MINISTER CYFRYZACJI

Mateusz Morawiecki

DNK.WK.1743.1.2022.JG

Warszawa, /elektroniczny znacznik czasu/

Pani
Anna Moskwa

Minister
Klimatu i Środowiska

WYSTĄPIENIE POKONTROLNE

Przedstawiam Pani Minister *Wystąpienie pokontrolne* (dalej: *Wystąpienie*) z kontroli przeprowadzonej[1] przez Kancelarię Prezesa Rady Ministrów w Ministerstwie Klimatu i Środowiska[2] (dalej: MKiŚ, Ministerstwo, Jednostka) w zakresie *wykorzystania systemów teleinformatycznych do realizacji zadań publicznych w okresie od 6 października 2020 r. do 23 maja 2022 r.*[3].

Podstawa prawna:
Art. 25 ust. 1 pkt 3 lit. c i 25a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4] (dalej: *ustawa o informatyzacji*) oraz art. 46 ust. 1 i 3 oraz art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[5] (dalej: *ustawa o kontroli*).

MKiŚ wykorzystywało 3 systemy teleinformatyczne do realizacji zadań publicznych:

BDO – *Baza danych o produktach i opakowaniach oraz gospodarce odpadami* jest systemem teleinformatycznym utworzonym na podstawie *ustawy o odpadach*[6]. BDO to rejestr podmiotów wprowadzających produkty, produkty w opakowaniach i gospodarujących odpadami. Umożliwia kompleksowe gromadzenie i zarządzanie danymi z zakresu gospodarowania odpadami. Minister Klimatu i Środowiska powierzył[7] administrowanie systemem BDO Instytutowi Ochrony Środowiska – Państwowemu Instytutowi Badawczemu (dalej: IOŚ).

PDWD – *Publicznie dostępny wykaz danych*, system ten wykorzystywany jest do:

- publikowania informacji o dokumentach związanych z ochroną środowiska, przez urzędy administracji;
- udostępniania informacji o środowisku naturalnym i jego ochronie.

Stanowi on zbiór kart informacyjnych, z których każda opisuje pojedynczy dokument, jego miejsce przechowywania oraz odniesienie do dokumentów z nim powiązanych. Obowiązek prowadzenia publicznie dostępnych wykazów danych przez jednostki administracji właściwe w sprawach dot. informacji o środowisku i jego ochronie wynika z *ustawy o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko*[8].

---

[1] Kontrolę przeprowadzili pracownicy Kancelarii Prezesa Rady Ministrów: Magda Jarosławska, radca, kierownik zespołu kontrolującego, Jakub Gicka, główny specjalista, członek zespołu kontrolującego. Czynności kontrolne realizowano w okresie od 16 maja do 15 lipca 2022 r. w siedzibie Ministerstwa przy ul. Wawelskiej 52/54, 00-922 Warszawa. Kontrolerzy spełniają wymagania określone w art. 28 ust. 1 *ustawy o informatyzacji*, w tym posiadają jeden z certyfikatów wymienionych w załączniku do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz. U. Nr 177, poz. 1195).

[2] MKiŚ powstało 6 października 2020 r. w drodze przekształcenia Ministerstwa Klimatu (dalej: MK). Wtedy do MK obsługującego działy administracji rządowej *energia* i *klimat* dołączono działy *środowisko* oraz *gospodarka wodna* (na podst. rozporządzenia Rady Ministrów z dnia 7 października 2020 r. w sprawie utworzenia MKiŚ, Dz. U. poz. 1734). Następnie na mocy rozporządzenia Rady Ministrów z dnia 10 października 2020 r. w sprawie przekształcenia MKiŚ (Dz. U. poz. 2005) z jego struktury wyłączono sprawy z działu *gospodarka wodna*. Od 13 listopada 2020 r. Minister KiŚ kieruje 3 działami administracji rządowej (*energia*, *klimat* i *środowisko*).

[3] Z wyłączeniem obszarów dot. zabezpieczeń techniczno-organizacyjnych systemów oraz wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami/rejestrami informatycznymi i wspomagania świadczenia usług drogą elektroniczną.

[4] Dz. U. z 2021 r., poz. 2070, t. j. ze zm. W okresie objętym kontrolą obowiązywał tekst jednolity opublikowany w Dz. U. z 2020 r. poz. 346 oraz z 2021 r. poz. 670.

[5] Dz. U. z 2020 r., poz. 224 t. j.

[6] Art. 79 ust. 1 ustawy z 14 grudnia 2012 r. (Dz. U. z 2022 r. poz. 699 t. j.).

[7] Na podstawie porozumienia nr 1 zawartego 7 grudnia 2018 r. wraz z 3 aneksami.

[8] Ustawa z 3 października 2008 r. (Dz. U. z 2022 r. poz. 1029, t. j. ze zm.).

EZD PUW – system służący do elektronicznego zarządzania dokumentacją autorstwa Podlaskiego Urzędu Wojewódzkiego z Białegostoku. Wdrażany jest w administracji rządowej jako jednolity system, rozwijany na zasadach niekomercyjnych, będący narzędziem wymiany informacji oraz usprawnienia funkcjonowania urzędów.

Systemy te poddano badaniu, w zakresie w jakim za ich administrowanie i rozwój odpowiadało MKiŚ.

OCENA KONTROLOWANEGO OBSZARU

Ministerstwo nie posiadało kompleksowego i spójnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI). Wymaga on istotnego wzmocnienia oraz pilnych działań naprawczych w celu zapewnienia bezpieczeństwa informacji (dalej: BI). W obszarze tym stwierdzono szereg nieprawidłowości, których usunięcie wymaga podjęcia niezwłocznych czynności. Do skutecznego jego wdrożenia potrzebna jest identyfikacja obszarów wymagających zmiany/korekty oraz proaktywne zarządzanie systemem. W szczególności niezbędne jest opracowanie rzetelnej analizy ryzyka dot. wszystkich aktywów, przeprowadzonej na podstawie uporządkowanych zasad, opracowanie całościowej dokumentacji oraz wdrożenie narzędzi nadzorczych dostarczających Kierownictwu MKiŚ pełnych informacji nt. poszczególnych etapów jego ustanawiania.

Istotnym jest, że główne osoby zaangażowane w BI, tj. Pełnomocnik ds. BI i Administrator Bezpieczeństwa Teleinformatycznego (dalej: ABT), odeszły z pracy, przez co Ministerstwo zostało pozbawione ważnych informacji nt. funkcjonowania systemu, ponieważ nie posiadało aktualnej i kompletnej dokumentacji SZBI.

System zarządzania bezpieczeństwem informacji

- **[SZBI]** Warunkiem skutecznego zarządzania BI jest posiadanie kompleksowej dokumentacji, podczas gdy wszystkie wdrożone regulacje na dzień rozpoczęcia czynności kontrolnych były nieaktualne, wymagały zmiany bądź uzupełnienia lub dostosowania do funkcjonujących rozwiązań.
- **[Wsparcie Kierownictwa w zarządzaniu BI]** Dyrektor Generalny nie był efektywnie wspierany w zarządzaniu BI przez Zespół ds. SZBI. Wynika to z niewystarczającej aktywności Zespołu i nieprzekazywania przez niego materiałów dających podstawę do skutecznego zarządzania BI. W szczególności Zespół nie przedstawiał zbiorczych informacji, które są kluczowe w procesie zarządzania, tj. planu/strategii rozwoju i doskonalenia SZBI. Kierownictwo nie posiadało zatem instrumentów zarządczych do podejmowania adekwatnych decyzji w zakresie systemu. Ponadto w MKiŚ nie został zrealizowany całościowy przegląd SZBI, wykonano go jedynie w odniesieniu do wybranych obszarów.
- **[Porozumienie dot. BDO]** Brak precyzyjnego określenia zadań i odpowiedzialności w zakresie administrowania oraz utrzymywania BDO stanowi istotną lukę w SZBI. W tym przedmiocie zawarto Porozumienie[9] pomiędzy MKiŚ a IOŚ, jednak nie określono w nim szczegółowego podziału zadań, nie sprecyzowano zasad i obszarów współpracy obu stron Porozumienia.
- **[Analiza ryzyka]** Funkcjonowanie dwóch odmiennych metodologii wykonywania analizy ryzyka w odrębnych regulacjach nie zapewniało przejrzystości procesu. Ponadto zastrzeżenia budzą przyjęte w nich założenia. Proces nie jest uporządkowany, w Polityce Bezpieczeństwa Informacji MKiŚ[10] (dalej: PBI lub Polityka) nie wdrożono podziału pomiędzy aktywami istotnymi i krytycznymi. Regulacje nie określały także podziału

[9] Porozumienie nr 1 z 7 grudnia 2018 r. wraz z 3 aneksami (nr 1 z 23 stycznia 2019 r., nr 2 z 29 sierpnia 2019 r., nr 3 z 3 grudnia 2020 r.).
[10] Z 2 lutego 2021 r.

pomiędzy środkami przetwarzania informacji w zakresie komórek organizacyjnych, a aktywami odnoszącymi się do środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych. Dokumenty dotyczące analizy ryzyka były nierzetelnie i nieterminowo przygotowane.

- **[Audyt]** W Ministerstwie wdrożono regulacje[11] określające konieczność realizacji corocznego audytu BI. Zrealizowano 2 audyty w latach 2020-2021, jednak ze względu na przedłużający się termin zawarcia umowy na doskonalenie SZBI w ramach, której planowano kolejny audyt w 2022 r., obowiązek jego wykonania przynajmniej raz w roku nie został spełniony. Ponadto audyty z lat 2020-2021 nie objęły badaniem wszystkich obszarów BI, co przy braku przeglądów SZBI, nie zapewniło pełnej identyfikacji słabości systemu i nie wspierało Jednostki w ich eliminacji. Zastrzeżenia również budzi niewdrożenie rekomendacji z tych audytów.
- **[Baza CMDB]** MKiŚ nie posiadało relacyjnej bazy konfiguracji CMDB, tym samym nie spełniono wymogów określonych w § 20 ust. 2 pkt 2 Rozporządzenia KRI[12]. Procedura pn. *Baza konfiguracji CMDB* była nieaktualna i nie przestrzegano jej postanowień.
- **[Uprawnienia]** Nie ustanowiono kompleksowych regulacji w obszarze nadawania, modyfikacji i odbierania uprawnień do PDWD i BDO, a regulacje te w stosunku do EZD PUW wymagały aktualizacji. Podjęcia działań naprawczych wymaga funkcjonalność BDO pozwalająca pracownikowi z dostępem użytkownika głównego na tworzenie kont dla innych użytkowników (m.in. z tym samym zakresem uprawnień), mimo braku stosownego upoważnienia. Ponadto nie dokonywano cyklicznych przeglądów nadanych uprawnień, z wyjątkiem systemu EZD PUW, jednak nie dokumentowano tych działań.
- **[Incydenty]** W obszarze incydentów (z wyłączeniem BDO) funkcjonowały szczątkowe regulacje, a szereg zagadnień mających na celu wskazanie właściwych norm postępowania nie został określony. Realizowano obowiązek rejestracji incydentów, jednak rejestr ten nie był rzetelnie prowadzony przez Zespół ds. SZBI, tzn. nie wszystkie dane w poszczególnych pozycjach zostały uzupełniane. Dodatkowo zakres danych w nim gromadzonych wymaga rozszerzenia w szczególności o dane dot. priorytetu/poziomu incydentów, godziny ich zgłoszenia i zamknięcia (czasu obsługi).
- **[Szkolenia]** Kontynuacji wymagają działania dot. zwiększania świadomości pracowników w zakresie BI. Z powodu trwających prac nad nową PBI szkolenie wstrzymano, a wymóg corocznego udziału w nim zrealizowano jedynie w odniesieniu do 14 z 973 (1,5%) pracowników. W toku kontroli wznowiono je i przeszkolono 779 pracowników. W stosunku do stażystów, praktykantów i wolontariuszy nie monitorowano obowiązku zapoznania się z PBI oraz nie przestrzegano konieczności uwzględnienia w umowach cywilnoprawnych tego wymogu przez osoby, które świadczyły na rzecz Ministerstwa usługi wpływające na poufność, integralność lub dostępność informacji.
- **[Umowy]** Umowy dotyczące serwisu oraz rozwoju infrastruktury i systemów informatycznych częściowo zabezpieczały interesy Skarbu Państwa. Zasadnym byłoby rozszerzenie ich postanowień, w szczególności o kwestię dot. bezstronności wykonawców. Nie opracowano regulacji wewnętrznych w zakresie zawierania takich umów.
- **[Praca zdalna]** Na urządzeniach mobilnych stosowano zabezpieczenia chroniące informacje, w szczególności przez uwierzytelnienie użytkownika, bezpieczne szyfrowane połączenie VPN oraz instalację aktualnego oprogramowania antywirusowego. Wdrożono narzędzia umożliwiające monitorowanie użytkowników, jednakże czynności te nie były dokumentowane. Ponadto zasadnym byłoby rozszerzenie przyjętych zasad pracy zdalnej

[11] § 5 zarządzenia w sprawie SZBI oraz § 9 pkt 10 PBI.
[12] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, t. j.).

o informacje nt. możliwości korzystania z ogólnodostępnej lub domowej sieci Wi-Fi, a w przypadkach jej dopuszczenia wskazanie opisu wymaganych zabezpieczeń.

- **[Kopie zapasowe]** Działania w zakresie wykonywania i przechowywania kopii zapasowych wymagają intensyfikacji. Wykonywano kopie zapasowe 3 badanych systemów teleinformatycznych, jednakże okres retencji ich przechowywania wymaga zwiększenia. Zasadnym byłoby również przeniesienie macierzy na przechowywanie kopii poza lokalizację, gdzie uruchomione są systemy teleinformatyczne oraz wdrożenie rozwiązań dot. dokumentowania działań związanych z ich odtworzeniem. Czynności w tym przedmiocie nie były wspierane przez regulacje, które były nieaktualne i nie określały funkcjonujących rozwiązań.
- **[Zabezpieczenia organizacyjno-techniczne dostępu do informacji]** W MKiŚ nie zostały określone zasady naprawy sprzętu informatycznego, a zasady ochrony fizycznej oraz utylizacji nośników danych nie były aktualne.

  Wdrożono rozwiązania zapewniające rejestrację ruchu osobowego, jednak nie wszystkie tymczasowe karty dostępu wydane Generalnej Dyrekcji Ochrony Środowiska[13] (dalej: GDOŚ) zostały przypisane imiennie do danego użytkownika, co nie pozwalało na pełną kontrolę osób przebywających w MKiŚ. Ponadto w toku kontroli doszło do wyniesienia klucza poza teren MKiŚ oraz wydania klucza pracownikowi firmy zewnętrznej.
- **[Projektowanie, eksploatacja oraz wdrażanie zmian w systemach]** Istnieje potrzeba aktualizacji i uzupełnienia regulacji w zakresie projektowania, wdrażania oraz przeprowadzania zmian w systemach. Nie przestrzegano postanowień *Procedury zgłaszania zmiany i wykonywania testów*. Podejmowano działania dot. monitorowania systemów, a proces wdrażanych zmian w PDWD oraz EZD PUW był przejrzysty.
- **[Plan ciągłości działania]** W MKiŚ nie wdrożono całościowego planu ciągłości działania. Celem obowiązujących regulacji było *minimalizowanie zakłóceń w realizacji działalności zadań Ministerstwa Środowiska w związku z uszkodzeniem systemu informatycznego*, podczas gdy plan ciągłości działania to plan wznawiania działania jednostki w obszarze kluczowych procesów w przypadku wystąpienia katastrofy. Ponadto na skutek odejścia z pracy głównych osób zaangażowanych w BI, Ministerstwo nie było w stanie potwierdzić czy *Plan ciągłości działania systemów informatycznych w Ministerstwie Środowiska* był w badanym okresie testowany.
- **[Rozliczalność działań]** Użytkowane przez MKiŚ 3 systemy teleinformatyczne zapewniały rozliczalność działań użytkowników, a informacje zawarte w dziennikach systemów (logach) były przechowywane przez 2 lata. Realizowano działania związane z przeglądem logów i ich analizą w celu identyfikacji działań niepożądanych, jednak ich nie dokumentowano. Wdrożone regulacje nie były zaktualizowane i nie określały zasad przeglądu dzienników systemów (logów) i ich analizy.

OCENY I USTALENIA SZCZEGÓŁOWE

I. System zarządzania bezpieczeństwem informacji

1. [stan *SZBI*] Negatywnie należy ocenić, że Ministerstwo nie posiadało kompleksowego i spójnego SZBI. System potrzebuje istotnego wzmocnienia oraz pilnych działań naprawczych w celu zapewnienia bezpieczeństwa informacji. W szczególności jego wdrożenie wymaga przeprowadzenia przeglądu, rzetelnej analizy ryzyka w odniesieniu do wszystkich aktywów, przeprowadzonej na podstawie uporządkowanych zasad oraz opracowania całościowej dokumentacji, która jest warunkiem skutecznego zarządzania BI. Wszystkie wdrożone

[13] GDOŚ użytkuje pomieszczenia MKiŚ na podstawie zawartego porozumienia z 11 maja 2021 r. *w sprawie udostępnienia powierzchni i miejsca w serwerowni MKiŚ*.

w Jednostce regulacje na dzień rozpoczęcia czynności kontrolnych były nieaktualne, wymagały zmiany bądź uzupełnienia albo dostosowania do funkcjonujących rozwiązań.

Wśród regulacji SZBI, obowiązywało ogólne zarządzenie *w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w MKiŚ*[14] (dalej: Zarządzenie w sprawie SZBI), w szczególności powierzające nadzór nad systemem Dyrektorowi Generalnemu, którego w zarządzaniu nim wspierał Zespół ds. SZBI. Wymagało ono uzupełnienia, w szczególności w przedmiocie określenia terminu i zakresu informacji, jakie powinny być przekazywane Kierownictwu Ministerstwa przez Zespół ds. SZBI.

Ponadto obowiązywały następujące polityki / procedury / zasady:

- PBI wraz z 9[15] załącznikami;
- 24[16] procedury eksploatacyjne;
- Polityka Bezpieczeństwa Informacji Systemu BDO (dalej: PBI BDO) wraz z 6[17] załącznika mi, przy czym w przypadku 2[18] z nich Ministerstwo nie posiadało podpisanych dokumentów, co wskazuje, że nie zostały one wdrożone.

Pomimo upływu ponad 19[19] m-cy od przekształcenia Ministerstwa Klimatu i utworzenia MKiŚ nadal nie zaktualizowano znacznej części regulacji, tj.: *PBI w zakresie bezpieczeństwa fizycznego, Polityki bezpieczeństwa w zakresie przetwarzania danych osobowych w Ministerstwie Klimatu* (zał. nr 7 i 9 do PBI), 22 z 24 (92%) procedur eksploatacyjnych (pomimo że część z nich sięga lat 2012-2014); PBI BDO wraz z 5 załącznikami.

Pozostałe dokumenty, tj. PBI z 7 załącznikami, 2[20] procedury eksploatacyjne i 1 załącznik do PBI BDO – *Procedura kontroli (zarządzania) dostępu do systemu BDO*, mimo że podlegały aktualizacji po utworzeniu MKiŚ, nadal wymagają zmiany, ponieważ z dniem 13 kwietnia 2022 r. wyodrębniono ze struktury Biura Dyrektora Generalnego (dalej: BDG)[21] Departament Informatyzacji (dalej: DI), w tym zmieniono odpowiedzialność za poszczególne zadania.

Na potrzebę przeglądu i aktualizacji regulacji wskazywał już w 2020 r. audyt systemu BDO[22] w odniesieniu do PBI BDO wraz z załącznikami, jak i w 2021 r. audyt wewnętrzny[23]. Pomimo tego decyzja nt. tego przeglądu została podjęta przez Zastępcę Pełnomocnika ds. BI dopiero 31 grudnia 2021 r. Przygotowano do zmiany 17[24] procedur eksploatacyjnych, a ich zatwierdzenie planowane było do sierpnia 2022 r.

Wyjaśniono[25], że nie są znane powody dla których ówczesny Pełnomocnik ds. BI nie zintensyfikował prac nad regulacjami z zakresu SZBI. Wskazano również, że prace te zostały wstrzymane z uwagi na ogłoszenie zamówienia w zakresie udoskonalenia SZBI.

Pomimo zawarcia 3 sierpnia 2020 r. umowy z Europejską Agencją Wykonawczą ds. Klimatu, Infrastruktury i Środowiska (CINEA) w sprawie wspomożenia organu właściwego do spraw cyberbezpieczeństwa, postępowanie o udzielenie zamówienia publicznego pn. *Świadczenie specjalistycznych usług w zakresie doskonalenia SZBI w MKiŚ,* w ramach którego

---

[14] Zarządzenie Ministra Klimatu i Środowiska z dnia 15 stycznia 2021 r. (Dz. Urz. Ministra KiŚ poz. 5).

[15] **1.** *Wzór potwierdzenia zapoznania z Polityką Bezpieczeństwa*; **2.** *Wzór tabeli aktywów*; **3.** *Wzór tabeli szacowania ryzyka*; **4.** *Zestawienie przykładowych zagrożeń dla informacji*; **5.** *Mapa procesu zarządzania incydentem*; **6.** *Zasady korzystania z zasobów informatycznych MKiŚ*; **7.** *PBI w Ministerstwie Środowiska w zakresie bezpieczeństwa fizycznego*; **8.** *PBI w MKiŚ w zakresie cyberbezpieczeństwa*; **9.** *Polityka bezpieczeństwa w zakresie przetwarzania danych osobowych w Ministerstwie Klimatu.*

[16] **1.** *Baza konfiguracji CMDB – Określenie polityki konfiguracji, elementów składowych oraz zakresu i szczegółowości bazy konfiguracji*; **2.** *Procedura otwierania, modyfikowania oraz zamykania kont w systemach informatycznych MKiŚ*; **4.** *Polityka monitorowania parametrów – Polityka określa zasady monitorowania paramentów mających wpływ na ciągłość działania systemów informatycznych w MŚ*; **5.** *Procedura utrzymywania rejestru awarii oraz dziennika czynności technologicznych systemów teleinformatycznych i urządzeń sieciowych*; **7.** *Procedura bezpieczeństwa i utylizacji sprzętu elektronicznego wraz z załącznikami*; **8.** *Procedura zgłaszania zmiany i wykonywania testów* wraz z załącznikiem; **9.** *Procedura stosowania środków kryptograficznych*; **10.** *Procedura określania specyfikacji technicznych wymagań odbioru systemów IT*; **13.** *Procedura wydawania komputerów* wraz z załącznikami; **14.** *Procedura wydawania i aktywacji Tokena VPN*; **15.** *Procedura backupu systemu EZD*; **18.** *Procedura zarządzania incydentem bezpieczeństwa teleinformatycznego*; **19.** *Procedura utrzymywania rejestru konferencji i spotkań*; **20.** *Procedura dodawania kart do systemu kontroli dostępu (UniKD) oraz wprowadzania kart do systemu wydruku centralnego*; **22.** *Procedura włączania i wyłączania systemów informatycznych*; **23.** *Procedura awaryjna*; **24.** *Procedura tworzenia, modyfikacji i zamykania kont użytkowników autoryzowanych Publicznie dostępnego wykazu danych (PDWD)*; **25.** *Procedura odzyskiwania danych logowania i akceptacji żądań certyfikacyjnych w Wykazie*; **26.** *Polityka kontroli dostępu*; **27.** *Procedura zakładania, modyfikowania i zamykania kont kandydatów na platformie Moodle*; **28.** *Regulamin przebywania w Centrum Danych Ministerstwa Środowiska (DC MŚ)*; **29.** *Odebranie/nadanie uprawnień w systemie QUORUM (QNT)* wraz z załącznikiem; **30.** *Plan ciągłości działania systemów informatycznych w Ministerstwie Środowiska*; **31.** *Zasady zarządzania i obsługi bazy wiedzy MKiŚ.*
Katalog procedur i instrukcji bezpieczeństwa (dalej: Katalog) stosowanych w MKiŚ wskazuje, że zostało wdrożonych 31 procedur eksploatacyjnych, jednakże **procedura 3** pn. *Procedury eksploatacyjne systemów informacyjnych*, to nie jedna procedura, a instrukcje, podręczniki użytkownika i administratora wdrożonych systemów informatycznych; **procedura 6** pn. *Dziennik wejść i wyjść do serwerowni* nie obowiązywała (została zastąpiona *Procedurą utrzymywania dzienników administratora systemu / bazy oraz administratora sieci LAN*, a ta z kolei *Procedurą utrzymywania rejestru awarii oraz dziennika czynności technologicznych systemów teleinformatycznych i urządzeń sieciowych* i była to procedura 5 z Katalogu); **pozycja 11** pn. *Dokument żądania zmiany w systemie* to nie odrębna regulacja, a załącznik do procedury nr 8 pn. *Procedura zgłaszania zmiany i wykonywania testów*; **procedura 12** pn. *Procedura zmiany hasła*, to załącznik do procedury 13 *Procedura wydawania komputerów*; Ministerstwo nie posiadało zatwierdzonej **procedury 16** pn. *Procedura aktywacji karty kryptograficznej – kwalifikowany certyfikat z dodatkowymi danymi.* W skład procedur eksploatacyjnych wchodziły także: **17**. *Zasady publikowania materiałów na stronach internetowych MŚ* oraz **21.** *Procedura dotycząca realizacji przez WESI/WRSI działań wykonywanych w stopniach alarmowych,* które były poza zakresem objętym kontrolą.

[17] **1.** *Procedura kontroli (zarządzania) dostępu do Systemu BDO*; **2.** *Procedura kontroli dostępu dla użytkowników uprzywilejowanych Systemu BDO*; **3.** *Procedura zarządzania incydentami w Systemie BDO*; **4.** *Procedura zarządzania zmianą w Systemie BDO*; **5.** *Procedura Disaster Recovery w Systemie BDO* (*Plan awaryjny dla BDO)*, **6.** *Rejestr ryzyk w bezpieczeństwie informacji dla Systemu BDO.*

[18] *Procedura kontroli dostępu dla użytkowników uprzywilejowanych systemu BDO* oraz *Procedura Disaster Recovery w Systemie BDO* (*Plan awaryjny dla BDO).*

[19] Licząc do końca okresu objętego kontrolą.

[20] *Procedura otwierania. modyfikowania, oraz zamykania kont w systemach informatycznych MKiŚ* oraz *Zasady zarządzania i obsługi Bazy Wiedzy MKiŚ.*

[21] Zarządzenie nr 72 Prezesa Rady Ministrów z dnia 11 kwietnia 2022 r. zmieniające zarządzenie w sprawie nadania statutu Ministerstwu Klimatu i Środowiska.

[22] *Raport z audytu systemu BDO* z 14 października 2020 r.

[23] Sprawozdanie z audytu wewnętrznego na temat *Ocena realizacji działań prowadzonych w zakresie bezpieczeństwa informacji.*

[24] Oraz 2 regulacje: *Zasady publikowania materiałów na stronach internetowych MŚ* i *Procedurę dotycząca realizacji przez WESI/WRSI działań wykonywanych w stopniach alarmowych,* które były poza zakresem objętym kontrolą.

[25] Pismo z 13 lipca 2022 r., znak: DI-WRSI.081.14.2022.AS.

zaplanowano aktualizację dokumentacji, ogłoszono dopiero 13 maja 2022 r., tj. po upływie 21 miesięcy.

Wskazano[26], że od 2021 r. trwał proces przygotowania opisu przedmiotu zamówienia, przy czym nie bez znaczenia było utworzenie MKiŚ 6 października 2020 r. Ustalenie procesów i zasobów wymagało czasu i uzgodnień z kierownictwem. Prośbę o decyzję w kierunku udoskonalenia SZBI przekazano do Dyrektora Generalnego 25 sierpnia 2021 r., który zgodę na rozpoczęcie prac wydał następnego dnia. MKiŚ nie było w stanie ustalić przyczyn ogłoszenia postępowania po upływie 8 m-cy od wydania zgody. Jednakże wskazało, że po jej uzyskaniu rozpoczęto prace nad przygotowaniem projektu umowy, trwały konsultacje w tym zakresie z Inspektorem Ochrony Danych (dalej: IOD), ABT oraz Administratorem Bezpieczeństwa Fizycznego (dalej: ABF). Jednym z powodów opóźnienia mogła być fluktuacja kadrowa pracowników pełniących kluczowe role w SZBI[27].

MKiŚ 24 czerwca 2022 r. zawarło umowę na świadczenie specjalistycznych usług w zakresie udoskonalenia SZBI (dalej: umowa na doskonalenie SZBI). Wykonanie jej przedmiotu miało nastąpić do 26 sierpnia 2022 r. i objąć 4 etapy:

1) Etap I – przeprowadzenie audytu SZBI dot. spełniania wymagań organizacyjnych, technicznych oraz prawnych ze szczególnym uwzględnieniem RODO, zgodności z normami ISO wraz z opracowaniem rekomendacji zmian w dokumentacji SZBI oraz przeprowadzenie inwentaryzacji aktywów podstawowych;
2) Etap II – aktualizacja dokumentacji z uwzględnieniem rekomendacji z audytu SZBI;
3) Etap III – przygotowanie i przeprowadzenie szkoleń w zakresie wprowadzonych zmian w dokumentacji oraz opracowanie i dostarczenie materiałów z zakresu BI, w tym ochrony danych osobowych i bezpieczeństwa teleinformatycznego na potrzeby uruchomienia przez Ministerstwo szkoleń wewnętrznych w formie e-learningu;
4) Etap IV – świadczenie konsultacji specjalistycznych, polegających na wsparciu Zespołu ds. SZBI w eksploatacji, utrzymywaniu i doskonaleniu SZBI.

Ustanowienie SZBI, który zapewnia poufność, dostępność i integralność informacji wymaga wdrożenia kompleksowych regulacji gwarantujących sprawność jego działania. Dlatego MKiŚ powinno zintensyfikować prace nad ich przygotowaniem. Zrozumiałe jest, że uporządkowanie SZBI po utworzeniu Jednostki wymaga czasu, to jednak tak długi okres aktualizacji regulacji nie był zasadny.

2. Wdrożone regulacje nie są ze sobą spójne i nie zapewniły przejrzystości w zakresie ich stosowania, ponieważ posługują się odmiennymi pojęciami (w tym takimi, które nie zostały wyjaśnione), powołują się na role, które nie zostały zdefiniowane oraz regulacje, które nie obowiązują bądź zostały wdrożone pod inną nazwą, a także poszczególne zagadnienia są rozproszone po różnych regulacjach.

W szczególności PBI, jako dokument nadrzędny w SZBI, nie wyjaśnia czym jest SZBI. Posługuje się pojęciem *system informacyjny*, nie posługuje się pojęciami system informatyczny i system teleinformatyczny, nie wdraża podziału pomiędzy nimi, podczas gdy w procedurach eksploatacyjnych pojęcia te są stosowane, np. *Procedura otwierania, modyfikowania oraz zamykania kont w systemach informatycznych MKiŚ*, *Procedura utrzymywania rejestru awarii oraz dziennika czynności technologicznych systemów teleinformatycznych i urządzeń sieciowych* (dalej: *Procedura utrzymywania rejestru awarii*). W niektórych procedurach dodatkowo stosowane jest pojęcie *system IT*[28].

W *Zasadach korzystania z zasobów informatycznych MKiŚ* w jednej definicji stosuje się wyjaśnienie 2 pojęć, tj. wprowadza się definicję zasobu informatycznego, w której jednocześnie wyjaśnia się jak należy rozumieć pojęcie *urządzenia teleinformatyczne*. Natomiast procedury eksploatacyjne nie posługują się pojęciem *urządzeń teleinformatycznych*, a m.in. pojęciem *sprzęt informatyczny*.

Definicja *incydentu* zawarta jest w PBI, a odmienna znajduje się w procedurze *Baza konfiguracji CMDB*, która dodatkowo wprowadza definicję *problemu*. Kolejna definicja wskazana była w PBI BDO wraz z definicją *Awarii* i *Usterki*, powtórzona w *Procedurze zarządzania incydentami w Systemie BDO* z podziałem na różne rodzaje incydentów. PBI

[26] Pismo z 5 lipca 2022 r., znak: DI-WRSI.081.12.2022.AS.
[27] Pismo z 3 sierpnia 2022 r., znak: DI-WRSI.081.22.2022.AS.
[28] *Procedura określania specyfikacji technicznych wymagań odbioru systemów IT*.

częściowo reguluje obszar incydentów, dodatkowo obowiązuje *Procedura zarządzania incydentem bezpieczeństwa teleinformatycznego,* przy czym nie zdefiniowano incydentu bezpieczeństwa teleinformatycznego. PBI mówi o incydentach w obszarze cyberbezpieczeństwa, a załącznik nr 5 do PBI wskazuje na incydenty bezpieczeństwa teleinformatycznego.

PBI w zakresie cyberbezpieczeństwa wskazuje, że instrukcja wykonywania kopii zapasowych znajduje się w *Polityce kopii zapasowych*, podczas gdy dokument ten to *Procedura awaryjna*. *Procedura otwierania, modyfikowania oraz zamykania kont w systemach informatycznych MKiŚ* wskazuje, że użytkownik ustanawia nowe hasło, zgodnie z procedurą określoną w *Zarządzeniu w sprawie ustalenia regulaminu korzystania z zasobów informatycznych Ministerstwa Środowiska*, podczas gdy dokument ten już w momencie modyfikacji nie obowiązywał, bo został zastąpiony *Zasadami korzystania z zasobów informatycznych MKiŚ*.

Celem regulacji wewnętrznych jest usystematyzowanie obowiązujących procesów i rozwiązań oraz wsparcie ich uczestników w realizacji określonych czynności. Dlatego dla skutecznej i efektywnej ich realizacji istotnym jest zapewnienie przejrzystych i spójnych przepisów określających te procesy.

3. [role i odpowiedzialność] PBI oraz zarządzenie w sprawie SZBI określały role i odpowiedzialność głównych osób zaangażowanych w BI. W Ministerstwie zostały wyznaczone osoby pełniące te role. Jednakże regulacje te wymagają uzupełnienia, bowiem w *Zasadach korzystania z zasobów informatycznych MKiŚ* określono rolę *Administratora Systemu Informacyjnego*, a w *Procedurze kontroli (zarządzania) dostępu do systemu BDO* funkcję *Administratora Systemu Informatycznego*, które nie zostały wskazane w PBI oraz zarządzeniu w sprawie SZBI. Ponadto PBI nie wyjaśnia pojęcia bezpieczeństwo teleinformatyczne / system teleinformatyczny przez co zakres zadań *Administratora Bezpieczeństwa Teleinformatycznego* może budzić wątpliwości.

W skład Zespołu ds. SZBI, który miał wspierać Dyrektora Generalnego w zarządzaniu BI wchodził: Pełnomocnik ds. BI, pełniący funkcję przewodniczącego Zespołu ds. SZBI, Z-ca Pełnomocnika ds. BI, Z-ca Przewodniczącego Zespołu ds. SZBI, Pełnomocnik ds. Ochrony Informacji Niejawnych, IOD wraz z zastępcami, ABT, ABF, Koordynator Zarządzania Ryzykiem BI oraz osoba wyznaczona przez dyrektora komórki właściwej ds. informacji o środowisku. Dyrektor Generalny wyznaczył osoby do pełnienia tych funkcji bądź powołał je w skład Zespołu ds. SZBI.

Wyjaśniono[29], że PBI nie uwzględniała roli *Administratora Systemów Informatycznych* z uwagi na techniczny aspekt wykonywanych czynności przez administratora, który jest tożsamy z rolami administratora aplikacji / systemów wdrożonych w Ministerstwie. Zadeklarowano, że rola taka zostanie wprowadzona w znowelizowanej PBI – administrator systemów informatycznych będzie rozumiany jako osoba, której Administrator Danych powierzył pełnienie obowiązków Administratora Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją (aktywami) funkcjonującą w systemach informatycznych.

Posługiwanie się pojęciami ról, dla których nie został określony zakres odpowiedzialności nie zapewnia rozliczalności działań podejmowanych w zakresie BI.

4. [wsparcie Kierownictwa w zarządzaniu BI] Wsparcie Dyrektora Generalnego w zarządzaniu BI przez Zespół ds. SZBI nie było dostateczne i skuteczne. Aktywność tego Zespołu była niewystarczająca, a przekazywane przez niego notatki nt. funkcjonowania SZBI nie były informacją zarządczą dającą podstawę do skutecznego zarządzania BI. W szczególności nie były to zbiorcze informacje, które są kluczowe w procesie zarządzania (tj. plan/strategia rozwoju i doskonalenia SZBI ze wskazaniem osób odpowiedzialnych za realizację poszczególnych działań wraz z planowanym terminem wdrożenia), a monitorowanie zaproponowanych działań do wdrożenia w danym roku nie było dokumentowane. Ponadto nie został zrealizowany całościowy przegląd SZBI – wykonano go

[29] Pismo z 13 lipca 2022 r., znak: DI-WRSI.081.14.2022.AS.

jedynie w oparciu o wybrane obszary. Kierownictwo MKiŚ nie posiadało zatem instrumentów zarządczych do podejmowania adekwatnych decyzji w zakresie systemu.

W okresie objętym kontrolą Zespół ds. SZBI przedstawił Dyrektorowi Generalnemu 2[30] notatki nt. funkcjonowania SZBI za okres od maja 2019 r. do grudnia 2020 r. oraz 2021 r. Zgodnie z § 4 ust. 6 zarządzenia w sprawie SZBI, Zespół powinien przedstawić raport dot. swojej działalności, nie zaś funkcjonowania SZBI. Ponadto raporty te powinny być przedstawiane także Ministrowi Klimatu i Środowiska, co nie było realizowane. Jak wyjaśniono[31], Dyrektor Generalny na spotkaniach kierownictwa przedstawiał informacje zawarte w tej notatce.

W badanym okresie odbyło się tylko jedno spotkanie Zespołu ds. SZBI w dniu 21 lipca 2021 r., dot. omówienia wyników audytu wewnętrznego[32]. Jak wskazano[33], inne zagadnienia były omawiane w innych trybach poza posiedzeniami Zespołu ds. SZBI, jednakże MKiŚ nie przedstawiło żadnej dokumentacji w tym zakresie. Poinformowano także, że nie jest możliwe, wskazanie przyczyn małej aktywności tego Zespołu, gdyż ówczesny Pełnomocnik ds. BI przesłał pracować w MKiŚ 19 marca 2022 r. i nie przekazał wiedzy w tym zakresie. Zapewniono, że pomimo tej sytuacji informacje związane z BI były przekazywane na cyklicznych spotkaniach kierownictwa z dyrektorami komórek oraz uzgadnianie na spotkaniach wewnątrzorganizacyjnych.

Przegląd SZBI ograniczył się do przedstawienia obszarów dot. analizy ryzyka, incydentów bezpieczeństwa, monitorowania 3[34] wskaźników oraz szkoleń, o czym informował Zespół ds. SZBI w notatkach nt. funkcjonowania systemu. Informacje te nie były rzetelne. Spowodowane było to m.in. brakiem regulacji, które określałyby zasady jego wykonywania oraz zakres i termin przekazywania informacji do Dyrektora Generalnego przez ten Zespół.

Podano[35], że normy ISO oraz ustawa o normalizacji[36] nie narzucają ustanowienia regulacji w tym przedmiocie. Niemniej zadeklarowano, że w zaktualizowanej PBI znajdą się postanowienia dot. przeglądów, jak również zmienione zostanie zarządzenie w sprawie SZBI w części zakresu i terminu sporządzania raportu przez Zespół. W notatce nt. funkcjonowania SZBI w 2021 r. przedstawiono nierzetelne informacje nt. liczby aktywów istotnych[37], wskaźnika zapoznania się z PBI przez nowych pracowników[38], liczby incydentów[39]. Ponadto wskazano *najistotniejsze zagrożenia,* wśród nich wymieniono wybrane ryzyka, a nie wskazano ryzyk z wyższym poziomem[40]. Wyjaśniono[41], że intencją było pokazanie przekrojowego zakresu ryzyk, tj. najczęściej występujących i tym samym z najwyższym poziomem ryzyka końcowego. W MKiŚ nie wdrożono wytycznych w tym zakresie.

W notatkach nt. funkcjonowania SZBI wskazywano propozycję działań na dany rok, w tym związanych z zapewnieniem infrastruktury teleinformatycznej. Jednakże Ministerstwo nie posiadało dokumentacji w zakresie monitorowania wdrożenia tych działań. Zamieszczono także *propozycje zmian techniczno-organizacyjnych,* jednakże żadna z nich nie została zrealizowana w 2021 r. i wszystkie przeniesiono do wykonania w 2022 r.

Wskazano[42], że zmiany dot. zapewnienia infrastruktury teleinformatycznej monitorowane są na bieżąco przez Pełnomocnika ds. BI. Dyrektor Generalny był informowany w trakcie spotkań bilateralnych, jak i spotkań dyrektorów komórek z kierownictwem o ryzykach związanych z zaplanowanymi działaniami. Poinformowano[43] także, że nie są znane powody, dla których ówczesny Pełnomocnik ds. BI monitorował jedynie zmiany dot. zapewnienia infrastruktury teleinformatycznej. Ministerstwo nie posiada dokumentów związanych z monitoringiem. Zadania te wykonywane były przez pracowników, którzy odeszli z pracy i omawiali te kwestie z ówczesnym Pełnomocnikiem ds. BI.

Propozycje zmian techniczno-organizacyjnych, które z 2021 r. przeniesiono do realizacji w 2022 r. dot. modyfikacji procedury szacowania ryzyka w zakresie aktywów podstawowych, aktywów wspierających oraz weryfikacji rodzajów skutków, aktualizacji postanowień *Metodyki*

[30] Z 25 sierpnia 2021 r. oraz 21 stycznia 2022 r.
[31] Pismo z 24 czerwca 2022 r., znak: DI-WRSI.081.4.2022.AS.
[32] Sprawozdanie z audytu wewnętrznego na temat *Ocena realizacji działań prowadzonych w zakresie bezpieczeństwa informacji.*
[33] Pismo z 13 lipca 2022 r., znak: DI-WRSI.081.14.2022.AS.
[34] Wskaźnik poziomu BI (monitorowany %, jako stosunek liczby przypadków przełamań zabezpieczeń do liczby zidentyfikowanych incydentów), wskaźnik liczby pracowników zapoznanych z PBI (monitorowany %, jako stosunek liczby pracowników zapoznanych z PBI do liczby nowych) oraz dostępność krytycznych systemów informatycznych.
[35] Pismo z 24 czerwca 2022 r., znak: DI-WRSI.081.4.2022.AS.
[36] Ustawa z dnia 8 września 2015 r. (Dz. U. z 2015 r., poz. 1483, t. j.).
[37] Wskazano, że zidentyfikowano 328 takich aktywów, podczas gdy *Zbiorczy wykaz aktywów krytycznych* [istotnych] *wykorzystywanych w procesach przetwarzania informacji w Ministerstwie za 2021 r.* zawiera 297 aktywów istotnych.
[38] Wskazano, że 28 osób nie dopełniło tego obowiązku podczas gdy nie zrealizowała go 1 osoba.
[39] Wskazano, że w 2021 r. 242 zdarzenia zakwalifikowano jako incydenty, podczas gdy było ich 317.
[40] M.in. dot. błędnej konfiguracji systemu backupu; ujawnienia danych poprzez pozostawienie wydruków w drukarce.
[41] Pismo z 20 lipca 2022 r., znak: DI.WRSI.081.15.2022.AS.
[42] Pismo z 24 czerwca 2022 r., znak: DI-WRSI.081.4.2022.AS.
[43] Pismo z 13 lipca 2022 r., znak: DI-WRSI.081.14.2022.AS.

zarządzania ryzykiem dla aktywów odnoszących się do środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych (dalej: *Metodyka zarządzania ryzykiem*), połączenia ról Koordynatorów zbiorów danych oraz szacowania ryzyka w jedną rolę Koordynatora bezpieczeństwa informacji w komórce, a także zawarcia umowy na udoskonalenie SZBI. Udzielono informacji[44], że propozycje te jako nadal aktualne przeniesiono do wykonania w 2022 r. z uwagi na realizowaną umowę dot. udoskonalenia SZBI.

SZBI wymaga diagnozy istniejących rozwiązań, identyfikacji jego słabości oraz opracowania planu/strategii, które przyczyniłyby się do skuteczniejszego zarządzania obszarem BI. Dokument taki umożliwiłby także hierarchizację / ustalenie priorytetów w zakresie działań do podjęcia. Ułatwiłoby to analizę i ocenę wdrażanych rozwiązań. Kierownictwo Ministerstwa posiadałoby również narzędzie zarządcze do podejmowania adekwatnych decyzji.

5. [porozumienie dot. BDO] Brak precyzyjnego określenia zadań i odpowiedzialności w zakresie administrowania oraz utrzymywania BDO stanowi istotną lukę w SZBI. W tym przedmiocie zawarte było Porozumienie[45] pomiędzy Ministerstwem a IOŚ, jednak nie określało ono szczegółowego podziału zadań, nie precyzowało zasad współpracy i obszarów, w których wymagane jest działanie obu stron Porozumienia.

Zawarte Porozumienie dot. w szczególności administrowania, utrzymywania BDO, realizacji Projektu w przedmiocie zaprojektowania, wytworzenia, wdrożenia modułów BDO dot. ewidencji oraz sprawozdawczości w zakresie gospodarki odpadami[46], a także integracji z funkcjonującym modułem Rejestr Podmiotów wraz z utrzymaniem zintegrowanego systemu.

W Porozumieniu w odniesieniu do administrowania systemem BDO zawarto jedynie ogólny podział zadań, w szczególności wskazano, że za utrzymanie BI przez zapewnienie właściwego poziomu poufności, integralności, dostępności oraz zbieranie, przechowywanie i zabezpieczenie przed utratą danych i informacji gromadzonych w BDO, odpowiedzialny jest:

- IOŚ w obszarze funkcjonowania wszystkich modułów aplikacji i oprogramowania BDO,
- Ministerstwo w obszarze funkcjonowania infrastruktury technicznej.

Załącznikiem do Porozumienia była m.in. PBI BDO, jednakże również ona nie określała precyzyjnego podziału zdań.

Przykładowo nie wskazywała kto jest odpowiedzialny za prowadzenie ewidencji aktywów systemu związanych z BI oraz środkami przetwarzania informacji, kto i w jakim zakresie odpowiada za analizę ryzyka (tj. nie wskazywała, że analiza ta jest realizowana przez MKiŚ w zakresie infrastruktury systemu, w uzgodnieniu z IOŚ w zakresie warstwy aplikacyjnej oraz we współpracy z Departamentem Gospodarki Odpadami (dalej: DGO) MKiŚ w zakresie przetwarzania informacji, w tym danych osobowych), kto i w jakim zakresie odpowiada za przegląd zarządzania BDO. MKiŚ nie posiadało także wyników przeglądu zarządzania[47] i nie mogło określić dlaczego odpowiedzialność za ewidencję aktywów i przegląd zarządzania nie została wskazana w PBI BDO.

Wyjaśniono[48], że w Porozumieniu został określony podział zadań. W dokumencie tym wskazano bowiem, że szczegółowy podział zadań ustalany będzie przez Komitet Sterujący oraz Kierownika Projektu.

Nie można zgodzić się wyjaśnieniami, że w Porozumieniu został określony precyzyjny podział zadań. Jak wskazano był on ogólny, zatem nie zapewniał efektywnego egzekwowania wykonanych zadań. Ponadto przedstawione wyjaśnienia, skupiają się na realizacji Projektu, a nie na administrowaniu i utrzymywaniu eksploatowanego systemu BDO, a to, w szczególności w tym zakresie ogólny podział zadań budzi zastrzeżenia.

6. [analiza ryzyka] Określenie dwóch odmiennych metodologii wykonywania analizy ryzyka w odrębnych regulacjach nie zapewniało przejrzystości procesu. W szczególności PBI nie wprowadziła podziału pomiędzy aktywami istotnymi i krytycznymi. Ponadto zarówno Polityka, jak i *Metodyka zarządzania ryzykiem* nie wprowadzały podziału pomiędzy aktywami

[44] Pismo z 24 czerwca 2022 r., znak: DI-WRSI.081.4.2022.AS.
[45] Porozumienie nr 1 z 7 grudnia 2018 r. wraz z 3 aneksami (nr 1 z 23 stycznia 2019 r., nr 2 z 29 sierpnia 2019 r., nr 3 z 3 grudnia 2020 r.).
[46] Na realizację projektu składało się 9 produktów: 1) Moduł Ewidencji Odpadów, Modułu Zarządzania Kontem, Moduł Integracyjny oraz Integracji z Rejestrem BDO, 2) Moduł Sprawozdawczości i Moduł Elektronicznych wniosków, 3) Moduł Sprawozdawczości JAP, 4) Moduł Raportowy, 5) Moduł Potwierdzeń, 6) Architektura rozwiązania, 7) Szkolenia, 8) Contact Center, 9) Disaster Recovery.
[47] Dysponowało tylko Raportem z audytu systemu BDO (14 października 2020 r.) oraz Raportem z oceny bezpieczeństwa aplikacji (19 listopada 2021 r.).
[48] Pismo z 3 sierpnia 2022 r., znak: DI-WRSI.081.22.2022.AS.

dot. środków przetwarzania informacji w zakresie komórek organizacyjnych, a aktywami odnoszącymi się do środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych i zakresu analizy ryzyka w odniesieniu do tych aktywów. Brak jasnego podziału w tym przedmiocie wprowadza wątpliwości, czy analiza ryzyka została przeprowadzona w pełnym zakresie w odniesieniu do wszystkich aktywów Jednostki.

W Ministerstwie sporządzane były 3 analizy ryzyka:

- wykonywana przez wszystkie komórki w stosunku do zidentyfikowanych aktywów. Metodologia jej sporządzania została określona w PBI, a aktywa o wartości wysokiej i ekstremalnej oraz aktywa, w ramach których przetwarza się dane osobowe, traktowane były jako aktywa istotne;
- realizowana w odniesieniu do aktywów odnoszących się środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych, wykonywana na podstawie *Metodyki zarządzania ryzykiem*. Wprowadzała ona zasady oceny ważności aktywów i wszystkie aktywa o wartości wysokiej należało traktować jako krytyczne;
- rejestr ryzyk w bezpieczeństwie informacji dla systemu BDO – stanowił on załącznik nr 6 do *Polityki Bezpieczeństwa Informacji Systemu BDO*. Szacowanie ryzyka prowadzono zgodnie z *Metodyką zarządzania ryzykiem. Rejestr ryzyk IT dla systemu BDO* sporządzono 1 lipca 2020 r.[49], a kolejny został opracowany dopiero 1 czerwca 2022 r.[50], podczas gdy zgodnie z *Metodyką zarządzania ryzykiem* identyfikację ryzyka prowadzi się okresowo nie rzadziej niż raz na rok.

Regulacje określające metodologię sporządzania analiz ryzyka nie były uporządkowane, w szczególności PBI, jako nadrzędy dokument w BI nie wprowadzała podziału pomiędzy aktywami istotnymi i krytycznymi. Wskazywała[51], że poziom BI jest odpowiedni m.in. gdy *określono aktywa krytyczne*, podczas gdy przepis ten należało interpretować[52] zarówno jako aktywa istotne, jak i aktywa krytyczne.

W odniesieniu do braku podziału pomiędzy aktywami dot. środków przetwarzania informacji podano[53], że PBI zawiera jedynie ogólny podział przedmiotowych aktywów z uwagi na umożliwienie kierownikom komórek zgłoszenia i oszacowania ryzyka dowolnych aktywów z tej grupy. Nie było precyzyjnego opisu podziału w tym zakresie, nie określono też szczegółowych wytycznych ani zasad w tym przedmiocie, oprócz ogólnego wskazania w dokumencie pn. *Opisy pomocnicze do arkusza Szacowania ryzyka* (dot. komórek organizacyjnych), że środki te to m.in. sprzęt komputerowy, podstawowe systemy informatyczne (EZD, Zimbra, Quorum), dysk sieciowy. ABT szacuje ryzyko tych samych aktywów, *pod kątem technicznego utrzymania dostępności środków przetwarzania informacji wykorzystywanych do zapewniania usług teleinformatycznych*. Poinformowano także, że w ramach umowy na udoskonalenie SZBI podział ten zostanie uszczegółowiony.

Brak tego podziału rodzi wątpliwości kto odpowiada za identyfikację ryzyk dot. informacji przetwarzanych na tabletach, telefonach komórkowych, laptopach. Jak poinformowano[54], są one wskazywane jedynie przez kierowników komórek, w których aktywa te są wykorzystywane.

Odnosząc się do tych wyjaśnień wskazać należy, że dokument pn. *Opisy pomocnicze do arkusza Szacowania ryzyka,* wskazywał w stosunku do wymienionych urządzeń tylko jedno zagrożenie związane z utratą poufności danych na skutek kradzieży laptopa, tabletu lub telefonu, a przetwarzanie informacji na urządzeniach mobilnych rodzi szereg ryzyk. W arkuszu szacowania ryzyka za 2020 r. i 2021 r. również odniesiono się tylko do tego ryzyka, co wskazuje na niepełną analizę ryzyka w tym zakresie.

7. Wdrożone metodologie sporządzania analizy ryzyka budzą zastrzeżenia w zakresie przyjętych założeń, które podważają prawidłowość i rzetelność czynności zrealizowanych w procesie szacowania ryzyka.

[49] Data podpisu dokumentu przez ówczesnego Pełnomocnika ds. BI.
[50] Data podpisu dokumentu przez IOD, tj. ostatnią osobę podpisującą dokument przed zatwierdzeniem go przez Dyrektor Generalną (1 czerwca 2022 r.).
[51] § 6 ust. 1 pkt 1 PBI.
[52] Wyjaśnienia z 23 czerwca 2022 r. (brak znaku pisma).
[53] Pismo z 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.
[54] Pismo z 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.

Zgodnie z PBI *Plan postępowania z ryzykiem* jest przygotowywany wyłącznie w stosunku do nieakceptowalnego ryzyka[55]. Przy czym ryzyko nieakceptowalne, występuje gdy:

- jeden ze skutków oceniony został na poziomie 4 albo 5, a prawdopodobieństwo wystąpienia zagrożenia na poziomie 5 (pewne);
- poziom ryzyka końcowego przekroczy wartość 71.

Żadne ze zidentyfikowanych ryzyk nie spełniało tych warunków, tym samym nie było konieczności sporządzania takiego dokumentu. Udzielono informacji[56], że norma PN-ISO/IEC 27001 stanowi *tzw. miękkie prawo* określając zbiór wytycznych do stosowania w organizacji. Ówczesny Pełnomocnik ds. BI *bazując na normach ISO, podjął decyzję o przygotowaniu zapisów obowiązujących do dnia dzisiejszego*.

Wskazać należy, że plan postępowania z ryzykiem jest podstawowym dokumentem wykonawczym do podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy. Niezasadne było ustalenie progu ryzyka nieakceptowalnego na tak wysokim poziomie prawdopodobieństwa (5-pewne) bez uwzględnienia innych istotnych poziomów, tj. 3-prawdopodobny i 4-bardzo prawdopodobny. Ponadto poziom ryzyka nieakceptowalnego, po którym należy opracować powyższy plan nie powinien dotyczyć ryzyka końcowego, a ryzyka początkowego. Bowiem to po ocenie ryzyka początkowego, dla którego wielkość jest nieakceptowalna należy określić sposób postępowania z ryzykiem.

PBI nie uwzględnia konieczności oceny prawdopodobieństwa wystąpienia zagrożenia po zastosowaniu zabezpieczeń, tj. poziom ryzyka nie był ponownie oceniany jako iloczyn skutku ryzyka i prawdopodobieństwa, a stanowił on iloraz poziomu ryzyka początkowego do skuteczności zabezpieczeń. Wskazano[57], że prawdopodobieństwo wystąpienia zagrożenia jest uwzględniane tylko do wyliczenia poziomu ryzyka początkowego, na podstawie którego wyliczana jest wartość ryzyka końcowego.

Ocena skuteczności zabezpieczeń powinna sprawdzać, jak zabezpieczenia te redukują prawdopodobieństwo zagrożenia i łatwość wykorzystania podatności lub skutek incydentu.

Zgodnie z PBI ryzyko było oceniane z uwzględnieniem 8 skutków, przy czym w przypadku oceny ryzyk nieakceptowalnych spośród nich wyłączono ryzyka o 3[58] skutkach. W Polityce nie wskazano powodów takiego wyłączenia. Podano[59], że skutki te w mniejszym stopniu mogą generować sytuacje, w których są one ocenione na poziomie 4 lub 5. Poinformowano również, że w ramach umowy na doskonalenie SZBI planowane są zmiany w tym zakresie.

Działania związane z zarządzaniem ryzykiem w szczególności skupiają się na ryzykach nieakceptowalnych. MKiŚ w metodologii sporządzania analizy ryzyka powinno uzasadnić z jakich powodów ryzyka o danych skutkach nie są traktowane jako ryzyko nieakceptowalne.

W arkuszach szacowania ryzyka za 2020 r. oraz 2021 r. w odniesieniu do większości ryzyk wymieniono te same zastosowane zabezpieczenia, np. wskazano zabezpieczenia organizacyjne w postaci regulacji SZBI, zamiast przywołać konkretne zabezpieczenia z nich wynikające. Wskazano[60], że dla utrzymania spójności szacowania ryzyka we wszystkich komórkach, wydano rekomendacje, aby dla poszczególnych aktywów zastosować obligatoryjne zakresy zabezpieczeń organizacyjnych, informatycznych, technicznych i fizycznych wynikających z PBI. W trakcie przekazywania rekomendacji wskazano informacje o konieczności wykazywania innych zastosowanych zabezpieczeń, o ile są stosowane w przypadku aktywa poddawanego szacowaniu ryzyka.

Celem procesu zarządzania ryzkiem jest m.in. określenie sposobu postępowania z ryzykiem, w tym wskazanie stosowanych zabezpieczeń. Z dokumentacji powinno wynikać, jakie zabezpieczenia stosuje Jednostka by minimalizować poziom ryzyka. PBI nie jest *stricte* zabezpieczeniem, zawiera ona natomiast informacje nt. stosowanych zabezpieczeń i to one powinny być wskazane.

---

[55] § 16 ust. 14 PBI.
[56] Pismo z 23 czerwca 2022 r. (brak znaku pisma).
[57] Pismo z 23 czerwca 2022 r. (brak znaku pisma).
[58] Skutki: reputacyjne związane z możliwą utratą wizerunku w oczach pracowników lub obywateli; organizacyjne związane z możliwymi zakłóceniami w funkcjonowaniu pojedynczej, kilku lub większości komórek albo możliwym wpływem na podejmowanie decyzji przez Ministra KiŚ; związane z utratą zaufania obywateli do władzy publicznej.
[59] Pisma z 23 czerwca (brak znaku pisma) oraz 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.
[60] Pismo z 23 czerwca 2022 r. (brak znaku pisma).

W *Metodyce zarządzania ryzykiem* w pkt. *2.3.3 Określanie poziomu ryzyka* przewidziano wartość prawdopodobieństwa na poziomie 0*,* która oznacza *zdarzenie nieprawdopodobne (zagrożenie nie występuje).* Wskazać należy, że skoro ryzyko nie występuje nie ma potrzeby uwzględniania go w analizie ryzyka.

Jak poinformowano[61] wartość 0 została wyszczególniona w celu możliwości wykazania również tych zagrożeń, dla których prawdopodobieństwo zdarzenia zostało w trakcie analizy określone jako *wysoce nieprawdopodobne*.

Nie można zgodzić się z wyjaśnieniami, ponieważ w *Metodyce zarządzania ryzykiem* wprost wskazano, że prawdopodobieństwo 0 oznacza *zdarzenie nieprawdopodobne (zagrożenie nie występuje),* a nie zdarzenie wysoce nieprawdopodobne. Ponadto uwzględnienie wyjaśnień Kontrolowanego powodowałoby trudności w rozdzieleniu zdarzeń z prawdopodobieństwem 0 oraz 1, gdyż wartość 0 należałoby przypisywać zdarzeniom wysoce nieprawdopodobnym, a 1 – zdarzeniom prawie nieprawdopodobnym, co w zasadzie oznaczałoby tą samą kategorię.

8. Dokumenty dotyczące analizy ryzyka nie były rzetelnie i terminowo przygotowane. Ponadto rejestr ryzyk dot. aktywów odnoszących się do środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych za 2021 r. (dalej: rejestr ryzyk IT) nie został przekazany do akceptacji do Dyrektora Generalnego, co stanowiło naruszenie pkt 4 ppkt 2 *Metodyki zarządzania ryzykiem.*

Wyjaśniono[62], że *Rejestr ryzyk IT za 2021 r.* nie został przedłożony do akceptacji Dyrektora Generalnego i należy go traktować jako wkład do notatki służbowej nt. funkcjonowania SZBI w 2021 r. Natomiast *Rejestr ryzyk IT za 2020 r.* został przekazany 25 sierpnia 2021 r., podczas gdy zgodnie z *Metodyką zarządzania ryzykiem* powinien być przedłożony do 31 stycznia 2021 r., przekazano go zatem blisko 7 miesięcy po terminie. Poinformowano, że ówczesny Pełnomocnik ds. BI odpowiedzialny za ten proces nie jest już pracownikiem MKiŚ i powody przekazania dokumentu po terminie nie są możliwe do ustalenia.

W odniesieniu do dokumentów dot. analizy ryzyka stwierdzono, że:

- *Zbiorczy wykaz aktywów krytycznych* [istotnych] *wykorzystywanych w procesach przetwarzania informacji w Ministerstwie za 2021 r.* nie określał ważności jednego aktywa, a w odniesieniu do kolejnych pięciu wskazano, że są to aktywa krytyczne, podczas gdy PBI nie przewidywała takiej wartości i były to aktywa o wartości wysokiej. Wskazano[63], że sformułowanie *aktywo krytyczne* zapewne zostało zamieszczone omyłkowo;
- W arkuszu dot. szacowania ryzyka w 2021 r. nie uwzględniono aktywa Biura Kontroli i Audytu pn. *Regulamin/Procedura w sprawie zgłaszania nieprawidłowości w MKiŚ*, co jak poinformowano[64], wynikało prawdopodobnie z błędu przy przenoszeniu informacji do zbiorczego zestawienia;
- *Rejestr ryzyk IT za 2021 r. oraz za 2020 r.* nie obejmował 13[65] aktywów. W odniesieniu do 10 z nich wyjaśniono[66], że powinny być one przypisane do arkusza *Systemy Aplikacyjne*. Powodu nieścisłości nie można było ustalić, ponieważ osoba szacująca ryzyka IT, tj. ówczesny ABT nie pracuje w MKiŚ. Natomiast w stosunku do kolejnych 3 poinformowano, że powinny być one przypisane do arkusza *Systemy zarządzania*.

Analiza ryzyka BI jest jednym z najistotniejszych elementów SZBI. Pozwala na proaktywne zarządzanie BI, w tym przeciwdziałanie zagrożeniom oraz ograniczanie skutków w przypadku zmaterializowania się ryzyk. Z tego powodu proces ten powinien być przejrzysty, a stosowanie zabezpieczeń powinno wynikać z rzetelnej analizy.

9. **[plan ciągłości działania]** W MKiŚ nie wdrożono całościowego planu ciągłości działania. Opracowano dokument *pn.: Plan ciągłości działania systemów informatycznych w Ministerstwie Środowiska* (dalej: Plan)*,* który, podobnie jak inne procedury, nie został zaktualizowany. Ponadto na skutek odejścia z pracy m.in. Pełnomocnika ds. BI, Ministerstwo nie było w stanie potwierdzić, czy Plan był testowany w badanym okresie.

[61] Pismo z 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.
[62] Pismo z 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.
[63] Pismo z 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.
[64] Pismo z 23 czerwca 2022 r. (brak znaku sprawy).
[65] Poz. 3, 4, 7, 10, 11, 37, 59, 67, 68, 75, 79, 84, 89 wykazu *Systemów IT.*
[66] Pismo z 20 lipca 2022 r., znak: DI-WRSI.081.15.2022.AS.

Załączniki do Planu stanowiły: wykaz aktywów odnoszących się środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych, *Rejestr ryzyk IT*, *Procedura zarządzania incydentem bezpieczeństwa teleinformatycznego*, *Procedura awaryjna*, *Protokół z testu ciągłości działania*. Dokumenty te nie są jednak pełnym planem ciągłości działania. Celem wdrożonego Planu było *minimalizowanie zakłóceń w realizacji działalności zadań Ministerstwa Środowiska w związku z uszkodzeniem systemu informatycznego*, podczas gdy plan ciągłości działania to plan wznawiania działania jednostki w obszarze kluczowych procesów w przypadku wystąpienia katastrofy[67]. Dlatego niezbędne jest wskazanie kluczowych procesów MKiŚ, tj. dokonanie analizy jaki wpływ na działalność miałoby ewentualne poważne zakłócenie lub przerwanie tych procesów wraz z dokonaniem analizy ryzyka w zakresie zagrożeń dla tych procesów. Następnie na ich podstawie opracowanie planu ciągłości działania określającego w jaki sposób Ministerstwo będzie zarządzać destrukcyjnymi zdarzeniami i wznawiać działanie.

W ocenie[68] MKiŚ przekazany Plan określa postępowanie w przypadku zaistnienia zdarzeń mających wpływ na bezpieczeństwo informacji oraz ciągłość działania. Wyjaśniono, że powołano personel reagujący na incydenty z niezbędnym zakresem obowiązków, uprawnień oraz kompetencji, a ponadto opracowano i zatwierdzono plany i procedury reagowania i odtwarzania. Dodano, że do planów ciągłości działania należy także zaliczyć procedury pn.: *Baza konfiguracji CMDB* oraz *Procedura włączania i wyłączania systemów Informatycznych*.

Nie można zgodzić się z wyjaśnieniami, bowiem Plan dotyczy uszkodzeń systemów informatycznych, a nie wznawiania działania w kluczowych procesach. Słabości działań i regulacji w zakresie kopii zapasowych, które są istotnym elementem zapewniającym ciągłość działania przedstawiono w *Wystąpieniu* w pkt. 27-28, a *Bazy konfiguracji CMDB* – w pkt. 12-13 *Wystąpienia*. *Procedura włączania i wyłączania systemów Informatycznych*, także była nieaktualna. Dodatkowo została wprowadzona przed wdrożeniem systemu BDO, zatem go nie obejmowała. W odniesieniu do PDWD wskazywała na nieaktualną maszynę wirtualną, a w zakresie EZD PUW nie uwzględniała maszyny sql1.mos.gov.pl.

10. [audyt] W Ministerstwie wdrożono regulacje[69] określające konieczność realizacji corocznego audytu BI. Zrealizowano 2 audyty, tj. audyt systemu BDO oraz wybranych obszarów SZBI. Jednak ze względu na przedłużający się termin zawarcia umowy na doskonalenie SZBI, w ramach której planowano kolejny audyt w 2022 r., obowiązek jego wykonania przynajmniej raz w roku został naruszony. Ponadto audyty te nie objęły badaniem wszystkich obszarów BI, co dodatkowo przy braku przeglądów SZBI, nie zapewniło pełnej identyfikacji słabości systemu i nie wspierało Jednostki w ich eliminacji.

W badanym okresie przeprowadzono 2 audyty, tj. w 2020 r. audyt *Bazy danych o produktach i opakowaniach oraz gospodarce odpadami* (dalej: audyt systemu BDO)[70] i audyt pn. *Ocena realizacji działań prowadzonych w zakresie bezpieczeństwa informacji* (dalej: audyt BI)[71] realizowany na przełomie 2020 i 2021 r. Po ich wykonaniu kolejne zadanie audytowe zaplanowano w ramach umowy na udoskonalenie SZBI (umowa zawarta 24 czerwca 2022 r.).

Oba te audyty nie objęły swym zakresem wszystkich obszarów SZBI, w szczególności nie dot. one obszarów zarządzania ryzykiem[72], kompleksowego przeglądu SZBI, szkoleń, umów serwisu i rozwoju infrastruktury oraz systemów informatycznych, inwentaryzacji sprzętu i oprogramowania informatycznego[73], projektowania i wdrażania systemów teleinformatycznych, rozliczalności oraz zabezpieczeń organizacyjno-technicznych dostępu do informacji i systemów. Ponadto zagadnienia dot. zarządzania incydentami, zmianą w systemie, tworzenia kopii zapasowych, opracowania planu ciągłości działania oceniono jedynie w odniesieniu do dokumentacji BDO.

Wyjaśniono[74], że w zakresie audytu systemu BDO oceniono cały obszar funkcjonowania PBI BDO. Natomiast w wyniku realizacji audytu BI nie było możliwości objęcia jego zakresem

[67] Dot. zdarzeń o niskim prawdopodobieństwie wystąpienia, ale o katastrofalnych skutkach, np.: pożar, powódź, skażenie chemiczne, sabotaż, terroryzm itp., których czasu wystąpienia nie można przewidzieć.
[68] Pismo z 21 lipca 2022 r., znak: DI-WRSI.080.2.2022.AS.
[69] § 5 zarządzenia w sprawie SZBI oraz § 9 pkt 10 PBI.
[70] Raport z audytu systemu BDO z 14 października 2020 r.
[71] Termin przeprowadzania zadania 10 grudnia 2020 r. – 31 marca 2021 r.
[72] Audyt pn. *Ocena realizacji działań prowadzonych w zakresie bezpieczeństwa informacji* zawierał jedynie informacje nt. szacowania ryzyka do zadań Zespołu ds. SZBI.
[73] Audyt pn. *Ocena realizacji działań prowadzonych w zakresie bezpieczeństwa informacji* zawierał informacje w tym zakresie, jednakże jego oceny dot. działań podejmowanych na podstawie zarządzenie nr 60 Ministra Środowiska z dnia 22 października 2012 r. *w sprawie Instrukcji inwentaryzacyjnej Ministerstwa Środowiska* (Dz. Urz. MŚ z 2012 r., poz. 61), podczas gdy rejestr zasobów informatycznych nie jest tożsamy z zapisami księgi inwentarzowej dla potrzeb rachunkowości.
[74] Pismo z 24 czerwca 2022 r., znak: BKA-RI.081.5.2022.BW.

wszystkich obszarów SZBI z uwagi na trwającą w latach 2020-2021 reorganizację Ministerstwa oraz pandemię.

Realizacja audytów w niepełnym zakresie, przy braku przeglądów SZBI nie zapewnia pełnej oceny funkcjonowania systemu, w tym nie pozwala na skuteczną identyfikację potencjalnych słabości lub zagrożeń BI.

11. Zastrzeżenia budzi zwłoka w realizacji większości rekomendacji obu audytów wewnętrznych, przez co system nie był efektywnie doskonalony. Prawidłowo monitorowano stopień wykonania rekomendacji audytu BI, natomiast w zakresie audytu systemu BDO zadeklarowano jego prowadzenie, choć nie przedstawiono stosownej dokumentacji.

W wyniku realizacji audytu systemu BDO przedstawiono 7[75] rekomendacji, z których żadna nie została wdrożona i wszystkie znajdowały się w fazie realizacji. Wyjaśniono, że w 2020 r. Ministerstwo przeszło wielokrotną reorganizację, która wymuszała kompleksową aktualizację całego SZBI, co było zaplanowane w ramach umowy na udoskonalenie SZBI. Natomiast w przypadku audytu BI z 8 zaleceń 4[76] zostały wdrożone, 1[77] zrealizowano częściowo, a 3[78] nie zostały wykonane. Również w tym przypadku realizację zaleceń niewykonanych planowano w ramach powyższej umowy.

Realizacja audytów, bez podejmowania działań naprawczych, nie przyniesie wartości dodanej. To działania naprawcze usprawniają system. Dlatego MKiŚ powinno podejmować skuteczne czynności dot. wdrożenia ich rekomendacji.

12. [baza CMDB] Ministerstwo nie posiadało relacyjnej bazy konfiguracji CMDB zawierającej informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku, tym samym nie spełniono wymogów określonych w § 20 ust. 2 pkt 2 Rozporządzenia KRI.

MKiŚ prowadziło bazę konfiguracji CMDB przy użyciu programu OTRS, jednakże nie była to baza relacyjna. Obejmowała ona wykaz sprzętu i oprogramowania, ale nie zawierała informacji w zakresie środków komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. W odniesieniu do komputerów / laptopów wprowadzane były jedynie informacje dot. nazwy sprzętu, modelu, numeru seryjnego, numeru inwentarzowego oraz daty wygaśnięcia gwarancji. W niektórych przypadkach dodatkowo odnotowywano właściciela, system operacyjny, procesor, pamięć RAM, dysk twardy.

Ponadto baza ta nie podlegała aktualizacji. Zawierała ona częściowo informacje nt. niewykorzystywanego sprzętu i nieaktualnego użytkownika (jeśli został on wskazany), a nie obejmowała, np. telefonów komórkowych i tabletów.

Wyjaśniono[79], że wpływ na to miały zmiany organizacyjne oraz przejście (na okres 1,5 roku) na całkowity tryb pracy zdalnej. Spowodowało to konieczność zmiany priorytetów kierownictwa i skierowanie zasobów do utrzymania ciągłości działania, zapewnienia pracownikom sprzętu komputerowego, udostępnienia zasobów do rozpoczęcia pracy zdalnej. Służbom informatycznym zabrakło pracowników, jak i czasu, do aktualizacji bazy. Jak słusznie zauważono, przy dużej rotacji sprzętu i zmianach konfiguracji, problem stanowił brak automatyzacji w jej prowadzeniu, gdyż wszystkie informacje wprowadzane były do niej ręcznie.

---

[75] 7 rekomendacji wymagało podjęcia działań. W przypadku obszaru dot. zarządzania zmianą i dokumentacją oraz segmentacji nie wydawano dodatkowych zaleceń, rekomendowano utrzymanie dotychczasowych praktyk.

[76] **Zalecenie 5** dot. przekazywania na bieżąco informacji kadrowych o pracownikach z którymi rozwiązano umowę o pracę oraz przebywającymi na urlopach bezpłatnych oraz uregulowania kwestii odbierania uprawnień pracownikom długotrwale nieobecnym, będących na urlopach rodzicielskich/wychowawczych.
Zalecenie 7 dot. akceptacji przez przełożonego pracownika oraz Dyrektora BDG (aktualnie Dyrektora DI) formularzy bezpiecznego dostępu z sieci zew. do zasobów MKiŚ.
Zalecenie 6 dot. świadczenia pracy zdalnej na sprzęcie służbowym. Jednocześnie zapewniając sprzęt służbowy nie było konieczności realizacji **zalecenie 8**, tj. monitorowania sprzętu prywatnego wykorzystywanego do realizacji zadań służbowych pod kątem aktualizacji przez użytkowników programu antywirusowego.

[77] **Zalecenie 2** dot. uregulowania w wew. przepisach kwestii dot.: 1) odbioru uprawnień pracownikom przebywających na urlopach rodzicielskich/wychowawczych, 2) obowiązku rozliczenia się ze sprzętu w przypadkach urlopów bezpłatnych, urlopów rodzicielskich/wychowawczych, 3) określenia zawartości raportu z działalności Zespołu ds. SZBI oraz terminu jego przekazywania właściwym adresatom. Zalecenie to zostało zrealizowane w odniesieniu do pkt. 1. Pozostałe pkt. 2 i 3 nie zostały wykonane.

[78] **Zalecenie 1** dot. zaktualizowania PBI w części przeprowadzenia audytu BI przez niezależną jednostkę zewnętrzną, wyłonioną zgodnie z wewnętrznymi procedurami w zakresie zawierania umów, z określeniem częstotliwości przeprowadzania takiego audytu.
Zalecenie 3 dot. przeprowadzenia szkolenia w zakresie inwentaryzacji aktywów oraz na bieżąco monitorowania przekazywania wnioskowanych informacji.
Zalecenie 4 dot. przeglądu istniejących w MKiŚ procedur i instrukcji o tej samej tematyce, a następnie zaktualizowania ich, ujednolicenia w zakresie nazewnictwa, akceptacji, określenia ról w procesie i wskazania ich w jednym dokumencie, tak by dostęp do nich i ich treść nie stwarzał dla odbiorcy problemów.

[79] Pismo z 5 lipca 2022 r., znak: DI-WRSI.081.10.2022.AS.

13. Wdrożona procedura *Baza konfiguracji CMDB* była nieaktualna i nie przestrzegano jej postanowień.

> Procedura wskazywała na obowiązek prowadzenia relacyjnej bazy konfiguracji CMDB. Z powodu braku jej aktualizacji określała obowiązek zamieszczania w bazie sprzętu, który nie był już wykorzystywany (palmtopy, pagery, terminale BlackBerry, nawigacje GPS, faxy, xero, karty rozszerzeń), i nie uwzględniała konieczności gromadzenia informacji nt. tabletów i modemów. Określała potrzebę ewidencji pendrive, klawiatury, myszki, stacji dokujących, które, jak wyjaśniono[80], nie były jednostkowo wprowadzane do bazy, ze względu na niską wartość tego sprzętu. Wprowadzała konieczność gromadzenia danych nt. niszczarek, które nie kwalifikują się jako sprzęt komputerowy. Poinformowano, że procedura ta nie podlegała aktualizacji i nie była przestrzegana z powodu zmian organizacyjnych. Dodano, że służby informatyczne zostały uszczuplone o 7 pracowników. Niemniej w niedługim czasie zostaną wzmocnione o 2 osoby, co stworzy możliwość sprawnej realizacji tej procedury.

MKiŚ w pierwszej kolejności powinno dokonać aktualizacji procedury, w tym przeprowadzić analizę zakresu danych jakie będą w niej przetwarzane nt. sprzętu i oprogramowania. Baza konfiguracji CMDB powinna m.in. umożliwić odtworzenie infrastruktury teleinformatycznej po katastrofie lub innym zdarzeniu losowym, jak również dostarczać niezbędnych informacji przy wprowadzaniu wszelkich zmian w środowisku teleinformatycznym.

14. **[uprawnienia]** W Ministerstwie nie wdrożono całościowych regulacji wspierających proces nadawania i odbierania uprawnień w odniesieniu do systemów PDWD oraz BDO. Nie określono zasad nadawania, zmiany i odbierania uprawnień dla pracowników w systemie BDO oraz dla administratorów do zarządzania kontami użytkowników w systemie PDWD. W procedurze, odnoszącej się do systemu EZD PUW, obszar ten uregulowano, choć wymagała ona aktualizacji. Zasadne byłoby również określenie w niej, że zakres uprawnień przypisany do danej grupy zdefiniowanej jest w systemie oraz wskazanie kto odpowiada za modyfikację i aktualizację uprawnień w danej grupie, w szczególności po wprowadzeniu nowych funkcjonalności. Procedura ta nie zawierała zasad współpracy w zakresie obsługi *Jednolitego wniosku o usługi IT* (dalej: *jednolity wniosek*) pomiędzy Wydziałem Eksploatacji Systemów Informatycznych (dalej: WESI) DI a Wydziałem Organizacji i Archiwum (dalej: WOA) BDG.

> Zasady otwierania, modyfikowania oraz zamykania kont w EZD PUW uregulowano w *Procedurze otwierania, modyfikowania oraz zamykania kont w systemach informatycznych MKiŚ*[81] (dalej: *Procedura otwierania kont*), która jednocześnie dot. utworzenia konta w Active Directory. Zawarto w niej odwołanie do niewykorzystywanego już *Formularza użytkownika systemów informatycznych MŚ*, podczas gdy podstawą tworzenia konta w EZD PUW i Active Directory był *jednolity wniosek*. Podpisywany był on przez dyrektora właściwej komórki i przekazywany za pośrednictwem EZD PUW do DI. Do poszczególnej roli organizacyjnej (np. pracownik, naczelnik, sekretariat) przypisana została w systemie dana grupa uprawnień.
>
> Udzielono informacji[82], że uprawnienia w EZD PUW są nadawane poprzez przypisanie użytkownika do grupy lub kilku grup uprawnień, które podlegają zmianom kilka lub kilkanaście razy w roku m.in. ze względu na nowe funkcjonalności systemu i związane z tym nowe uprawnienia. *Procedura otwierania kont* nie określała jednak, że zakres uprawnień przypisany do danej grupy zdefiniowany jest w systemie i nie wskazywała kto odpowiada za modyfikację i aktualizację uprawnień w danej grupie, w szczególności po wprowadzeniu nowych funkcjonalności. Jednocześnie nie określała, że każde odstępstwo dot. zwiększenia / zmniejszenia zakresu uprawnień wymaga wskazania w *jednolitym wniosku*.
>
> Zasady nadawania uprawnień do systemu PDWD dla jednostek administracji (w tym 4 komórek MKiŚ[83]) zobowiązanych do prowadzenia publicznie dostępnych wykazów danych określono w *Procedurze tworzenia, modyfikacji i zamykania kont użytkowników autoryzowanych Publicznie dostępnego wykazu danych (PDWD)*[84] (dalej: *Procedura PDWD*), a reguły odzyskiwania hasła do konta w *Procedurze odzyskiwania danych logowania i akceptacji żądań*

[80] Pismo z 5 lipca 2022 r., znak: DI-WRSI.081.10.2022.AS.
[81] Zatwierdzona 27 stycznia 2022 r.
[82] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[83] Departament Ochrony Przyrody, Departament Geologii i Koncesji Geologicznych, Departament Ropy i Paliw Transportowych, Departament Instrumentów Środowiskowych.
[84] Zatwierdzona 5 września 2017 r.

certyfikacyjnych w Wykazie[85]. Jednak w regulacjach tych nie przedstawiono postanowień nadawania i odbierania uprawnień administratorom do zarządzania kontami użytkowników.

Poinformowano[86], że określone zostało to w opisach stanowisk pracy administratorów. Zauważyć należy, że opis stanowiska pracy wskazuje na zadania realizowane przez pracownika, a nie stanowi zasad postępowania w przedmiocie nadania uprawnień.

W stosunku do systemu BDO wdrożono *Procedurę kontroli (zarządzania) dostępu do systemu BDO*[87] (dalej: *Procedura dostępu do BDO*), jednak nie zawierała ona postanowień dot. nadawania, zmiany i odbierania uprawnień dla pracowników MKiŚ. Natomiast *Procedura kontroli dostępu dla użytkowników uprzywilejowanych systemu BDO*, określała jedynie warunki dostępu do serwerów dla administratorów, a dodatkowo nie została podpisana przez Pełnomocnika ds. BI.

W opinii MKiŚ[88] wdrożenie procedury w tym zakresie nie jest niezbędne, ponieważ uprawnienie do nadawania uprawnień przez naczelników i kierowników zespołów wynika z posiadanych przez nich upoważnień. Ponadto prowadzone są prace nad modułem Zarządzania Kontem w BDO. Wskazać należy, że wydanie upoważnienia nie jest argumentem do braku wdrożenia procedur. To procedury określają zasady postępowania, a w dalszej kolejności na ich podstawie powinno zostać wydane upoważnienie oraz powinny być realizowane czynności dot. nadania uprawnień.

Istotnym elementem polityki BI jest właściwe zarządzanie dostępem do systemów teleinformatycznych. Dlatego proces ten powinien być całościowo uregulowany i w szczególności zapewniać, że osoby przetwarzające informacje posiadają uprawnienia w stopniu adekwatnym do realizowanych obowiązków.

15. W PDWD i EZD PUW uprawnienia nadawano prawidłowo, zgodnie z kompetencjami użytkowników. Funkcjonalności tych systemów pozwalały na nadanie różnego ich zakresu, a zasada ograniczenia uprawnień do niezbędnego minimum potrzebnego do realizacji zadań była stosowana. Jednak w przypadku systemu EZD PUW istotne zastrzeżenia budzi fakt wystąpienia sporadycznych sytuacji, w których nadawane były uprawnienia, mimo że pracownik nie posiadał upoważnienia do przetwarzania danych osobowych.

Zmiany wymaga funkcjonalność systemu BDO pozwalająca pracownikowi posiadającemu do niego dostęp, jako użytkownik główny, na tworzenie kont dla innych użytkowników (m.in. z tym samym zakresem uprawnień), mimo braku stosownego upoważnienia wydanego przez Dyrektora DGO. Ponadto w przypadku tego systemu naruszono zasadę bezzwłocznego odebrania uprawnień, o której mowa § 20 ust. 2 pkt 5 Rozporządzenia KRI, tj. w toku kontroli konta w systemie posiadały 3 osoby, które nie były już pracownikami Ministerstwa.

Obsługą *jednolitego wniosku* w zakresie utworzenia konta w Active Directory zajmowali się pracownicy WESI DI, zaś nadaniem uprawnień w systemie EZD PUW pracownicy WOA BDG, którym *jednolity wniosek* był udostępniany przez DI. Modyfikowanie i odebranie/cofnięcie uprawnień oraz zamknięcie konta w Active Directory oraz EZD PUW następowało na podstawie przekazanej w EZD PUW informacji z Wydziału Kadr Biura Zarządzania Kapitałem Ludzkim (tzw. informacja kadrowa). Zamknięcie konta powinno następować z dniem zakończenia pracy.

Zgodnie z *Procedurą otwierania kont* warunkiem nadania uprawnień w EZD PUW było uzyskanie przez użytkownika upoważnienia do przetwarzania danych osobowych wydanego przez IOD. Występowały jednak sytuacje[89], w których pracownikowi nadawane były uprawnienia w EZD PUW, pomimo braku posiadania przez niego takiego upoważnienia.

Wskazano[90], że ówczesne kierownictwo BDG nie zdecydowało się na wdrożenie automatycznej weryfikacji informacji o wydanym upoważnieniu, ponieważ opóźniłoby to znacznie możliwość rozpoczęcia pracy nowym pracownikom w tym systemie. Wyeliminowano również praktykę wydawania powyższych upoważnień przez IOD. 21 czerwca 2022 r. Administrator Danych upoważnił Zastępcę Dyrektora BDG do realizacji czynności w tym przedmiocie. Poinformowano, że obecnie komórki dokonują przeglądu wydanych upoważnień i są przygotowywane wnioski o wydanie nowych.

[85] Zatwierdzona 30 sierpnia 2017 r.
[86] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[87] Zatwierdzona 31 grudnia 2021 r.
[88] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[89] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 6 lipca 2022 r.
[90] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.

Pracownik powinien posiadać upoważnienie do przetwarzania danych osobowych z dniem zatrudnienia, a obowiązek założenia konta w EZD PUW pod warunkiem jego wydania powinien być bezwzględnie przestrzegany. W przeciwnym wypadku może dojść do sytuacji przetwarzania danych osobowych bez stosownego upoważnienia.

Nadawanie i odbieranie uprawnień administratorom do zarządzania kontami użytkowników w systemie PDWD realizowane było na podstawie wniosku wysyłanego mejlem przez naczelnika lub Dyrektora DI do upoważnionego pracownika[91].

W zakresie BDO, upoważnieni przez Dyrektora DGO naczelnicy i kierownik zespołu nadawali uprawnienia użytkownika głównego lub podrzędnego dla podległych pracowników. Czynności te nie były dokumentowane[92]. Ponadto pracownicy, którzy uzyskali dostęp do BDO nie składali oświadczeń o zapoznaniu się z PBI BDO, pomimo takiego obowiązku[93]. W toku kontroli zobowiązano pracowników do spełnienia tego wymogu. Pracownicy MKiŚ nie mieli możliwości odbierania uprawnień użytkownikom BDO, dlatego, jak wyjaśniono[94], obecnie prowadzone są prace nad modułem Zarządzania Kontem w celu wdrożenia tej funkcjonalności. Wśród 24 kont użytkowników, 3 konta należały do osób, które zakończyły już pracę. Kontrolowany poinformował[95], że zwrócił się do IOŚ z prośbą o usunięcie kont i dostęp został odebrany.

W BDO istniały 2 rodzaje użytkowników: użytkownik główny i podrzędny. Użytkownik główny posiadał pełny zakres uprawnień, tj. poza wykonywaniem czynności materialno-technicznych, mógł on również tworzyć konta innych użytkowników m.in. z tym samym zakresem uprawnień. Zatem dochodziło do sytuacji, w której upoważniony przez naczelnika lub kierownika zespołu pracownik posiadający uprawnienia użytkownika głównego w systemie miał dostęp do funkcjonalności pozwalającej na dalsze zakładanie kont[96]. Nie powinien realizować takich czynności, bowiem nie posiadał upoważnienia w tym zakresie, jednak system nie blokował takiej możliwości.

Udzielono informacji[97], że wdrożenie funkcjonalności uniemożliwiającej takie działanie odłożono w czasie, z uwagi na realizację bardziej priorytetowych funkcjonalności. Trwają prace nad Panelem Administratora blokującym m.in. zarządzanie dostępem użytkowników do BDO, z którego korzystać będą mogli tylko wybrani użytkownicy.

Za zarządzanie infrastrukturą techniczną w EZD PUW i BDO odpowiedzialny był Zespół ds. Utrzymania Infrastruktury Teleinformatycznej, a w zakresie PDWD wykonawca zewnętrzny we współpracy z tym zespołem.

Koniecznym jest rozdzielenie w systemie BDO uprawnień użytkownika głównego, tj. uprawnień do czynności materialno-technicznych od możliwości tworzenia kont dla innych użytkowników, by nie dochodziło do sytuacji nadmiernej koncentracji uprawnień, przekraczającej zakres realizowanych zadań.

16. W MKiŚ nie dokonywano cyklicznych przeglądów nadanych uprawnień do systemów teleinformatycznych – z wyjątkiem EZD PUW, jednakże nie dokumentowano tych działań. Ponadto nie wdrożono zasad przechowywania wniosków o nadanie/cofnięcie uprawnień.

W MKiŚ nie było wyodrębnionego miejsca na przechowywanie *jednolitych wniosków*. Ich obsługą zajmowało się 3 pracowników WESI DI. Gromadzono je na imiennych kontach pracowników w EZD PUW[98].

Wnioski o nadanie/cofnięcie uprawnień administratorom w PDWD przechowywane były w skrzynce pocztowej pracownika upoważnionego do nadawania uprawnień[99].

Natomiast w zakresie BDO nie były one sporządzane, ponieważ każdy naczelnik / kierownik zespołu nadawał uprawnienia dla podległych pracowników. Sytuacja taka nie pozwalała na weryfikację prawidłowości procesu nadawania uprawnień (przeglądu uprawnień).

W stosunku do PDWD nie wskazano przyczyn przechowywania wniosków w skrzynce pocztowej. W odniesieniu do EZD PUW wyjaśniono[100], że sposób przechowywania

[91] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 1 lipca 2022 r.
[92] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 5 lipca 2022 r.
[93] Obowiązek wynikający z *Procedury kontroli (zarządzania) dostępu do systemu BDO*, stanowiącej załącznik nr 1 do PBI BDO.
[94] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 5 lipca 2022 r.
[95] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[96] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 5 lipca 2022 r.
[97] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[98] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 4 lipca 2022 r.
[99] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 1 lipca 2022 r.
[100] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.

jednolitych wniosków wynika z *Instrukcji Kancelaryjnej MKiŚ*[101], tj. są one dołączane do istniejącej sprawy w EZD PUW. Oprócz dołączenia *jednolitego wniosku* do istniejącej sprawy, MKiŚ powinno wdrożyć dodatkowe działania zapewniające możliwość szybkiego dostępu do nich w celu weryfikacji prawidłowości procesu nadawania uprawnień (przeglądu uprawnień).

Jedynie w stosunku do BDO określona została konieczność dokonywania cyklicznego przeglądu nadanych uprawnień. W *Procedurze dostępu do BDO* uwzględniono obowiązek administratora BDO dot. przeglądu uprawnień nie rzadziej niż raz do roku. Jak wskazano[102], z uwagi na ograniczoną funkcjonalność kont użytkownika głównego i podrzędnego, nie dostrzegano konieczności dokonywania takiego przeglądu.

Podano[103] także, że w MKiŚ nie wdrożono regulacji dot. cyklicznego przeglądu nadanych uprawnień do EZD PUW oraz PDWD niemniej jednak został on zaplanowany z terminem realizacji do 10 sierpnia 2022 r. Dodano, że uprawnienia użytkowników w EZD PUW są przeglądane przy każdej zmianie kadrowej i w przypadku zgłoszeń dot. nieprawidłowego działania systemu, a prowadzenie dokumentacji potwierdzającej te czynności byłoby czasochłonne, z uwagi na dużą liczbę dokonywanych sprawdzeń. Ponadto poinformowano, że uprawnienia do PDWD modyfikowane są na bieżąco, nie odniesiono się natomiast do przeglądu uprawnień administratorów do zarządzania kontami użytkowników.

17. Prawidłowo zarządzano hasłami w EZD PUW[104], tj. stosowano zasady złożoności hasła, jego zmiany przy pierwszym logowaniu i okresowej zmiany, zapamiętywania, ochrony przed udostępnianiem oraz określono czas aktywności sesji, po upływie którego system rozłączał się, a dostęp do niego wymagał ponownego logowania. Wprowadzone były rozwiązania blokowania dostępu do konta po określonej liczbie prób błędnego logowania.

W PDWD zasadnym byłoby wdrożenie, aby przy pierwszej próbie zalogowania system wymuszał zmianę hasła oraz zapamiętywał hasła, zapobiegając ich ponownemu wykorzystaniu. Logowanie użytkownika podrzędnego do BDO nie zapewniało takich funkcjonalności, za wyjątkiem ochrony hasła przed udostępnianiem i określenia czasu aktywności sesji, co wynikało z zakresu uprawnień takiego użytkownika, tj. posiadał on jedynie możliwość podglądu złożonych sprawozdań i prowadzonej przez podmioty ewidencji. Użytkownik główny logował się do BDO przez Krajowy Węzeł Identyfikacji Elektronicznej (login.gov.pl). Praktyka nadawania identyfikatorów we wszystkich 3 systemach pozwalała na ustalenie użytkowników.

Zasady dot. zarządzania hasłami oraz nadawania identyfikatorów zostały określone jedynie w odniesieniu do EZD PUW.

MKiŚ nie wdrożyło jednolitych postanowień dot. nadawania identyfikatora użytkownika. Każdy użytkownik posiadał niepowtarzalny identyfikator dostępności do systemu, ale sposób jego ustalania był różny. W systemie EZD PUW [redacted]. Z kolei w systemie PDWD nadawany był zgodnie z zasadą: [redacted]. Natomiast w systemie BDO identyfikator użytkownika podrzędnego to [redacted].

Kontrolowany nie wyjaśnił przyczyn braku regulacji dot. zarządzania hasłami systemu PDWD. Brak ich wdrożenia w systemie BDO argumentowano[105] tym, że były to funkcjonalności mniej priorytetowe niż te, których termin zrealizowania wynikał z przepisów ustaw. Dodano, że ich wprowadzenie zostanie poddane analizie w ramach kolejnych prac wytwórczych systemu.

18. **[incydenty]** W obszarze incydentów (z wyłączeniem systemu BDO[106]) funkcjonowały szczątkowe regulacje. Określały one jedynie konieczność niezwłocznego ich zgłaszania, rejestrowania oraz przeprowadzenia ich analizy (przy czym zakres tej analizy nie został określony) i wskazania działań korygujących, za co odpowiedzialny był Zespół ds. SZBI.

---

[101] Stanowiącej załącznik nr 1 do Zarządzenia Ministra Klimatu i Środowiska z 19 grudnia 2020 r. (poz. 31).
[102] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[103] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[104] EZD PUW jest systemem domenowym tj. dostęp do systemu możliwy jest po zalogowaniu się przez pracownika do komputera.
[105] Pismo z 2 sierpnia 2022 r., znak: DI-WRSI.081.18.2022.AS.
[106] Słabości obszaru zarządzania incydentami BDO zostały zidentyfikowane w toku audytu systemu BDO jednak MKiŚ nie wdrożyło jego rekomendacji. Zalecenie w zakresie zarządzania incydentami dot. budowy szczegółowych procedur postępowania np. w przypadku gromadzenia elektronicznych dowodów działań sprawcy (np. logi, postępowanie z urządzeniami po zidentyfikowanym ataku cyberterrorystycznym). Zorganizowania akcji uświadamiającej dot. konieczności i powodów zgłaszania takich naruszeń oraz przeprowadzania raz do roku weryfikacji procedury podczas symulacji wystąpienia incydentu.

Regulacje nie zawierały postanowień dot. obowiązku zgłaszania przez pracowników wszystkich zdarzeń związanych z BI, definicji zdarzenia związanego z BI i kategorii takich zdarzeń, planowania i przygotowania do reagowania na incydenty, klasyfikacji incydentów (określania ich priorytetów) wraz z maksymalnym czasem ich obsługi dla danego priorytetu, monitorowania, wykrywania i analizowania incydentów, w tym wyszukiwania powiązań oraz szacowania słabości zabezpieczeń, przekazywania informacji zwrotnej dla pracownika, który zgłosił zdarzenie/incydent o sposobie jego załatwienia, gromadzenia materiału dowodowego, zakresu informacji, jakie mają być gromadzone w rejestrze incydentów, zasad analizy tego rejestru oraz, w uzasadnionych sytuacjach, mechanizmów umożliwiających monitorowanie rozmiarów, a także kosztów incydentów związanych z BI.

> PBI nie wprowadzała definicji zdarzenia związanego z BI[107], a pracownicy zobowiązani byli do niezwłocznego zgłaszania incydentów. Z uwagi na odejście z pracy głównych osób zaangażowanych w BI, MKiŚ nie wyjaśniło przyczyn niezamieszczenia w regulacjach tej definicji oraz kategorii zdarzeń związanych z naruszeniem BI[108]. Wskazać należy, że nie każdy pracownik dysponuje specjalistyczną wiedzą pozwalającą na zakwalifikowanie danego zdarzenia związanego z BI jako incydent. Zatem zasadne byłoby wprowadzenie konieczności zgłaszania wszystkich tych zdarzeń. Natomiast jego kwalifikacja i ewentualne uznanie za incydent powinna być realizowana przez kompetentny personel. Wyjaśniono[109], że wprowadzenie takiego obowiązku nie jest do wyegzekwowania i uzależnione jest *de facto* od świadomości i chęci danego pracownika.

Wprowadzenie tego rozwiązania uwzględnia właśnie mniejszą świadomość pracowników, wskazując na możliwość zgłaszania każdego zdarzenia związanego z BI. Następnie, to kompetentne osoby, posiadające specjalistyczną wiedzę, zobowiązane byłyby do analizy, czy dane zdarzenie zostanie uznane za incydent (bowiem nie każde musi go wywołać).

> MKiŚ nie posiadało spójnych regulacji w zakresie kanałów zgłaszania incydentów. PBI wskazywała adres mejlowy incydent@klimat.gov.pl, podczas gdy *Procedura zarządzania incydentem bezpieczeństwa teleinformatycznego*[110] rozszerzała go o kontakt telefoniczny i przekaz ustny, które, jak wyjaśniono[111], gwarantowały prawidłowe zgłoszenie incydentu.
>
> W odniesieniu do braku postanowień w regulacjach wskazano[112], że nieokreślenie:
>
> - mechanizmów umożliwiających monitorowanie rozmiarów i kosztów incydentów związanych z BI, zasad klasyfikowania incydentów i określenia maksymalnego czasu ich obsługi z uwzględnieniem danego priorytetu, spowodowane było tym, że ówczesne kierownictwo nie dostrzegało potrzeby wdrożenia takich postanowień;
> - zasad gromadzenia materiału dowodowego, wynika z faktu, że są one oparte na przepisach prawa powszechnie obowiązującego, tj. ustawy *Kodeks postępowania karnego*[113]. Przepisy te jednak ogólnie normują kwestie dowodów, a MKiŚ powinno posiadać indywidualne rozwiązania dot. gromadzenia materiału dowodowego, dostosowane do swoich potrzeb;
> - postanowień dot. planowania i przygotowania do reagowania na incydenty wiązało się tym, że brano pod uwagę wytyczne dot. przygotowania planu reakcji na incydenty i zarządzania incydentami z wykorzystaniem norm PN-EN ISO/IEC 27005, 27001 i 27002. MKiŚ powinno posiadać regulacje wskazujące jakie rozwiązania wdrożyło w zakresie przestrzegania jej wymagań, a samo branie pod uwagę wytycznych z nich wynikających nie jest wystarczające;
> - zakresu informacji, jakie powinny zostać gromadzone w rejestrze incydentów wynikało z decyzji jaką w tej sprawie podjął ówczesny Pełnomocnik ds. BI.
>
> Kontrolowany nie odniósł się do powodów nieuregulowania: zasad analizy rejestru incydentów, kwestii monitorowania, wykrywania i analizowania incydentów, w tym wyszukiwania powiązań

[107] Określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.
[108] Pismo z 21 lipca 2022 r., znak: DI-WRSI.081.21.2022.AS.
[109] Pismo z 28 czerwca 2022 r., znak: DI-WRSI.081.3.2022.AS.
[110] Zatwierdzona 30 marca 2016 r.
[111] Pismo z 28 czerwca 2022 r., znak: DI-WRSI.081.3.2022.AS.
[112] Pismo z 28 czerwca 2022 r., znak: DI-WRSI.081.3.2022.AS.
[113] Ustawa z dnia 6 czerwca 1997 r., Dz. U. z 2022 r. poz. 1375, t. j.

oraz szacowania słabości zabezpieczeń[114] i przekazywania informacji zwrotnej dla pracownika, który zgłosił zdarzenie/incydent o sposobie jego załatwienia[115].

Udzielono informacji[116], że biorąc pod uwagę podpisaną umowę na świadczenie usług związanych z udoskonaleniem SZBI, Ministerstwo planuje zwrócić uwagę na postanowienia PBI związane z zarządzaniem incydentami i wprowadzić stosowne zmiany z uwzględnieniem powyższych elementów.

Uregulowanie wymienionych zagadnień służy wskazaniu właściwych norm postępowania. Całościowo określony sposób reagowania i postępowania z incydentami, zapewnia szybkie podjęcie działań naprawczych, co z kolei pozwala na ograniczenie skutków incydentów oraz doskonalenie zabezpieczeń.

19. Realizowano obowiązek rejestracji incydentów, zarówno tych pochodzących od pracowników, jak i z CSIRT.GOV.PL. Prowadzono 2 rejestry, tj. rejestr złośliwej/niechcianej poczty mailowej oraz rejestr incydentów prowadzony przez Zespół ds. SZBI (dalej: *rejestr incydentów*). Jednak *rejestr incydentów* nie był rzetelnie prowadzony, tzn. nie wszystkie dane w poszczególnych pozycjach zostały uzupełniane.

Katalog gromadzonych informacji w *rejestrze incydentów* wymaga rozszerzenia w szczególności o dane dot. priorytetu/poziomu incydentów, godziny ich zgłoszenia i zamknięcia (czasu obsługi). Pozwoliłoby to na ocenę skuteczności zastosowanych rozwiązań. Działania w tym zakresie powinny być dokumentowane, ponieważ ocena ta ma istotny wpływ na dobór właściwych zabezpieczeń.

W badanym okresie w rejestrze złośliwej/niechcianej poczty mailowej (wygenerowanym z informatycznego systemu przyjmowania zgłoszeń OTRS) zarejestrowano 363 takie zdarzenia, które uznano za incydenty. Wyjaśniono[117], że w takich sytuacjach służby informatyczne dokonywały blokady danego adresu mejlowego, a z uwagi na techniczny charakter tych czynności, nie były one opisywane w rejestrze.

Natomiast w *rejestrze incydentów* odnotowano 10 incydentów, w tym w 2021 r. 7 incydentów uznano za poważne. W regulacjach nie zdefiniowano pojęcia *incydent poważny*[118]. W ramach dobrych praktyk przyjęto, że to taki incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi. W związku z tym incydenty kwalifikowano uznaniowo jako incydenty poważne na podstawie kolumny zawierającej opis incydentu. Informacje nt. uznania danego incydentu za poważany nie zostały udokumentowane, dlatego Ministerstwo nie było w stanie wskazać które incydenty zostały za takie uznane. W rejestrze tym nie odnotowywano danych dot. priorytetu/poziomu incydentów, godziny ich zgłoszenia i zamknięcia (czasu obsługi). Ministerstwo nie podało z jakich powodów rejestr incydentów nie zawierał tych informacji.

20. **[szkolenia]** Wynikający z PBI obowiązek zapewnienia dla pracowników szkoleń w zakresie BI co najmniej raz w roku, nie został spełniony. W okresie objętym kontrolą szkolenie odbyło 113 z 973 (12%) pracowników zatrudnionych na dzień 20 maja 2022 r. Jednakże w przypadku większości z nich (tj. 96) od odbycia tego szkolenia minął rok, a nie zostało ono powtórzone. Z kolei 3 pracowników odbyło szkolenie w 2022 r., ale we wcześniejszym okresie nie uczestniczyło w nim (od 6 października 2020 r. do 31 grudnia 2021 r.). Z tego powodu wskazany wymóg corocznego udziału w szkoleniu został zrealizowany jedynie w odniesieniu do 14 z 973 (1,5%) pracowników. W toku czynności kontrolnych Ministerstwo wznowiło szkolenie. Udział w nim wzięło 779 pracowników.

W badanym okresie szkolenie w zakresie BI pn. *Polityka Bezpieczeństwa Informacji* realizowano z wykorzystaniem platformy e-learningowej hlearning.mos.gov.pl[119]. Szkolenie

[114] Wskazano jedynie, że odpowiedzialni za to byli administratorzy systemów z Zespołu ds. Utrzymania Infrastruktury Teleinformatycznej w ówczesnym BDG (pismo z 28 czerwca 2022 r., znak: DI-WRSI.081.3.2022.AS).
[115] Poinformowano tylko, że w przypadku incydentów, które nie były masowe oraz tych, zgłaszanych przez kierownictwo MKiŚ pracownicy WESI przekazywali informację zwrotną do zainteresowanego (pismo z 28 czerwca 2022 r., znak: DI-WRSI.081.3.2022.AS).
[116] Pismo z 28 czerwca 2022 r., znak: DI-WRSI.081.3.2022.AS.
[117] Pismo z 21 lipca 2022 r., znak: DI-WRSI.081.21.2022.AS.
[118] Pismo z 3 sierpnia 2022 r., znak: DI-WRSI.081.22.2022.AS.
[119] Na platformie tej dostępne było również szkolenie pn. *Bezpieczeństwo informacji*, jednakże w badanym okresie nie było ono realizowane.

to zostało wstrzymane na skutek trwających prac nad nową PBI[120], przez co wymóg jego odbycia co najmniej raz w roku wykonano jedynie w odniesieniu do 14 pracowników. W opinii MKiŚ[121] stan taki należało uznać *za wielce niepożądany*, dlatego Pełnomocnik ds. BI przypomniał dyrektorom komórek o konieczności uczestnictwa w nim.

Oprócz szkolenia e-learningowego, zapewniano pracownikom szkolenia zewnętrzne, np. *Auditor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001:2017*, *Zarządzanie ryzykiem w Systemach Bezpieczeństwa Informacji zgodnie z ISO/IEC 27005:2018*. Były to szkolenia uzupełniające, w szczególności dla Zespołu ds. SZBI i audytorów wewnętrznych i nie były traktowane jako wypełnienie nałożonego obowiązku[122].

Prace nad nową PBI nie mogą stanowić uzasadnienia dla braku organizacji szkolenia w zakresie BI, zatem słusznie wznowiono jego realizację. Działania te należy kontynuować, by wszyscy pracownicy odbyli szkolenie.

21. W MKiŚ wprowadzono wymóg zapoznania się z PBI przez wszystkich pracowników oraz osoby odbywające praktykę, staż lub wolontariat. Osoby te z chwilą rozpoczęcia pracy potwierdzały zapoznanie się z Polityką przy pierwszym zalogowaniu do EZD PUW. Ponadto, w przypadku osób niemających dostępu do tego systemu ustanowiono zastępczy mechanizm zapoznania się z jej treścią, tj. konieczność złożenia *Potwierdzenia zapoznania z PBI*[123]. Obowiązek ten w przypadku pracowników w 2022 r. został zrealizowany, a w 2021 r. nie dopełnił go tylko 1 ze 163 (1%) nowych pracowników, natomiast w przypadku stażystów i praktykantów nie zrealizowały go 4 z 17 (24%) badanych osób (3 stażystów i 1 praktykant). Spełnienie obowiązku monitorowane było jedynie w odniesieniu do pracowników MKiŚ.

Wymóg zapoznania się z PBI przez pracowników był monitorowany przez Zespół ds. SZBI, a jego wskaźnik[124] wskazywany w notatkach nt. funkcjonowania SZBI. W 2020 r. był on akceptowalny (91%)[125], natomiast w 2021 r. niedopuszczalny (83%), tj. z PBI nie zapoznało się 28 pracowników. Wyjaśniono[126], że ponowna, pogłębiona analiza danych dot. wskaźnika w 2021 r. wykazała, że przedstawione w notatce dane były niepoprawne. Z PBI nie zapoznał się 1 pracownik przebywający na urlopie bezpłatnym. Wszystkie osoby zatrudnione w Ministerstwie w 2022 r. spełniły ten obowiązek (82 pracowników).

Nie monitorowano natomiast obowiązku zapoznania się z PBI przez stażystów, praktykantów i wolontariuszy, a Kontrolowany nie wskazał powodów takiej sytuacji. Wymóg ten nie został zrealizowany przez 4 osoby (24%, tj. 3 stażystów i 1 praktykant) z 17[127] badanych.

Poinformowano[128], że ze względu na okres pandemii, staże realizowane były w formie zdalnej, a opiekunowie stażystów zostali poinformowani o konieczności dopełnienia wszelkich formalności. Dodatkowo w przypadku 1 z 3 stażystów poinformowano, że zapoznał się on z PBI podczas odbywania wcześniejszego stażu w okresie lipiec-sierpień 2018 r. Jednakże w tym okresie obowiązywała inna Polityka i staż odbywał się w innej jednostce.

Działania związane z monitorowaniem spełnienia obowiązku zapoznania się z PBI powinny dotyczyć wszystkich osób, w stosunku do których obowiązek ten wdrożono.

22. W MKiŚ nie przestrzegano obowiązku uwzględnienia w umowach cywilnoprawnych wymogu zapoznania się z PBI przez osoby świadczące na rzecz Ministerstwa usługi, które wpływały na poufność, integralność lub dostępność informacji.

Umowy nie zawierały postanowień, w których sformułowana byłaby konieczność zapoznania się z treścią PBI, mimo że w § 3 ust. 2 PBI wskazano na taki obowiązek przez osoby świadczące usługi, które *mogą wpływać na poufność, integralność lub dostępność informacji wykorzystywanych w MKiŚ*. Jego spełnienie zweryfikowano na podstawie wytypowanych do badania umów w zakresie serwisu infrastruktury IT oraz rozwoju infrastruktury i systemów

[120] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 7 czerwca 2022 r.
[121] Pismo z 15 lipca 2022 r., znak: DI-WRSI.081.17.2022.AS.
[122] Pismo z 23 czerwca 2022 r., brak znaku sprawy (nr 2156181.7830480.6252229).
[123] Załącznik nr 1 do PBI.
[124] Wskaźnik był obliczany jako stosunek liczby nowych pracowników, którzy zapoznali się z PBI do liczby wszystkich nowych pracowników zatrudnionych w danym okresie.
[125] Wartość akceptowalna wskaźnika występuje, gdy jest ona większa lub równa 90%.
[126] Pismo z 23 czerwca 2022 r., 2156181.7830480.6252229.
[127] W przypadku stażystów, praktykantów i wolontariuszy doboru próby dokonano metodą losową, ze stałym interwałem n+10, tj. wybrano 17 ze 170 (10%) stażystów, praktykantów, wolontariuszy, którzy rozpoczęli wykonywanie czynności po 6 października 2020 r. Dobór próby rozpoczęto od poz. 19 przekazanego 13 czerwca 2022 r. *Zestawienia stażystów, praktykantów oraz wolontariuszy wykonujących czynności na rzecz MKiŚ w okresie od 6 października 2020 r. do 20 maja 2022 r.*, gdyż poz. od 1 do 18 dot. osób, które rozpoczęły wykonywanie tych czynności przed 6 października 2020 r.
[128] Pismo z 15 lipca 2022 r., znak: DI-WRSI.081.17.2022.AS.

informatycznych (dalej: umowy IT)[129], a także 5[130] umów cywilnoprawnych[131] zawartych w innym przedmiocie. W przypadku umów IT obowiązek ten nie został spełniony w odniesieniu do 2[132] z 7 (29%) umów, w których konieczne było jego wskazanie. Natomiast w przypadku pozostałych 5 umów, w żadnej z nich nie uwzględniono postanowień, w których wykonawca oświadczałby, że zapoznał się z treścią PBI.

Ponadto Ministerstwo nie dysponowało zestawieniem zawartych umów cywilnoprawnych, które wpływały na poufność, integralność lub dostępność informacji, a ustalenie tych danych na potrzeby kontroli wymagało ręcznego przejrzenia każdej umowy[133]. Brak takiego narzędzia uniemożliwia weryfikację dopełnienia tego obowiązku.

23. [umowy] Postanowienia zawarte w umowach dot. serwisu infrastruktury IT oraz rozwoju infrastruktury i systemów informatycznych w niewystarczającym stopniu gwarantowały odpowiedni poziom BI i należyte zabezpieczenie interesów MKiŚ. W szczególności w umowach brakowało reguł dot. zachowania poufności po zakończeniu umowy (5 umów), zachowania bezstronności (9 umów), obecności wyznaczonego pracownika MKiŚ przy realizacji przedmiotu umowy w siedzibie Ministerstwa (7 umów), mechanizmów dot. kontroli lub audytu wykonawcy (5 umów).

Natomiast we wszystkich zbadanych umowach wskazano postanowienia dot.: parametrów świadczonych usług (parametrów SLA), obowiązku przeniesienia autorskich praw majątkowych do wytworzonych w ramach umów dzieł, kar umownych na wypadek niewykonania lub nienależytego wykonania umowy oraz warunków rozwiązania umowy.

W badanym okresie obowiązywało 167[134] umów dot. serwisu infrastruktury IT oraz rozwoju infrastruktury i systemów informatycznych. Kontroli poddano 10 z nich (6%)[135].

W 5[136] z 9[137] umów wskazano ogólne postanowienia dot. zachowania poufności, ale nie zobowiązano wykonawców do jej zachowania również po zakończeniu realizacji przedmiotu umowy. Kontrolowany nie odniósł się do tej kwestii.

Obowiązek zapewnienia poufności nie powinien ograniczać się wyłącznie do czasu trwania przedmiotu umowy. Zabezpieczenie takie powinno obowiązywać również po jej zakończeniu.

W 9[138] umowach brak było postanowień dot. zasad zachowania bezstronności przy jej realizacji, a w 1[139] przypadku nie było konieczności wskazywania takich postanowień, bowiem umowa dot. zakupu licencji. W opinii[140] Departamentu Prawnego MKiŚ, akceptującego umowy pod względem formalnoprawnym, nie było konieczności zawierania w nich postanowień dot. bezstronności. Natomiast DI wskazał, na przykładzie jednej z umów[141], że jej wykonawca będzie kierował się etyką zawodową, co obliguje go do zachowania bezstronności.

Samo kierowanie się etyką zawodową w przypadku umów dot. serwisu i rozwoju sprzętu i oprogramowania informatycznego jest niewystarczające dla zachowania bezstronności. Konieczne jest, aby wykonawca w swoich działaniach nie kierował się jakimikolwiek interesami, czy motywami mogącymi naruszać interesy stron. Ponadto wprowadzenie mechanizmów zapewnienia bezstronności minimalizuje ryzyko braku obiektywizmu i wystąpienia konfliktu interesów.

---

[129] Szczegóły doboru próby przedstawiono w projekcie w punkcie pn. umowy.
[130] Umowy nr: DLŁ/1/2022; BDG-wl/85/2020; DOZE/1/2021; BF/1/2022; DEK/17/2022.
[131] Dokonano doboru losowego, uwzględniając zakres realizowanych czynności przez wykonawców umów. Wybrano 5 z 18 umów z przekazanego zestawienia umów, stanowiącego załącznik do pisma Dyrektora Biura Kontroli i Audytu z 7 lipca 2022 r.
[132] Umowy nr: BDG-WESI-91/2020, BDG-WRSI-7/2021.
[133] W toku kontroli nie uzyskano danych nt. wszystkich zawartych umów cywilnoprawnych, które wpływały na poufność, integralność lub dostępność informacji, ze względu na czasochłonność przygotowania pełnego zestawienia. Ministerstwo przekazało zestawienie obejmujące tylko 6 z 26 komórek organizacyjnych (dot. 18 umów).
[134] Zestawienie 165 umów obowiązujących w MKiŚ na serwis infrastruktury IT oraz rozwoju infrastruktury i systemów informatycznych (pismo z 23 maja 2022 r.) oraz 2 umowy (nr BDG-WRSI-75/2020 oraz nr BDG-WRSI-98/2021) dot. wsparcia technicznego/serwisowego systemu PDWD.
[135] Próbę do badania dobrano metodą celową uwzględniając: wartość umowy, zasadność jej zawarcia oraz istotność przedmiotu umowy dla badanego obszaru. Zbadano umowy nr: BDG-WESI-91/2020, BDG-WESI-74/2021, BDG-WESI-80/2021, BDG-wrsi-1/2020, BDG-WRSI-63/2020, BDG-WRSI-71/2020, BDG-WRSI-7/2021, BDG-WRSI-12/2021, BDG-ZUIT.260.20.2021.RG-ZUIT.260/2021, BDG-WRSI-6/2022.
[136] Umowy nr: BDG-WESI-91/2020, BDG-wrsi-1/2020, BDG-WRSI-63/2020, BDG-WRSI-7/2021, BDG-WRSI-12/2021.
[137] W przypadku 1 umowy nie było konieczności wskazywania takich postanowień, ponieważ dotyczyła ona zakupu licencji. W pozostałych 4 umowach zobowiązano wykonawców do zachowania poufności również po zakończeniu realizacji ich przedmiotu.
[138] Nr: BDG-WESI-91/2020, BDG-WESI-74/2021, BDG-WESI-80/2021, BDG-wrsi-1/2020, BDG-WRSI-63/2020, BDG-WRSI-71/2020, BDG-WRSI-7/2021, BDG-WRSI-12/2021, BDG-WRSI-6/2022.
[139] Umowa nr BDG-ZUIT.260.20.2021.RG-ZUIT.260/2021.
[140] Pismo z 22 lipca 2022 r., znak: DI-WRSI.081.19.2022.AS.
[141] Umowa nr BDG-WESI-74/2021.

W przypadku 8[142] umów serwisowych ich przedmiot miał być realizowany m.in. w siedzibie Ministerstwa. W 1[143] dodano postanowienia o konieczności wykonywania tych czynności w obecności wyznaczonego pracownika MKiŚ, a pozostałych 7[144] umów nie zawierało takich postanowień. Obecność pracownika wpływa na zwiększenie poziomu BI oraz ogranicza ryzyko nieuprawnionego dostępu do informacji przez wykonawcę umowy. Wskazano[145], że kwestia ta nie została uregulowana w PBI. Dodano, *że w przygotowywanych przez służby informatyczne Ministerstwa umowach zawsze zawarte są szczegółowe postanowienia dotyczące sposobu realizacji umowy*.

W umowach serwisowych zawarto postanowienia dotyczące sposobu realizacji umowy, ale wśród nich nie ma postanowień dot. obecności wyznaczonego pracownika MKiŚ.

We wszystkich 5[146] umowach serwisowych, których przedmiot świadczony był m.in. zdalnie, tj. poza siedzibą MKiŚ nie określono mechanizmów umożliwiających Ministerstwu kontrolę / weryfikację działań wykonawcy dot. przestrzegania przez niego zasad BI. W sytuacji zdalnego dostępu istnieje wiele ryzyk w zakresie BI, dlatego zawarcie takich postanowień było istotne. Wyjaśniono[147], że możliwość audytu, w tym inspekcji w zakresie stosowania przez wykonawcę przepisów RODO[148] dopuszczono w umowach powierzenia przetwarzania danych osobowych.

Ochrona wyłącznie danych osobowych nie zapewnia pełnego bezpieczeństwa wszystkich informacji. Dlatego uprawnienia kontrolne/weryfikacyjne powinny zostać określone w szerszym zakresie. Umożliwiłoby to podejmowanie dodatkowych działań, w szczególności w sytuacjach powzięcia informacji nt. nieprzestrzegania przez wykonawców zasad BI.

24. W MKiŚ nie opracowano regulacji wewnętrznych w zakresie zawierania umów cywilnoprawnych określających katalog postanowień, jakie powinny być zamieszczane w umowach dot. serwisu oraz rozwoju sprzętu i oprogramowania informatycznego.

MKiŚ nie posiadało regulacji w zakresie zawierania umów cywilnoprawnych określających katalog postanowień, jakie powinny być zamieszczane w umowach dot. serwisu i rozwoju sprzętu i oprogramowania informatycznego, w szczególności odnoszących się do:

- poufności oraz bezstronności;
- parametrów świadczonych usług, poziomów niezawodności, w tym parametrów SLA na usługi serwisowe;
- mechanizmów kontroli i audytu wykonawcy w zakresie przestrzegania bezpieczeństwa informacji;
- odpowiedzialności i odszkodowania ze strony wykonawcy w przypadku niezastosowania się do procedur lub świadomego działania wpływającego na osłabienie systemu bezpieczeństwa;
- kwestii obecności (lub jej braku) wyznaczonego pracownika MKiŚ przy realizacji przedmiotu umowy;
- konieczności określenia w umowach osób odpowiedzialnych za sprawowanie bieżącego nadzoru nad ich realizacją lub upoważnionych do kontaktów w ramach tych umów;
- zasad odbioru przedmiotu umowy;
- przeniesienia autorskich praw majątkowych do wytworzonych dzieł;
- kar umownych na wypadek niewykonania lub nienależytego wykonania umowy oraz warunków jej rozwiązania;
- uwzględniania w umowach opisu i poziomu dostępu do urządzeń przetwarzających informacje lub do pomieszczeń, w których informacje są przetwarzane lub przechowywane.

Kontrolowany wyjaśnił[149], że nie jest w stanie odnieść się do przyczyn braku wdrożenia powyższych regulacji, mimo tego w każdej umowie zawarte są postanowienia merytoryczne oraz formalnoprawne. Odpowiadają za nie różne komórki Ministerstwa (DI, Departament Prawny) i IOD.

[142] Umowy nr: BDG-WESI-91/2020, BDG-WESI-74/2021, BDG-WESI-80/2021, BDG-wrsi-1/2020, BDG-WRSI-63/2020, BDG-WRSI-71/2020, BDG-WRSI-12/2021, BDG-WRSI-6/2022.
[143] Umowa nr BDG-WRSI-63/2020.
[144] Umowy nr: BDG-WESI-91/2020, BDG-WESI-74/2021, BDG-WESI-80/2021, BDG-wrsi-1/2020, BDG-WRSI-71/2020, BDG-WRSI-12/2021, BDG-WRSI-6/2022.
[145] Pismo z 22 lipca 2022 r., znak: DI-WRSI.081.19.2022.AS.
[146] Umowy nr: BDG-WESI-91/2020, BDG-wrsi-1/2020, BDG-WRSI-63/2020, BDG-WRSI-12/2021, BDG-WRSI-6/2022.
[147] Pismo z 22 lipca 2022 r., znak: DI-WRSI.081.19.2022.AS..
[148] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/W (Dz. Urz. UE.L nr 199, str. 1, ze sprost.).
[149] Pismo z 22 lipca 2022 r., znak: DI-WRSI.081.19.2022.AS.

Nie można zgodzić się z tymi wyjaśnieniami, bowiem w części umów nie określono postanowień, które zwiększyłyby BI, a opracowanie ich katalogu stanowiłby pomocnicze narzędzie, które zapobiegałoby pominięciu istotnych zabezpieczeń w umowach.

25. [praca zdalna] W MKiŚ przewidziano wykonywanie pracy zdalnej przy wykorzystaniu tokena uwierzytelniającego, a sprzęt komputerowy musiał posiadać aktualne oprogramowanie antywirusowe. Określono osoby uprawnione do wydania zgody na wykorzystywanie sprzętu prywatnego, zasady dot. miejsca wykonywania zadań, zlecania i organizacji pracy zdalnej, odbioru wyników pracy, ewidencję czasu pracy[150] i czynności wykonywanych zdalnie, prawa i obowiązki pracowników i pracodawcy. Zasadnym byłoby rozszerzenie przyjętych zasad o informacje nt. możliwości korzystania z ogólnodostępnej lub domowej sieci Wi-Fi, a w przypadkach jej dopuszczenia wskazanie opisu wymaganych zabezpieczeń.

Zasady korzystania z zasobów informatycznych MKiŚ[151] wskazywały na możliwość uzyskania takiego dostępu w przypadku wykonywania zadań poza siedzibą Ministerstwa za pomocą tokena uwierzytelniającego. Regulacja ta dopuszczała wykonywanie zadań służbowych z wykorzystaniem sprzętu prywatnego, ale w związku z zapewnieniem do 23 maja 2022 r. wszystkim pracownikom sprzętu służbowego, postanowienia te nie miały zastosowania po tym dniu. Wdrożono *Procedurę wydania i aktywacji Tokena VPN*[152]. W *Polityce kontroli dostępu*[153] zaznaczono, że stacje robocze przeznaczone do zdalnego korzystania z usług i zasobów sieci Ministerstwa nie mogą umożliwiać realizacji połączeń bez wykorzystania zabezpieczeń kryptograficznych. Praca zdalna opierała się o zasady publikowane w Intranecie oraz przekazywane pocztą elektroniczną przez Dyrektora Generalnego lub BDG. Odnosiły się one m.in. do zlecania pracy zdalnej i jej organizacji, sporządzania harmonogramów stanu realizacji zadań, praw i obowiązków pracowników i pracodawcy. Funkcjonował również: *Wniosek o pracę zdalną* oraz *Wniosek o pracę zdalną w związku z zagrożeniem koronawirusem*.

Ponadto w listopadzie 2020 r. Dyrektor Generalny polecił pracownikom przestrzeganie opracowanych *Zasad pracy zdalnej w MKiŚ.* Uregulowano tam m.in. warunki korzystania z prywatnego sprzętu do celów służbowych, ale nie wskazano, czy istnieje możliwość korzystania z ogólnodostępnej lub domowej sieci Wi-Fi. Stwierdzono tylko, że *Połącznie z Internetem powinno być zabezpieczone hasłem*. Powyższe zasady i wytyczne publikowane w Intranecie oraz przekazywane pocztą elektroniczną zaktualizowano 1 kwietnia 2022 r. poprzez wprowadzenie *Zasad świadczenia pracy zdalnej przez pracowników MKiŚ*.

Ponadto opracowano *Wytyczne w zakresie realizacji zadań w MKiŚ w związku z epidemią SARS-CoV-2*, jednak obejmowały one głównie działania mające na celu zapewnienie bezpieczeństwa sanitarnego.

26. Na urządzeniach mobilnych stosowano zabezpieczenia chroniące przetwarzane informacje, w szczególności przez uwierzytelnienie użytkownika, bezpieczne szyfrowane połączenie VPN oraz instalację oprogramowania antywirusowego, którego bazę danych o wirusach aktualizowano automatycznie. Wdrożono narzędzia umożliwiające monitorowanie użytkowników świadczących pracę zdalnie, jednakże czynności te nie były dokumentowane.

Na 1 grudnia 2020 r. sprzęt prywatny używany był przez 17 pracowników. Do 23 maja 2022 r. wszyscy pracownicy świadczący pracę zdalną wyposażeni zostali w służbowy sprzęt[154].

Poinformowano[155], że MKiŚ w okresie kontrolowanym nie prowadziło oddzielnej ewidencji osób, które pracowały na sprzęcie prywatnym. Sprzęt ten musiał posiadać zainstalowany i uruchomiony program antywirusowy, a dostęp do zasobów następował przez bezpieczne szyfrowane połączenie VPN. Zasadą było, że pracownicy pracujący zdalnie posiadali skonfigurowane urządzenia w taki sposób, aby zapewniały one dostęp do zasobów i uprawnień, jakie zostały przydzielone w przypadku świadczenia pracy w trybie stacjonarnym.

Za monitorowanie użytkowników świadczących pracę zdalnie odpowiedzialny był DI. W tym celu wykorzystywane było oprogramowanie służące do zapisywania zdarzeń i raportowania,

[150] Do 31 grudnia 2020 r. pracownicy wysyłali wiadomość mejlową dot. godziny rozpoczęcia i zakończenia pracy zdalnej do swoich sekretariatów oraz bezpośrednich przełożonych, a od 1 stycznia 2021 r. wprowadzono Wirtualny Rejestrator Czasu Pracy.
[151] Załącznik nr 6 do PBI.
[152] Zatwierdzona 5 września 2013 r.
[153] Zatwierdzona 27 maja 2014 r.
[154] Pismo z dnia 4 lipca 2022 r., znak: DI-WRSI.081.8.2022.AS.
[155] Pismo z 21 lipca 2022 r., znak: DI-WRSI.081.21.2022.AS.

zarządzania tożsamością użytkowników oraz zapewniające bezpieczeństwo. Wyjaśniono[156], że działania monitoringu nie są dokumentowane, ale oprogramowanie zachowuje monitorowane zdarzenia i istnieje możliwość podejrzenia zdarzeń (logów) dotyczących zdalnego dostępu do zasobów i systemów.

27. [kopie zapasowe] Działania w zakresie wykonywania i przechowywania kopii zapasowych wymają wzmocnienia. Ministerstwo dysponowało kopiami zapasowymi 3 badanych systemów teleinformatycznych, jednak okres retencji ich przechowywania wymaga zwiększenia. Zasadnym byłoby również przeniesienie macierzy na przechowywanie kopii zapasowych poza lokalizację, gdzie uruchomione są systemy teleinformatyczne oraz wdrożenie rozwiązań dot. dokumentowania działań związanych z odtworzeniem kopii zapasowych oraz danych z kopii.

W odniesieniu do EZD PUW oraz PDWD wykonywano syntetyczne kopie zapasowe (full backup) raz w tygodniu. Były one tworzone z kopii inkrementalnych (przyrostowych) tworzonych codziennie. Retencja przechowywania kopii została ustalona na 14 dni. W trakcie kontroli przygotowywane było postępowanie przetargowe, które miało zapewnić wystarczającą liczbę sprzętu serwerowego w celu tworzenia drugiej kopii zapasowej tych systemów.

System BDO składał się z 46 maszyn wirtualnych, zaś kopia zapasowa wykonywana była tylko dla 8 z nich. Retencja przechowywania kopii została ustalona na 7 punktów odtworzenia. Wyjaśniono[157], że takie rozwiązanie pozwala na odtworzenie infrastruktury pod system BDO. Odtworzenie klastra aplikacyjnego możliwe było z usługi chmurowej wykorzystywanej jako lokalizacja zapasowa do przechowywania kopii na wypadek awarii lokalizacji głównej. Usługa chmurowa świadczona była w ramach zawartej umowy. Wykonywanie kopii zapasowej wszystkich maszyn wirtualnych pozwoliłoby MKiŚ na dysponowanie drugą pełną kopią.

Mała retencja przechowywania kopii zapasowych w odniesieniu do 3 systemów teleinformatycznych (14 dniowa oraz 7 punktów odtworzenia, zamiast w szczególności 30 dniowej) wynikła[158] z braku zasobów dyskowych, tj. wystarczającego miejsca na przechowywanie kopii przez dłuższy okres. Wskazano, że zostanie to zmienione w ramach przygotowywanego postępowania przetargowego.

Ponadto MKiŚ nie dysponowało odpowiednio przystosowanym pomieszczeniem do uruchomienia macierzy na przechowywanie kopii zapasowych poza lokalizacją gdzie uruchomione były systemy teleinformatyczne. Brak przechowywania tych kopii w innej lokalizacji rodzi ryzyko niezapewnienia ich bezpieczeństwa w sytuacji uszkodzeń ośrodka podstawowego (serwerowni).

Działania związane z odtworzeniem kopii zapasowych oraz danych z kopii nie były dokumentowane. MKiŚ po odejściu administratorów oraz Pełnomocnika ds. BI nie posiadało dokumentacji potwierdzającej podejmowanie takich działań[159]. Niemniej obecnie po przeprowadzonej próbie odtworzenia danych z kopii zapasowej przedstawiono materiał potwierdzający pomyślną próbę ich odtworzenia.

28. Regulacje wewnętrzne dot. wykonywania, przechowywania i testowania kopii zapasowych nie były aktualne oraz wymagały uzupełnienia oraz dostosowania do rozwiązań funkcjonujących w Jednostce.

Ogólne postanowienia dot. kopii zapasowych zostały zawarte w PBI w zakresie cyberbezpieczeństwa, w szczególności dot. one celu wykonywania kopii oraz wskazania do czego służą. Ponadto MKiŚ nie posiadało[160] dokumentu określającego zakres, częstotliwość wykonywania i okres przechowywania kopii zapasowych ustaloną indywidualnie dla każdego systemu w zależności od oszacowanego ryzyka utraty danych i wpływu na ciągłość działania, pomimo że PBI w zakresie cyberbezpieczeństwa wskazuje na taką konieczność.

Obowiązywała *Procedura backupu systemu EZD* oraz *Procedura Awaryjna*. Jednakże *Procedura Awaryjna* została wprowadzona przed wdrożeniem systemu BDO, zatem nie regulowała przyjętych rozwiązań w zakresie tego systemu. Ponadto obie procedury nie określały retencji przechowywania kopii zapasowych z uwzględnieniem wymagań związanych z BI oraz krytyczności informacji dla ciągłości działania Ministerstwa, zasad postępowania w sytuacjach otrzymywania raportów dot. zapisu kopii z zastrzeżeniami oraz nieprawidłowego

[156] Pismo z dnia 4 lipca 2022 r., znak: DI-WRSI.081.8.2022.AS.
[157] Pismo z 21 lipca 2022 r., znak: DI-WRSI.080.3.2022.AS.
[158] Pismo z 21 lipca 2022 r., znak: DI-WRSI.080.3.2022.AS.
[159] Wyjaśnienia z 21 lipca 2022 r., znak: DI-WRSI.080.3.2022.AS.
[160] Wyjaśnienia z 27 czerwca 2022 r., znak: DI-WRSI.081.5.2022.AS.

zapisu i osób odpowiedzialnych za te działania, procedur odtwarzania i zasad dokumentowania tych działań, oraz wskazywały nieaktualne maszyny wirtualne.

29. [projektowanie, eksploatacja oraz wdrażanie zmian w systemach] Regulacje w zakresie projektowania, wdrażania oraz przeprowadzania zmian w systemach wymagały aktualizacji i uzupełnienia. Ponadto nie przestrzegano postanowień *Procedury zgłaszania zmiany i wykonywania testów*.

W badanym okresie nie wdrażano nowych systemów. Obowiązywała ogólna *Procedura określania specyfikacji technicznych wymagań odbioru systemów IT*, która, jak wyjaśniono[161] stanowiła wytyczne, natomiast w umowach uszczegóławiano postanowienia dot. specyfikacji technicznych. Procedura ta określała, wymagania dot. wdrażanego systemu, wymagania instalacji i przygotowania środowiska, przeniesienia autorskich praw majątkowych, obowiązek przeprowadzania testów oraz zakres platformy programowo-sprzętowej. Jednak była ona nieaktualna i wskazywała np. niższe parametry maszyny wirtualnej niż zostały wskazane w umowie na wsparcie serwisowe i usługi rozwojowe systemu PDWD[162].

Nie zaktualizowano *Procedury zgłaszania zmiany i wykonywania testów*. Nie określała ona zasad odbioru zmiany i obowiązku ich ewidencjonowania. Wskazano[163], że procedura ta będzie podlegała aktualizacji w ramach umowy na doskonalenie SZBI. Dodano, że przepisy umów określają procedurę zgłaszania zmiany, jej odbioru, terminów odbioru oraz określają wzór protokołu odbioru. Zamieszczany był on w EZD PUW w sprawie dot. umowy. Ponadto nie przestrzegano postanowień tej procedury, w szczególności w przypadku wdrożonej zmiany / modyfikacji PDWD[164], MKiŚ nie posiadało informacji o jej udokumentowaniu w systemie ITSM (OTRS) oraz utworzeniu w nim dokumentu RFC. Nie zostały także opracowane scenariusze testów wdrażanej zmiany.

Poinformowano[165], że funkcjonalność została wykonana zgodnie z załącznikiem do zlecenia jej wykonania[166], który zawiera dokładny opis zadań do wykonania. Załącznik ten oraz opis przyczyny zmiany zostały zaakceptowane przez ówczesnego Pełnomocnika ds. BI. Zmiana została przetestowana poprzez sprawdzenie poprawności zadań.

Dokumenty dot. wdrażanej zmiany systemu PDWD rzeczywiście zawierały wskazane informacje, jednakże dokument RFC, o którym mowa w *Procedurze zgłaszania zmiany i wykonywania testów,* dodatkowo wskazywał na konieczność podania w nim informacji nt. szacowania ryzyka wpływu zmiany na środowisko IT, a tego elementu załącznik do zlecenia wykonania zmiany nie zawierał. Ponadto MKiŚ powinno posiadać aktualne regulacje dostosowane do swoich potrzeb, wskazujące jakie dokumenty sporządzane są w procesie testowania zmiany.

30. Ministerstwo nie posiadało regulacji wewnętrznych opisujących proces monitorowania systemów teleinformatycznych, w szczególności pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanym. Podejmowało natomiast działania dot. monitorowania systemów.

Monitorowanie systemów teleinformatycznych odbywało się z wykorzystaniem specjalistycznego oprogramowania oraz narzędzi wbudowanych w systemy. Służby informatyczne monitorowały systemy pod względem wydajności (przeciążenia pamięci operacyjnej RAM, obciążenie procesora), jak i dostępnej przestrzeni dyskowej. Dodatkowo kluczowe systemy, z punktu widzenia zapewnienia ciągłości działania, monitorowano w zakresie obciążenia serwerów, macierzy oraz obciążenia infrastruktury sieciowej.

W MKiŚ obowiązywała *Polityka monitorowania parametrów*, ale skupiała się ona na monitorowaniu środowiska pracy systemów i działań użytkowników, a nie odnosiła się do procesu monitorowania systemów teleinformatycznych.

Podano[167], że nie są znane powody dla których ówczesny Pełnomocnik ds. BI nie zaktualizował tej polityki. Dodano, że każdy system informatyczny monitorowany jest w specyficzny dla niego

[161] Pismo z 8 lipca 2022 r., znak: DI-WRSI.081.9.2022.AS.
[162] Umowa nr BDG-WRSI-98/2021 z 25 listopada 2021 r.
[163] Pismo z 8 lipca 2022 r., znak: DI-WRSI.081.9.2022.AS.
[164] Dot. funkcjonalności edycji i wizualizacji obszaru na mapie w karcie informacyjnej.
[165] Pismo z 3 sierpnia 2022 r., znak: DI-WRSI.081.22.2022.AS.
[166] Pismo z 22 kwietnia 2021 r. (nr 1543906.5127452.4106927).
[167] Pismo z 8 lipca 2022 r., znak: DI-WRSI.081.9.2022.AS.

sposób, który z uwagi na dużą dynamikę zmian jest trudny do szczegółowego opisania. Wskazano także, że polityka ta zawiera przepis stanowiący, że monitorowanie dotyczy całego ruchu sieciowego w infrastrukturze informatycznej MKiŚ, zatem monitorowane i rejestrowane są wszystkie zdarzenia sieci, w których uczestniczą urządzenia sieciowe, a więc aktywne i pasywne urządzenia sieciowe, serwery, jak i oprogramowanie narzędziowe. Co do zasady monitorowane są więc parametry wydajnościowe i pojemnościowe.

Tak ogólne postanowienia regulacji nie zapewnią skutecznego procesu monitorowania systemów teleinformatycznych, w szczególności pod kątem wydajności i pojemności. Zrozumiałym jest, że niektóre systemy mogą wymagać indywidualnych rozwiązań w zakresie ich monitorowania. Ministerstwo powinno jednak wdrożyć ramowe zasady w tym przedmiocie, które dadzą podstawę do efektywnego działania.

31. Proces wdrażanej zmiany w PDWD był przejrzysty i uregulowany w umowie z wykonawcą. Wdrożenie zmiany przez wykonawcę nadzorowane było przez pracowników Ministerstwa i potwierdzone zostało testami. Prawidłowo przebiegły również zmiany wprowadzane w EZD PUW.

W badanym okresie w odniesieniu do systemu PDWD przeprowadzono zmianę w zakresie funkcjonalności edycji i wizualizacji obszaru na mapie w karcie informacyjnej. Usługa została zrealizowana przez wykonawcę terminowo. Dostęp do infrastruktury MKiŚ dla firmy zewnętrznej odbywał się poprzez aplikację RDM, która dawała możliwość monitoringu logowania i rejestracji sesji w formie archiwizowanego nagrania. Ponadto podczas wgrywanej zmiany zapewniony był kontakt z pracownikiem Ministerstwa, który poprzez RDM miał podgląd na czynności wykonawcy.

W zakresie EZD PUW zostały wdrożone 2[168] wersje systemu oraz wprowadzona zmiana konfiguracji polegająca na wyłączeniu funkcjonalności *zwykłego zakończenia koszulki*. Zmiany zostały przetestowane w środowisku testowym[169]. Ministerstwo prowadziło roboczy wykaz zmian zawierający informacje o wynikach testu, a informacje o wykrytych błędach były zgłaszane na pomoc@ezd.gov.pl. Kierowane były komunikaty do użytkowników informujące o planowanym wdrożeniu nowej wersji systemu.

Za modyfikację BDO i prowadzenie dokumentacji w tym zakresie odpowiedzialny był IOŚ.

32. W odniesieniu do BDO przeprowadzono badanie podatności (testy penetracyjne). Jednak 2 z 11 podatności przez 6 miesięcy nie zostało usuniętych. Wyeliminowanie kolejnej (1) z uwagi na niskie ryzyko, zostało włączone w prace dot. aktualizacji oprogramowania komponentów klastra. W zakresie PDWD nie przedstawiono dokumentacji potwierdzającej realizację takiego badania, choć jedna podatność została zidentyfikowana po otrzymaniu informacji z zespołu CSIRT.GOV i usunięta.

Badanie podatności systemu BDO przeprowadziła firma zewnętrzna, a jego wyniki przedstawiono w *Raporcie z oceny bezpieczeństwa aplikacji*[170]. Za wdrożenie rekomendacji odpowiedzialny był IOŚ, choć 2 podatności wymagały działań Ministerstwa, tj. jedna nie została wykonana, bowiem Ministerstwo nie wydało decyzji do skrócenia czasu trwania sesji (z godziny do 30 min.), w przypadku braku aktywności użytkownika, a w odniesieniu do kolejnej trwały analizy i ustalenia dot. wypracowania rozwiązania z dostawcą.

Podano[171], że czas trwania sesji został oszacowany w oparciu o zgłoszenia użytkowników. Wskazywali oni na uciążliwość dot. ponownego logowania, w przypadku krótkiego braku aktywności związanej z obsługą innych systemów w trakcie realizacji obowiązków.

Wskazać należy, że 30 minutowy brak aktywności użytkownika, nie jest krótkim czasem, a realizacja czynności w innych systemach nie powinna być uzasadnieniem do niepodjęcia decyzji o jego skróceniu. Ze względów BI oraz z uwagi na fakt, że podatność ta dotyczyła kont użytkownika głównego okres ten powinien zostać skrócony zgodnie z rekomendacją.

33. [zabezpieczenia techniczno-organizacyjne dostępu do informacji] W MKiŚ obowiązywały regulacje dot. minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji, w tym określające zasady ochrony fizycznej. Jednakże wymagały one aktualizacji,

[168] W dniu 22 stycznia 2021 r. oraz 24 maja 2021 r.
[169] Z wyjątkiem poprawki błędu przy przekazywaniu spraw i koszulek przy pomocy szablonu obiegu.
[170] Z 19 listopada 2021 r.
[171] Pismo z 3 sierpnia 2022 r., znak: DI-WRSI.081.22.2022.AS.

w szczególności w odniesieniu do pomieszczeń plombowanych, które zostały zabezpieczone w inny sposób bądź zmieniono ich przeznaczenie i nie wymagały już takiego zabezpieczenia. Regulacje te określały także zasady wydawania kluczy do pomieszczeń, które na skutek wdrożenia elektronicznego systemu zarządzania kluczami od 1 kwietnia 2022 r., przestały być aktualne. Ponadto nie przestrzegano postanowień *Regulaminu korzystania z miejsc postojowych Ministerstwa*[172] (dalej: Regulamin), w zakresie umieszczania przepustki w samochodzie w widocznym z zewnątrz miejscu[173].

Wdrożono *Politykę Bezpieczeństwa Informacji w Ministerstwie Środowiska w zakresie bezpieczeństwa fizycznego*[174] (dalej: PBI BF). Określała ona m.in. zasady dot. podziału budynku MKiŚ na strefy i dostępu do nich, przebywania osób na terenie MKiŚ. Regulacja ta wymagała aktualizacji, w szczególności w zakresie elektronicznego systemu zarządzania kluczami oraz wskazania wydzielonych pomieszczeń plombowanych, bowiem zostały one zlikwidowane, zmieniono ich przeznaczenie bądź zabezpieczenia[175].

Wyjaśniono[176], że trwają prace nad aktualizacją PBI BF. Rozpoczęły się one 26 października 2020 r., a długotrwałość tego procesu wynika z prowadzonych konsultacji i wdrażanych zmian organizacyjnych, powodujących konieczność ponownych uzgodnień. Usługi profesjonalnej całodobowej ochrony fizycznej osób i mienia w obiekcie świadczone były przez wyspecjalizowaną firmę w ramach zawartej umowy[177], która regulowała wymogi w tym zakresie.

Wdrożono rozwiązania zapewniające rejestrację ruchu pojazdów na terenie MKiŚ, w tym jego kontroli. Wspomniana firma zobowiązana była m.in. do kontroli uprawnień do parkowania pojazdów na parkingu wewnętrznym. Użytkownicy samochodów nie stosowali się do postanowień Regulaminu i nie umieszczali przepustki samochodowej w widocznym miejscu. Zatem kontrola ta nie była możliwa.

Udzielono informacji[178], że na bieżąco, ustnie przypominano o tym obowiązku. W ocenie MKiŚ nie było uzasadnienia aby odbierać z tego powodu uprawnień do korzystania z parkingów. Wskazać należy, że użytkownicy parkingów podpisują oświadczenie, w którym zobowiązują się do przestrzegania m.in. Regulaminu. W dokumencie tym pouczono, że nieprzestrzeganie jego postanowień może skutkować utratą prawa do korzystania z miejsca postojowego. Zatem MKiŚ może korzystać z prawa odebrania tych uprawnień.

34. Wdrożono rozwiązania zapewniające rejestrację ruchu osobowego na terenie Ministerstwa. Jednakże nie wszystkie tymczasowe karty dostępu wydane GDOŚ[179] zostały przypisane imiennie do danego użytkownika, co nie pozwalało na pełną kontrolę osób przebywających w MKiŚ.

Dostęp na teren odbywał się na podstawie magnetycznych kart dostępu (identyfikatorów). Wdrożono 3[180] rodzaje takich kart. Do sporządzania kart, nadawania uprawnień oraz kontroli dostępu wykorzystywany był program [redacted], który umożliwiał nadanie uprawnień do wybranych miejsc oraz gromadził dane ze wszystkich przejść. Pozwalał też na generowanie raportów nt. zdarzeń konkretnego pracownika[181] bądź zdarzeń na konkretnym przejściu. Rejestrował zdarzenia nieuprawnionych prób dostępu, tj. użycia identyfikatora na przejściu, do którego pracownik nie posiadał uprawnień. W przypadku pracowników kończących pracę w MKiŚ blokada dostępu następowała ostatniego dnia pracy, przy zdawaniu identyfikatora. Ponadto w toku kontroli wdrożono obowiązek potwierdzania odbioru i zdania karty dostępu.

39 z 41 kart tymczasowych wydanych dla GDOŚ nie posiadało imiennych informacji nt. ich użytkowników. MKiŚ nie znało powodów zaistniałej sytuacji[182]. Pracownik, który nadawał uprawnienia na kartach odszedł z pracy w kwietniu 2022 r. Poinformowano także, że karty te tymczasowo dezaktywowano, w celu identyfikacji osób je posiadających.

---

[172] Zał. do zarządzenia DG Ministerstwa Klimatu z 14 lipca 2020 r. *w sprawie zasad przydzielania miejsc postojowych oraz zasad korzystania z parkingów Ministerstwa Klimatu*.
[173] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 25 maja 2022 r.
[174] Zatwierdzona 5 stycznia 2017 r. i stanowiąca załącznik nr 7 do PBI.
[175] Pomieszczenia biblioteki i pokoju lekarskiego zostały zlikwidowane; pokoje 14, 24, 28, i 33 nie były plombowane, nie były także wykorzystywane przez księgowość, pomieszczenia ministra zamiast plomb posiadały system kontroli dostępu; pomieszczenia kasy, magazynów, archiwum nie były plombowane, natomiast plombowane były klucze do tych pomieszczeń i przechowywane w depozytorze skrytek.
[176] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 25 maja 2022 r. oraz aneks do protokołu z 4 lipca 2022 r.
[177] Umowa nr BDG-WZN-86/2021 z 28 października 2021 r.
[178] Pismo z 3 sierpnia 2022 r., znak: BDG-WZN.081.2.2022.KB.
[179] GDOŚ użytkuje pomieszczenia MKiŚ na podstawie zawartego porozumienia z 11 maja 2021 r. *w sprawie udostępnienia powierzchni i miejsca w serwerowni MKiŚ*.
[180] Były to karty: stałe – dla pracowników MKiŚ i GDOŚ; tymczasowe (okresowe) – dla m.in. pracowników jednostek podległych i nadzorowanych, praktykantów, stażystów, wolontariuszy, przedstawicieli instytucji kontrolujących; Gość – dla osób jednorazowo wchodzących do Ministerstwa.
[181] Przeszukiwanie zdarzeń danych osób w programie UniKD możliwe było na podstawie numeru karty dostępu lub nazwiska danej osoby.
[182] Pismo z 5 lipca 2022 r., znak: DI-WRSI.081.10.2022.AS.

35. Nie wszystkie klucze zostały objęte elektronicznym system zarządzania kluczami, który ograniczał nieuprawniony dostęp do pomieszczeń. W toku kontroli doszło do wyniesienia klucza poza teren MKiŚ oraz wydania klucza pracownikowi firmy zewnętrznej. Pobieranie i zdawanie kluczy znajdujących się w depozytorze skrytek, w sytuacjach przechowywania w danej skrytce więcej niż jednego klucza, nie zapewniało pełnej rozliczalności.

W Ministerstwie funkcjonował system elektroniczny zarządzania kluczami, do którego obsługi służył program [redacted]. Klucze przechowywane były w depozytorach kluczy oraz skrytek, a pracownicy pobierali i zdawali klucze przy użyciu karty dostępu (identyfikatora). Czynności te były rejestrowane w [redacted]. Za jego pomocą istniała możliwość wygenerowania raportów dot. m.in. informacji nt. pobrania i zdania kluczy. Wyjaśniono[183], że z [redacted] można uzyskać informacje, które klucze do pomieszczeń zostały pobrane, a nie zostały w tym samym dniu zdane. Jednak nie przedstawiono raportu potwierdzającego tę funkcjonalność.

Klucze nieobjęte elektronicznym systemem zarządzania wydawał i przyjmował pracownik ochrony[184]. Czynności te ewidencjonowano[185], jednak w maju 2022 r. w 8[186] przypadkach nie odnotowano zdania klucza.

W odniesieniu do wydania klucza pracownikowi firmy zewnętrznej[187] poinformowano, że sytuacja ta wynikała z pilnej interwencji, a działania tej osoby nadzorował pracownik ochrony. Potrzeba podjęcia pilnych działań nie może stanowić uzasadnienia do pobrania klucza przez osobę nieuprawnioną[188]. Fakt wyniesienia klucza grupowego przez pracownika serwisu sprzątającego poza teren MKiŚ został zgłoszony osobie sprawującej nadzór nad serwisem sprzątającym i sytuacja ta była wyjaśniana. Od 1 lipca 2022 r. klucze grupowe dla serwisu sprzątającego zostały włączone do elektronicznego systemu zarządzania kluczami.

W sytuacjach gdy w depozytorze skrytek w danej skrytce przechowywany jest więcej niż jeden klucz nie jest zapewniona pełna rozliczalność jego pobrania / zdania. W takich przypadkach nie były bowiem rejestrowane informacje do jakich konkretnie pomieszczeń pobrał klucz użytkownik danej skrytki. MKiŚ wskazało[189], że to użytkownik danej skrytki decyduje o sposobie jej wykorzystania, ponosi odpowiedzialność za jej zawartość i w jego gestii leży kwestia rozliczania pobrania / zdania kluczy.

36. Częściowe regulacje w zakresie utylizacji nośników danych wymagały aktualizacji i uzupełnienia, bowiem nie uwzględniały zasad niszczenia dysków SSD. Ponadto nie wdrożono postanowień dot. konieczności wymontowania nośników danych z komputerów i laptopów przeznaczonych do utylizacji / zbycia, zasad dokumentowania tych czynności oraz zasad usuwania danych m.in. z telefonów, tabletów, pendrive'ów, które także zostały przeznaczone do utylizacji lub zbycia. W badanym okresie doszło do zlikwidowania komputerów, laptopów oraz monitorów, jednak działania związane z wymontowaniem nośników danych nie zostały udokumentowane.

Stała Komisja Likwidacyjna dokonała oceny stanu m.in. komputerów, laptopów oraz monitorów przeznaczając je do likwidacji jako zużyte składniki majątkowe, a następnie nadzorowała ich zniszczenie przez pracowników firmy zewnętrznej. Czynności te udokumentowano[190], choć nie zawarto informacji o wymontowaniu z komputerów i laptopów nośników danych.

PBI w zakresie cyberbezpieczeństwa wskazywała, że *do postępowania z informatycznymi nośnikami danych stosuje się odpowiednio zasady postępowania ze składnikami aktywów Ministerstwa określonymi w procedurach kontroli finansowej*, tj. w zarządzeniu w sprawie polityki rachunkowości oraz procedur kontroli finansowej MKiŚ[191] (dalej: polityka rachunkowości). Zarządzenie to nie zawierało jednak postanowień w tym zakresie.

Poinformowano[192], że nie jest możliwym ustalenie co ówczesny Pełnomocnik BI miał na uwadze wprowadzając ten przepis.

---

[183] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 14 czerwca 2022 r.
[184] Klucze do: węzła ciepłowniczego(kotłowni)/wodomiaru, wejścia głównego i wyjść ewakuacyjnych, pomieszczeń technicznych, sal konferencyjnych, dla serwisu sprzątającego.
[185] Prowadzone były 3 książki dot. pobrania / zdania kluczy: do sal konferencyjnych, przez serwis sprzątający oraz do pozostałych pomieszczeń.
[186] Informacji tych brakowało w 5 przypadkach w zakresie kluczy do sal konferencyjnych, w 1 dot. kluczy pobieranych przez serwis sprzątający oraz w 2 dot. pozostałych pomieszczeń.
[187] Protokół oględzin oraz przyjęcia ustnych wyjaśnień z 14 czerwca 2022 r.
[188] Uprawnienie to przysługiwało tylko wyznaczonym pracownikom Wydziału Zarządzania Nieruchomością BDG.
[189] Pismo z 3 sierpnia 2022 r., znak: BDG-WZN.081.2.2022.KB.
[190] Protokół nr 2/2021 Stałej Komisji Likwidacyjnej powołanej przez Dyrektora Generalnego MKiŚ 5 listopada 2020 r. w celu dokonania przeglądu i oceny stanu środków trwałych, pozostałych środków trwałych (dot. wyposażenia) oraz środków znajdujących się w ewidencji ilościowej MKiŚ, kwalifikujących się do ich likwidacji, zatwierdzony przez Dyrektora Generalnego 19 lipca 2021 r. oraz protokół likwidacji z 4 sierpnia 2021 r.
[191] Zarządzenie z 26 listopada 2021 r. wraz z załącznikami oraz zmianą wprowadzoną zarządzeniem z 30 grudnia 2021 r.
[192] Pismo z 1 sierpnia 2022 r., znak: DI-WRSI.081.20.2022.GK.

Wdrożona *Procedura bezpieczeństwa i utylizacji sprzętu elektronicznego* dot. niszczenia nośników elektromagnetycznych oraz CD/DVD nie odnosiła się do niszczenia dysków SSD. Wskazano[193], że procedura nie została jeszcze zmieniona pod kątem likwidacji tego typu dysków, ze względu na niewielką liczbę nośników SSD. Zadeklarowano, że zostanie ona zaktualizowana w ramach umowy na udoskonalenie SZBI. Będzie obejmować nośniki SSD, tablety oraz telefony komórkowe. W odniesieniu do pendrive wskazano, że po jego wydaniu pracownik z niego korzysta i urządzenie nie podlega zwrotowi. Natomiast w zakresie komputerów podkreślono, że wymontowywane są z nich dyski twarde.

Obowiązek wymontowania nośników danych z komputerów przeznaczonych do utylizacji powinien wynikać także z regulacji wewnętrznych wraz z koniecznością dokumentowania tych czynności. Powinny istnieć także wymogi zdawania pendrive i usuwania z niego danych, eliminując ryzyko przetwarzania przez pracownika informacji po zakończeniu zatrudnienia.

37. W przypadku naprawy 3 z 4 laptopów zapewniono bezpieczeństwo informacji, w szczególności przez wymontowanie nośników danych, choć działania te nie zostały udokumentowane. Natomiast w przypadku 1 laptopa wyjęcie nośnika danych nie było możliwe bez uszkodzenia konstrukcji urządzenia, dlatego laptop został przywrócony do ustawień fabrycznych. W Ministerstwie nie zostały określone zasady naprawy sprzętu informatycznego.

W badanym okresie doszło do naprawy pogwarancyjnej 4 laptopów.

Wyjaśniono[194], że co do zasady sprzęt informatyczny naprawiany jest w siedzibie MKiŚ w ramach gwarancji. Naprawy pogwarancyjne wstępują sporadycznie. 3 z 4 laptopów zostało przekazanych do serwisu zewnętrznego bez nośników danych. Ministerstwo nie przedstawiło dokumentacji potwierdzającej ich wymontowanie.

W sprawie przyczyn braku naprawy laptopa w siedzibie MKiŚ (pod nadzorem upoważnionego pracownika), z którego nie było możliwości wyjęcia nośnika wskazano[195], że zdecydowana większość serwisów świadczy usługi naprawy tylko w siedzibie serwisu. Jeśli już usługa jest realizowana poza tą siedzibą, to naprawa jest znacznie droższa. Zaznaczono także, że w takim przypadku istniałaby konieczność oddelegowania pracownika służb informatycznych do nadzorowania naprawy, co w przypadku niewielkich zasobów kadrowych jest wielce problematyczne.

W zakresie braku regulacji dot. zasad napraw sprzętu informatycznego poinformowano[196], że ówczesny Pełnomocnik ds. BI postanowił, że z powodu rzadko występujących napraw pogwarancyjnych oraz wymontowania nośników danych wdrożenie szczególnych zasad naprawy sprzętu informatycznego było zbyteczne.

Nie można zgodzić się z tymi wyjaśnieniami, bowiem MKiŚ powinno wdrożyć zasady w tym przedmiocie. W szczególności wskazujące na konieczność wymontowania nośników w przypadku każdej naprawy i dokumentowania tych czynności, jak również zasady postępowania w przypadku braku takiej możliwości. Przywrócenie laptopa do ustawień fabrycznych nie gwarantuje pełnego zachowania bezpieczeństwa informacji.

38. [rozliczalność] Użytkowane przez Ministerstwo 3 systemy teleinformatyczne zapewniały rozliczalność działań użytkowników, a informacje zawarte w dziennikach systemów (logach) były przechowywane przez okres 2 lat. W przypadku systemu BDO dziennik dostępu uprzywilejowanego do systemu prowadził IOŚ. MKiŚ realizowało działania związane z przeglądem logów i ich analizą w celu identyfikacji działań niepożądanych, jednak nie były one dokumentowane. Wdrożone w tym zakresie regulacje wymagały aktualizacji i uszczegółowienia, w szczególności odnośnie do określenia zasad przeglądu dzienników systemów (logów) i ich analizy.

W przypadku 3 badanych systemów dostęp do aktywnych i pasywnych urządzeń sieciowych posiadali pracownicy Zespołu ds. Utrzymania Infrastruktury Teleinformatycznej DI. Dokonywali oni przeglądu logów i ich analizy. Ponadto do wsparcia tego zadania było wykorzystywane

[193] Pismo z 1 sierpnia 2022 r., znak: DI-WRSI.081.20.2022.GK.
[194] Pismo z 30 czerwca 2022 r., znak: DI-WRSI.081.7.2022.AS.
[195] Pismo z 1 sierpnia 2022 r., znak: DI-WRSI.081.20.2022.GK.
[196] Pismo z 30 czerwca 2022 r., znak: DI-WRSI.081.7.2022.AS.

narzędzie do korelacji i analizy logów. Wyjaśniono[197], że MKiŚ nie posiada dowodów/raportów na wykonywanie analiz, gdyż są one wykonywane na bieżąco w ramach standardowych działań administratora systemów. Dodano, że administratorzy aplikacji EZD PUW oraz PDWD także przeglądają logi oraz dokonują ich analizy.

Wdrożono ogólne regulacje dot. rejestracji zdarzeń i użytkowników, żadna z tych regulacji nie określała jednak zasad i zakresu przeglądu logów i ich analizy. Tj. wprowadzono:

- *Politykę monitorowania parametrów*, wskazującą w szczególności, że monitorowane i rejestrowane powinny być wszystkie zdarzenia w sieci, w których uczestniczą urządzenia sieciowe, oprogramowanie narzędziowe, ze wskazaniem co podlega rejestracji;

- *Procedurę utrzymywania rejestru awarii* zobowiązującą do dokonywania zmian konfiguracji na serwerach z zastosowaniem systemu zarządzania sesjami uprzywilejowanymi, a w przypadku dokonywania tych zmian bez wykorzystania tego systemu prowadzenia dziennika czynności technologicznych systemów informatycznych.

  W celu zachowania rozliczalności analogiczne postanowienia zawarte zostały w *Procedurze kontroli dostępu dla użytkowników uprzywilejowanych systemu BDO*, jednakże MKiŚ nie posiadało podpisanej wersji procedury. Ponadto *Procedura utrzymywania rejestru awarii* wskazywała na wykorzystanie systemu zarządzania sesjami uprzywilejowanymi CyberArk, a procedura dot. systemu BDO na wykorzystywany system Devolutions Desktop Manager.

Możliwość przypisania określonych działań konkretnej osobie oraz umiejscowienie ich w czasie zwiększa BI przetwarzanych w systemach.

Biorąc pod uwagę ustalenia i oceny przedstawione w *Wystąpieniu*, zalecam Pani Minister:

1. Opracowanie i wdrożenie kompleksowego, spójnego systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność, integralność informacji, w tym:
   - rzetelną analizę ryzyka w odniesieniu do wszystkich aktywów Jednostki wraz z planem postępowania z ryzykiem;
   - przegląd procedur i regulacji wewnętrznych w celu dostosowania do funkcjonujących rozwiązań w MKiŚ;
   - sporządzenie planów ciągłości działania na wypadek wystąpienia zdarzeń zagrażających realizacji zadań;
   - utworzenie pełnej bazy konfiguracji CMDB;
   - prawidłowe zarządzanie uprawnieniami użytkowników, zapewniające uprawnienia adekwatne do zadań i obowiązków pracowników.
2. Wdrożenie narzędzi i mechanizmów zarządczych gwarantujących Kierownictwu MKiŚ skuteczny nadzór w procesie ustanawiania, eksploatacji i doskonalenia SZBI.
3. Cykliczną identyfikację słabości SZBI, w szczególności poprzez realizację audytu oraz wdrażanie jego rekomendacji.
4. Uwzględnienie w Porozumieniu dot. administrowania oraz utrzymywania systemu BDO szczegółowego podziału zadań i odpowiedzialności pomiędzy MKiŚ a IOŚ.
5. Prawidłowe zabezpieczenie interesów Ministerstwa w zawieranych umowach oraz wprowadzenie mechanizmów wsparcia tego procesu, w tym rozważenie określenia katalogu postanowień gwarantujących właściwy poziom ochrony i bezpieczeństwa informacji.
6. Kontynuację działań mających na celu podnoszenie świadomości pracowników w obszarze bezpieczeństwa informacji oraz zapewnienie ich cykliczności.

[197] Pismo z 8 lipca 2022 r., znak: DI-WRSI.081.13.2022.AS.

7. Wyeliminowanie pozostałych nieprawidłowości wskazanych w *Wystąpieniu*.

Proszę Panią Minister o przedstawienie, w terminie 60 dni od daty otrzymania *Wystąpienia*, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Informuję, że od *Wystąpienia* nie przysługują środki odwoławcze.

Podstawa prawna:
Art. 46 ust. 3, art. 47, 48 i 49 *ustawy o kontroli.*

Z poważaniem

Z upoważnienia Ministra Cyfryzacji

Janusz Cieszyński
Sekretarz Stanu
w Kancelarii Prezesa Rady Ministrów
Pełnomocnik Rządu ds. Cyberbezpieczeństwa

/-podpisano kwalifikowanym podpisem elektronicznym-/