spółce ogłoszono sytuację kryzysową. Podstawą podjęcia tej decyzji było zagrożenie zdrowia pracowników, a w konsekwencji możliwe

[12] Notatka z posiedzenia KZZK powołanego w związku z sytuacją polityczno-militarną z dnia 28.02.2022 r.

[13] Notatka z posiedzenia KZZK powołanego w związku z planowanym strajkiem generalnym w Polregio S.A. z dnia 10.05.2022 r.

zakłócenie ciągłości świadczonych usług. Z chwilą wybuchu wojny na Ukrainie rozszerzono zakres działalności sztabu kryzysowego. W związku z wystąpieniem powyższych zagrożeń Zarząd PKP IK podjął m.in. działania:

- uruchomienia pracy w formie telepracy w celu ograniczenia ryzyka wzajemnych zarażeń i zachowania ciągłości świadczonych przez Spółkę usług,
- podwyższenia gotowości zespołów wsparcia oprócz już istniejących rozwiązań organizacyjnych.

W PKP IK celem zapewnienia ciągłości działania i dostępności usług informatycznych, w tym zapewnienia monitorowania zdarzeń w obszarze cyberbezpieczeństwa usług świadczonych na rzecz klientów Spółki, prowadzono działania w zakresie:

- całodobowych usług centrum operacji bezpieczeństwa (SOC),
- klasyfikacji incydentów bezpieczeństwa z wykorzystaniem metodologii Triage,
- reagowania na incydenty z zakresu cyberbezpieczeństwa zaistniałe w obszarach krytycznych elementów infrastruktury IT, używanych systemów, serwerów oraz sieci LAN/WAN, funkcjonowania usług i procesów lub niepożądanych działań użytkowników,
- szybkiej reakcji i obsługi incydentów na podstawie scenariuszy postępowania opracowanych z klientami Spółki,
- cyklicznego raportowania stanu bezpieczeństwa.

Prezes Zarządu PKP IK nie był zobowiązany do informowania Przewodniczącego KZZK o fakcie powołania sztabu kryzysowego. Powołanie tego sztabu nie wynikało bowiem z sytuacji zgłoszonej przez PKP PLK S.A., która prowadziła do zakłóceń w procesie eksploatacyjno-przewozowym realizowanym na liniach kolejowych zarządzanych przez PKP PLK S.A. Działania operacyjne w zakresie reagowania na sytuacje kryzysowe w Spółce wynikały z decyzji Zarządu PKP IK w tym zakresie.

W związku z powyższym Prezes Zarządu PKP IK nie przekazywał również meldunków i raportów do KZZK, o których mowa w §7 pkt 2 i §pkt 3 ppkt 2 Zasad organizacji. Powołanie sztabu kryzysowego oraz związane z tym działania były decyzjami Zarządu PKP IK, które wynikały z samodzielnie przeprowadzonej oceny sytuacji i zagrożeń, nie zaś ze współdziałania z KZZK w PKP PLK S.A.

W PKP IK nie opracowano własnych, wewnętrznych procedur dotyczących zarządzania (reagowania) kryzysowego. Członkowie Zarządu PKP IK wyjaśnili, iż *Porozumienie zawarte z PKP PLK S.A. nie nakłada na PKP IK takiego obowiązku, a przyjęte i stosowane w Spółce narzędzia i rozwiązania zapewniają należyty poziom bezpieczeństwa przetwarzanych danych i informacji w trybie całodobowym, przez siedem dni w tygodniu*.

[Dowód: akta kontroli str. 149-158]

W PKP IK wykorzystywano specjalistyczne narzędzia i rozwiązania, które kompleksowo i w czasie rzeczywistym pozwalały na analizę stanu bezpieczeństwa informatycznego Spółki oraz służyły zapewnieniu należytego poziomu bezpieczeństwa przetwarzanych danych i informacji. W PKP IK zabezpieczono infrastrukturę PKP IK przed niepowołanym dostępem osób nieuprawionych.

W ramach struktury PKP IK działały dwa zespoły: SOC reagujący na zdarzenia bezpieczeństwa oraz zespół NOC[14] monitorujący dostępność zasobów PKP IK i klientów. PKP IK należała do europejskiej organizacji zrzeszającej zespoły

[14] Centrum Operacyjne Sieci.

CERT[15]/CSIRT[16]. W listopadzie 2022 PKP IK spełniała wymagania kryteriów dojrzałości i uzyskała akredytacji Trusted Introducer.

Zespoły odpowiedzialne za cyberbezpieczeństwo podnosiły swoje kompetencje poprzez uczestnictwo w wydarzeniach tematycznych (konferencje, szkolenia, gry zespołowe polegające na zabezpieczaniu systemów przed realnymi atakami). Dla systemów i aplikacji przeprowadzane były testy bezpieczeństwa (pentesty) weryfikujące poprawność ich funkcjonowania oraz występowania w nich słabości.

[Dowód: akta kontroli str. 149-152, 155-158, 430, 991, 999-1000, 1006]

PKP IK posiadała certyfikaty potwierdzające spełnianie wymagań: norm Systemu Zarządzania Bezpieczeństwem Informacji: ISO/IEC 27001:2013, norm Systemu Zarządzania Jakością: ISO 9001: 2015 a także certyfikat potwierdzający spełnianie wymagań norm Systemu Zarządzania Usługami IT ISO/IEC 20000-1:2018. Ponadto zespół reagowania na incydenty komputerowe CERT PKP IK, przeszedł pozytywnie weryfikację i został akredytowanym członkiem międzynarodowej organizacji GÉANT TF-CSIRT Trusted Introducer zrzeszającej zespoły cyberbezpieczeństwa. Uzyskanie tego statusu poprzedzone zostało oceną dojrzałości zespołu CERT i SOC w obszarze organizacyjnym, zasobów ludzkich, technicznym i procesów zgodnie z metodyką Security Incident Management Maturity Model (dalej: SIM3), wytycznymi Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (dalej: ENISA) oraz Ustawą o Krajowym Systemie Cyberbezpieczeństwa[17].

[Dowód: akta kontroli str. 375]

PKP IK opracowała i wdrożyła wewnętrzne procedury dotyczące monitorowania i reagowania na incydenty i zdarzenia:

- procedurę reagowania na zdarzenia DDos,
- procedurę reagowania na zdarzenia z kategorii Malware,
- procedurę reagowania na zdarzenia z kategorii Phishing.

Ponadto na podstawie ustaleń z PKP S.A - PKP IK przeprowadziła kolejne działania dotyczące bezpieczeństwa informatycznego, m.in.:

- wdrożyła procedury związane z wprowadzeniem stopnia alarmowego Charlie CRP,
- dokonała przeglądu stosowanych procedur, w szczególności w zakresie obsługi incydentów bezpieczeństwa,
- zweryfikowała dostępność i funkcjonowanie wewnętrznych środków łączności,
- potwierdziła dostępność środków łączności z Ministerstwem Infrastruktury, CERT POLSKA oraz CERT GOV,
- przeprowadziła analizę dzienników zdarzeń pod kątem stanu bezpieczeństwa systemów teleinformatycznych i systemów telekomunikacyjnych,
- zweryfikowała dostępność posiadanych kopii zapasowych użytkowanych systemów biznesowych,
- sprawdziła dostępność funkcjonalności w zakresie zarzadzania incydentami dot. sprzętu mobilnego (lokalizacja, blokowanie i kasowanie danych). Ponadto PKP IK dokonała przeglądu dostępnych zasobów zapasowych pod

[15] Zespół PKP IK reagowania na incydenty (Computer Emergency Response Team).

[16] Zespół PKP IK reagowania na incydenty bezpieczeństwa komputerowego (Computer Security Incident Response Team).

[17] Dz.U. z 2023, poz. 913.

względem możliwości ich wykorzystania w przypadku potencjalnego zaistnienia ataku.

[Dowód: akta kontroli str. 432, 991-992, 1009-1029]

PKP IK pozyskiwała i wymieniała się ze spółkami kolejowymi informacjami oraz doświadczeniami z zakresu zapobiegania i reagowania na sytuacje kryzysowe w szczególności dotyczące cyberbezpieczeństwa na kolei. Odbywało się to w ramach porozumienia ISAC-Kolej[18] oraz bilateralnych kontaktów. Wśród sygnatariuszy porozumienia ISAC-Kolej były**:** PKP S.A., PKP Intercity S.A., PKP CARGO S.A., PKP Informatyka Sp. z o.o., PKP Linia Hutnicza Szerokotorowa Sp. z o.o., PKP Szybka Kolej Miejska w Trójmieście Sp. z o.o., PKP Polskie Linie Kolejowe S.A., Pomorska Kolej Metropolitarna, Instytut Kolejnictwa oraz NASK – Państwowy Instytut Badawczy.

Wymiana danych w ramach porozumienia ISAC-Kolej dotyczyła w szczególności:

- wiedzy o możliwych ryzykach, występujących incydentach,
- zapobiegania incydentom w obszarze cyberbezpieczeństwa,
- gromadzenia i pogłębiania wiedzy na temat podsektora kolejowego ze źródeł krajowych i zagranicznych,
- wypracowania standardów w zakresie cyberbezpieczeństwa w podsektorze kolejowym,
- edukacji pracowników podmiotów zrzeszonych w ISAC-Kolej w zakresie cyberbezpieczeństwa.

Ponadto w ramach realizacji zawartych umów do kontrahentów Spółki prowadzona była dystrybucja informacji o zagrożeniach (niebezpieczne adres IP, złośliwe domeny) poprzez materiały informacyjne, takie jak komunikaty, biuletyny.

[Dowód: akta kontroli str. 430, 993]

PKP IK wykonywała również zadania na rzecz PKP PLK S.A., m.in. w ramach świadczonej umowy w zakresie Centrum Operacji Bezpieczeństwa (SOC). Do zadań PKP IK należało min.: podjęcie działań mających na celu monitorowanie środowiska teleinformatycznego w zakresie cyberbezpieczeństwa, monitorowanie i reagowanie na incydenty cyberbezpieczeństwa teleinformatycznego w tym współpraca z właściwym CSIRT, raportowanie bieżącej sytuacji (w przypadku wystąpienia incydentu sklasyfikowanego jako krytyczny, poważny lub istotny, mający wpływ na środowisko teleinformatyczne) oraz przekazanie końcowych raportów o stanie realizacji przedmiotowych zadań.

[Dowód: akta kontroli str. 443, 996-997]

PKP IK w ramach porozumienia Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego „ISAC - Kolej" przekazywała do Urzędu Transportu Kolejowego informacje dotyczące obszaru cyberbezpieczeństwa, miedzy innymi: o możliwych ryzykach, zagrożeniach oraz występujących incydentach i sposobach ich skutecznej obsługi w obszarze cyberbezpieczeństwa, jak również o dobrych praktykach z obszaru cyberbezpieczeństwa.

[Dowód: akta kontroli str.432-433, 995]

PKP IK przekazywała do PKP S.A. następujące raporty:

- o stanie realizacji zadań, wynikających z wprowadzonego stopnia alarmowego Charlie-CRP dotyczących infrastruktury IT PKP S.A.
- o wystąpieniu zdarzeń mających znamiona incydentu (do Centrum Bezpieczeństwa Dworców Kolejowych PKP S.A.).

[18] Centrum Wymiany i Analizy Informacji.

PKP IK w przypadku zdarzeń mających znamiona incydentu przesyłała również doraźnie raport do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (dalej: CSIRT GOV). Natomiast w ramach obowiązującej z PKP PLK S.A. umowy SOC - PKP IK prowadziła monitoring bezpieczeństwa usług kluczowych PKP PLK S.A. tj. SEPE i ISZTP.

[Dowód: akta kontroli str. 147, 151-152, 430, 991]

W okresie objętym kontrolą w PKP IK miało miejsce 25 incydentów zakwalifikowanych jako incydenty bezpieczeństwa: w 2020 r. – 7 incydentów bezpieczeństwa, 2021 r. – 4, 2022 r. – 10, 2023 r. – 4. W 2022 r. zwiększyła się liczba ataków DDoS[19] tj. ataku, którego celem było zablokowanie dostępu do serwera lub usługi poprzez zalewanie go dużą liczbą fałszywych żądań. Informacje związane z atakami DDoS były przekazywane do CSIRT Agencji Bezpieczeństwa Wewnętrznego.

[Dowód: akta kontroli str.433, 996]

W okresie objętym kontrolą (w okresie obowiązywania stopnia alarmowego Charlie CRP) PKP IK otrzymała 2374 sygnały dotyczące potencjalnych zagrożeń[20]. Reakcja na otrzymywane od innych podmiotów ostrzeżenia dotyczące kampanii phishingowych lub niebezpiecznych adresów polegała na min. przesłaniu ostrzeżeń do pracowników, blokowaniu komunikacji z niebezpiecznymi adresem, usuwaniu niebezpiecznych wiadomości z serwerów.

[Dowód: akta kontroli str.433, 997]

W okresie objętym kontrolą, Decyzją z dnia 24 lutego 2022 .r Prezes Zarządu PKP S.A., wydał polecenie spółkom Grupy PKP przygotowywania od 25 lutego 2022 r. raportów dotyczących zakłóceń w funkcjonowaniu Spółki w związku z wojną na Ukrainie. Raportowanie obejmowało przekazywanie informacji: wpływu na funkcjonowanie spółki w związku z wojną na Ukrainie, zidentyfikowanych zakłóceń (zdarzenia, które wystąpiły, w tym incydenty w cyberprzestrzeni) i ocenę, prognozę skutków bieżących wydarzeń. PKP IK przekazała PKP S.A. (do Zespołu do spraw monitorowania sytuacji na Ukrainie) 66 raportów w okresie od 26 lutego 2022 r. do 28 lutego 2023 r. Na podstawie ww. raportów stwierdzono, że nie wystąpiły zdarzenia (incydenty), które miały wpływ na funkcjonowanie spółki PKP IK (wojna na Ukrainie i cyberprzestrzeń).

[Dowód: akta kontroli str. 147-193, 294-321]

W okresie objętym kontrolą PKP IK była stroną 168 umów tzw. przychodowych, których kontrahentami były podmioty odpowiedzialne za prowadzenie przewozów kolejowych, funkcjonowanie dworców kolejowych lub za obsługę pasażerów. PKP IK zawarła powyższe umowy w zakresie przedmiotu swojej działalności tj. m.in. w zakresie:

- eksploatacji systemów informatycznych,
- infrastruktury IT i jej utrzymania,
- zakupu usług w zakresie Operacyjnego Centrum Cyberbezpieczeństwa (SOC),
  np. monitorowania wystąpienia zdarzeń/incydentów,
- świadczenia usług utrzymania konserwacji systemów i urządzeń zainstalowanych na dworcach kolejowych,

[19] Distributed Denial of Service.

[20] Poszczególne sygnały o zagrożeniach PKP IK otrzymała od: ISAC-kolej – 769 ostrzeżeń, RCB – 786, CSIRT.GOV – 665, CERT.PL – 134, MON.GOV – 20.

Ponadto PKP IK była w okresie objętym kontrolą stroną ośmiu porozumień zawartych ze spółkami kolejowymi, które dotyczyły m.in.:

- potwierdzenia woli współpracy w zakresie realizacji zadań wdrożenia u kontrahenta dedykowanego oprogramowania,
- utworzenia Centrum Wymiany i Analizy Informacji dotyczących incydentów cyberbezpieczeństwa,
- budowy i uruchomienia Wspólnego Centrum Przetwarzania Danych,
- Porozumienia z 2017 r. zawartego z PKP PLK S.A. i innymi spółkami kolejowymi w sprawie organizacji kolejowego sytemu zarządzania kryzysowego.

Szczegółowemu badaniu poddano sześć umów zawartych w okresie objętym kontrolą.

PKP IK w celu wypełniania zadań wynikających z zawartych umów wprowadziła organizację czasu pracy pracowników w sposób ciągły (dyżury). Zatrudnieni pracownicy PKP IK pracowali również w zakresie Help Desk[21] - problemy w działaniu usług były zgłaszane przez kontrahentów Spółki telefonicznie i mailowo. W godzinach nocnych pracownicy monitorowali sieć i infrastrukturę IT kontrahentów PKP IK w ramach Centrum Operacji Bezpieczeństwa (SOC).

[Dowód: akta kontroli str. 194-196, 202, 212, 217-218, 232-236, 258, 260-261, 274-276, 287-288, 322-368]

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

IV. Uwagi i wnioski

Najwyższa Izba Kontroli nie formułuje uwag i wniosków.

[21] Komórka odpowiedzialna za usługę zgłoszeń od klientów PKP IK. Procedurę obsługi zgłoszeń określa każdorazowo umowa z danym klientem.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Prezesa NIK. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, grudnia 2023 r.

Najwyższa Izba Kontroli
Departament Infrastruktury
p.o. Dyrektor
Paweł Zambrzycki

.....
podpis

Kontroler prowadzący kontrolę
Szymon Tyburski
gł. specjalista kp.

.....
podpis