MINISTER CYFRYZACJI

Mateusz Morawiecki

DNK.WK.1743.1.2021.MJ

Warszawa, /elektroniczny znacznik czasu/

Pani
Marlena Maląg

Minister
Rodziny i Polityki Społecznej

WYSTĄPIENIE POKONTROLNE

Przedstawiam Pani Minister *Wystąpienie pokontrolne* (dalej: *Wystąpienie*) z kontroli przeprowadzonej[1] przez Kancelarię Prezesa Rady Ministrów w Ministerstwie Rodziny i Polityki Społecznej[2] (dalej: MRiPS, Ministerstwo, Jednostka) w zakresie *wykorzystania systemów teleinformatycznych do realizacji zadań publicznych w okresie od 6 października 2020 r. do 30 lipca 2021 r.*[3].

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

OCENA KONTROLOWANEGO OBSZARU

Pozytywnie ocenić należy działania Ministerstwa mające na celu zapewnienie bezpieczeństwa informacji (dalej: BI) w zakresie zarządzania infrastrukturą informatyczną dotyczące:

- bezpieczeństwa przy pracy zdalnej,
- zabezpieczenia dostępu do systemów i nadawania uprawnień,
- wdrożenia rozwiązań monitorujących ruch osobowy w obiektach MRiPS,
- monitorowania systemów teleinformatycznych i środowiska ich pracy, a także działań użytkowników w tych systemach,
- zapewnienia przejrzystego procesu wdrażania zmian w systemach oraz tworzenia kopii zapasowych.

Dla pełnego wdrożenia kompleksowego i spójnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej: *SZBI*) zasadna jest ponadto zmiana podejścia do jego ustanowienia. Skuteczne wprowadzenie tego systemu wymaga identyfikacji obszarów wymagających zmiany/korekty oraz proaktywnego zarządzania systemem. W szczególności niezbędne jest opracowanie całościowej analizy ryzyka w stosunku do wszystkich aktywów Jednostki,

[1] Kontrolę przeprowadzili pracownicy Kancelarii Prezesa Rady Ministrów: Magda Jarosławska, radca, kierownik zespołu kontrolującego, Gaweł Lisowski, główny specjalista, członek zespołu kontrolującego. Czynności kontrolne realizowano w okresie od 27 maja do 30 lipca 2021 r. W związku ze stanem epidemii spowodowanym zakażeniami wirusem SARS-CoV-2 kontrolę prowadzono hybrydowo, tj. część czynności zrealizowano w siedzibie Ministerstwa przy ul. Nowogrodzkiej 1/3/5, 00-513 Warszawa, a część poza nią. 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] MRiPS powstało 6 października 2020 r. w drodze przekształcenia Ministerstwa Rodziny, Pracy i Polityki Społecznej (na podstawie rozporządzenia Rady Ministrów z dnia 7 października 2020 r. w sprawie utworzenia Ministerstwa Rodziny i Polityki Społecznej (Dz. U. poz. 1735). Do dnia zakończenia czynności kontrolnych w jego skład wchodziło 19 komórek organizacyjnych obsługujących sprawy z działów administracji rządowej ***zabezpieczenie społeczne*** oraz *rodzina*. Na mocy rozporządzenia Rady Ministrów z dnia 12 sierpnia 2021 r. w sprawie przekształcenia Ministerstwa Rodziny i Polityki Społecznej (Dz. U. poz. 1471) dotychczasowy zakres działania Ministerstwa został rozszerzony i objął także dział *praca*.

[3] Z możliwością zasięgania informacji dot. funkcjonowania systemu zarządzania bezpieczeństwem informacji w Ministerstwie Rodziny, Pracy i Polityki Społecznej w latach 2019-2020, jeżeli podjęte działania w tym okresie miały wpływ na funkcjonowanie tego systemu w MRiPS.

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

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

kompleksowej dokumentacji *SZBI* oraz wdrożenie narzędzi nadzorczych dostarczających całościowych informacji nt. poszczególnych etapów jego ustanawiania.

System zarządzania bezpieczeństwem informacji

- **[*SZBI*]** Warunkiem skutecznego zarządzania BI jest posiadanie przez Jednostkę kompleksowej dokumentacji. Ministerstwo wdrożyło *Politykę Bezpieczeństwa Informacji w obszarze IT,* która regulowała szereg zagadnień wspierających proces zarządzania infrastrukturą informatyczną. Regulacja ta jednak dotyczyła wyłącznie bezpieczeństwa informatycznego i nie odnosiła się do wszystkich obszarów *SZBI*, w szczególności takich jak przeglądy *SZBI*, analiza ryzyka, audyt BI, baza konfiguracji CMDB.
- **[Nadzór]** Nadzór nad *SZBI* był rozproszony i nie wszystkie obszary systemu zostały nim objęte, w szczególności dotyczące przeglądów *SZBI*, analizy ryzyka, audytu BI oraz bazy konfiguracji CMDB. Ministerstwo nie posiadało także zbiorczych informacji, które są kluczowe w procesie zarządzania. Nie przeprowadzono bowiem całościowej analizy aktualnego stanu BI, umożliwiającej opracowanie planu/strategii rozwoju *SZBI.*
- **[Analiza ryzyka i plan postępowania z ryzykiem]** Realizowane były czynności dotyczące szacowania ryzyka, jednak podejmowane działania prowadzone były na potrzeby kontroli zarządczej. Identyfikowano ryzyka w stosunku do zadań, podczas gdy celem analizy ryzyka BI, powinna być w pierwszej kolejności ocena ryzyk związanych z utratą integralności, dostępności lub poufności.
- **[Audyt]** W Ministerstwie przeprowadzono audyt BI i podejmowano działania w celu doskonalenia *SZBI*. Audytem nie objęto wszystkich obszarów *SZBI*. Tym samym nie zidentyfikowano kompleksowo nieprawidłowości systemu, przez co nie zapewniono możliwości ich eliminacji. Pozytywnie należy ocenić wdrożenie rozwiązań zapewniających monitorowanie stopnia wykonania rekomendacji audytu.
- **[Baza CMDB]** Prowadzono inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji, ale w ewidencjach / rejestrach nie ujęto wszystkich aktywów informatycznych i nie wskazano relacji pomiędzy elementami konfiguracji. Tym samym nie można uznać, że dysponowano kompleksową bazą CMDB.
- **[Uprawnienia]** Ministerstwo posiadało regulacje w obszarze nadawania, modyfikacji i odbierania uprawnień. Wymagają one aktualizacji w zakresie wykorzystywanego narzędzia do przekazywania wniosków dotyczących uprawnień (samoobsługowy system rejestracji zgłoszeń[6] zastąpiono systemem eDok) oraz uzupełnień o przepisy gwarantujące niezwłoczne odbieranie uprawnień po zakończeniu zatrudnienia. Działania w zakresie nadawania uprawnień pracownikom, wykonawcom umów, a także zarządzania hasłami były wykonywane prawidłowo.
- **[Incydenty]** Realizowano działania w zakresie rejestracji incydentów oraz przeprowadzano analizę rejestrów incydentów w celu doskonalenia stosowanych zabezpieczeń. Nie sporządzano jednak dokumentacji z tych czynności, a regulacje z tego obszaru nie zostały zaktualizowane i uzupełnione.
- **[Zapewnienie wiedzy pracownikom]** Kontynuacji wymagają działania dotyczące zwiększania świadomości pracowników w zakresie BI. Od cyklu szkoleń e-learningowych (marzec-kwiecień 2019 r.), w wyniku których przeszkolono znaczą część pracowników (438), minął bowiem 2-letni okres, w którym pracownik, w myśl postanowień PBI IT, powinien odbyć takie szkolenie. Wpływ na niedotrzymanie terminu miała w szczególności pandemia COVID-19.
- **[Umowy]** Umowy dotyczące serwisu i rozwoju systemów teleinformatycznych zabezpieczały interesy Skarbu Państwa. Zasadnym byłoby jednak rozszerzenie

[6] http://serwis/maximo/ui/login.

postanowień umów o kwestię odszkodowania ze strony wykonawcy w przypadku niezastosowania się do procedur lub świadomego działania wpływającego na osłabienie systemu bezpieczeństwa oraz bezstronności wykonawców. Regulacje wewnętrzne w tym obszarze wymagają uzupełnienia o katalog niezbędnych postanowień dotyczących ochrony i bezpieczeństwa informacji.

- **[Praca na odległość]** Podejmowano właściwe działania zapewniające bezpieczną pracę na odległość. Zostały w tym zakresie wdrożone stosowne regulacje i zasady, a na urządzeniach mobilnych stosowano zabezpieczenia chroniące informacje. Wdrożono także narzędzia umożliwiające monitorowanie użytkowników świadczących pracę zdalnie w celu wykrycia nieuprawnionych działań.
- **[Kopie zapasowe]** Działania w zakresie wykonywania i testowania kopii zapasowych zostały dostosowane do potrzeb Ministerstwa i stanowiły wsparcie w zarządzaniu tym obszarem.
- **[Zabezpieczenia organizacyjno-techniczne dostępu do informacji]** Ministerstwo wdrożyło skuteczne rozwiązania zapewniające rejestrację ruchu osobowego na terenie obiektów Ministerstwa, w tym pozwalające na jego kontrolę. W Jednostce wprowadzono też regulacje dotyczące minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji, z uwzględnieniem zasad ochrony fizycznej.

  Jednakże na skutek zmian organizacyjnych regulacje te wymagają aktualizacji. Działania związane z plombowaniem pomieszczeń w celu zwiększenia bezpieczeństwa informacji w nich przetwarzanych były właściwe. Wymagają one uzupełnienia o wprowadzenie obowiązku ewidencji tych pomieszczeń oraz zasad zarządzania kluczami, w tym zasad dostępu do danego pomieszczenia przez poszczególnych pracowników.
- **[Zabezpieczenia organizacyjno-techniczne systemów]** Szczególnie pozytywnie należy ocenić stosowane zabezpieczenia serwerowni, które spełniały wysokie standardy oraz fakt wydzielenia pomieszczenia backupu do odrębnej lokalizacji. Oba rozwiązania sprzyjały zapewnieniu BI. Ministerstwo powinno również rozważyć wzmocnienie zabezpieczeń pomieszczenia backupu oraz jednego z wyjść ewakuacyjnych. Bezpieczeństwo systemów wzmacniały także wdrożone działania w zakresie ochrony antywirusowej oraz antyspamowej.
- **[Projektowanie, eksploatacja oraz wdrażanie zmian w systemach]** Ministerstwo posiadało ogólne regulacje w zakresie projektowania, wdrażania i eksploatacji systemów teleinformatycznych oraz przeprowadzania zmian w systemach, a szczegółowe wymogi w tym zakresie określane były w specyfikacji danego systemu teleinformatycznego. Zapewniono także przejrzysty proces wdrażania zmian w systemach.

  Wystąpiły natomiast problemy w zakresie przestrzegania postanowień PBI IT w części dotyczącej rejestracji zmian oraz dokumentowania zrealizowanych analiz zasadności wdrożenia zmiany, ryzyka, wykonalności, kosztu, zysku, wpływu na pozostałe części systemu oraz możliwości weryfikacji tej zmiany. Pozytywnie należy ocenić monitorowanie systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności.
- **[Plan ciągłości działania]** Podjęto działania mające na celu wdrożenie planu ciągłości działania. Opracowano projekt zasad zapewnienia ciągłości działania oraz wykonano inwentaryzację procesów. Dalsze prace kontynuowane były przez Zespół ds. zarządzania ryzykiem. Planowano je zakończyć w IV kw. 2021 r.
- **[Rozliczalność działań]** Ministerstwo dokonywało przeglądów logów oraz prowadzono ich analizę w celu identyfikacji działań niepożądanych. Należy jednak zadbać o opracowanie całościowych regulacji zawierających zasady prowadzenia i wykorzystania dzienników systemów (logów), w tym określających zakres danych podlegających dokumentowaniu w dziennikach.

Wymiana informacji w postaci elektronicznej

- Pozytywnie należy ocenić proces realizacji 26 usług elektronicznych. Zapewniono komunikację elektroniczną przez skrzynkę podawczą na platformie ePUAP. Zarządzanie usługami odbywało się w oparciu o udokumentowane procedury, które zostały ujęte w umowach oraz w specyfikacji technicznej systemów. Komunikacja systemów umożliwiała wymianę danych z innymi systemami. Kodowanie znaków w dokumentach wysyłanych i odbieranych przez badane systemy, a także wymienianych informacji z innymi w drodze teletransmisji, było zgodne z wymogami Rozporządzenia KRI.

  MRiPS wykorzystywało 10 systemów teleinformatycznych do realizacji zadań publicznych[7]:
  - Centralny System Informatyczny Zabezpieczenia Społecznego (CSIZS);
  - Elektroniczny Krajowy System Monitorowania i Orzekania o Niepełnosprawności (EKSMOoN);
  - Portal Informacyjno-Usługowy Emp@tia (PIU Emp@tia);
  - Rejestr Żłobków (RZ);
  - System Centralny FEAD (SC FEAD);
  - System Informatyczny Karta Dużej Rodziny (SI KDR);
  - Rejestr Jednostek Pomocy Społecznej (RJPS);
  - System Elektronicznego Zarządzania Dokumentacją eDok;
  - Centralna Aplikacja Statystyczna (CAS);
  - Centralny System Analityczno-Raportowy (CeSAR).

  Badaniu poddano 3[8] z 10 wspomnianych systemów (30%), tj. CSIZS, PIU Emp@tia, SI KDR.

  CSIZS jest platformą komunikacyjną w obszarze zabezpieczenia społecznego i rodziny, umożliwiającą udostępnianie oraz świadczenie usług kompleksowej wymiany informacji za pośrednictwem Internetu, zarówno dla beneficjentów pomocy społecznej, świadczeń rodzinnych, funduszu alimentacyjnego, obszaru spraw osób niepełnosprawnych, jak również dla systemów teleinformatycznych wewnętrznych i zewnętrznych (systemy dziedzinowe, systemy innych ministerstw oraz instytucji).

  PIU Emp@tia jest „frontendem" systemu CSIZS, dzięki części usługowej umożliwia obywatelowi realizację usług elektronicznych poprzez złożenie wniosku i przesłanie go do organu właściwego. Zawiera także część informacyjną, która pozwala na uzyskanie informacji o: zniżkach i podmiotach realizujących usługi w ramach Karty Dużej Rodziny, ośrodkach i organizatorach turnusów rehabilitacyjnych, jednostkach pomocy społecznej, żłobkach i klubach dziecięcych.

  SI KDR umożliwia realizację zadań wynikających z ustawy o Karcie Dużej Rodziny[9] zapewniając w sposób kompleksowy ich obsługę.

OCENY I USTALENIA SZCZEGÓŁOWE

I. System zarządzania bezpieczeństwem informacji

1. [stan *SZBI*] Ministerstwo podejmowało szereg działań mających na celu zapewnienie bezpieczeństwa informacji, w szczególności w obszarze IT, co należy ocenić pozytywnie. Wdrożenie kompleksowego i spójnego *SZBI* wymaga jednak zmiany podejścia do jego ustanowienia. Proces ten powinien rozpocząć się od przeprowadzenia przeglądu, opracowania całościowej analizy ryzyka oraz kompleksowej dokumentacji, która jest warunkiem skutecznego zarządzania BI. W Jednostce wdrożono *Politykę Bezpieczeństwa Informacji w obszarze IT*[10], określającą istotne zagadnienia bezpieczeństwa informatycznego. Jednak *SZBI* to nie tylko obszar IT. Dopiero wdrożenie całościowych regulacji będzie stanowiło spełnienie wymogów § 20 ust. 1 *Rozporządzenia KRI*[11].

[7] Do Systemu Inwentaryzacji Systemów Teleinformatycznych został zgłoszony także system Adopcja, jednak nie był to system teleinformatyczny, a system dziedzinowy, wewnętrzny dedykowany do obsługi procesu adopcyjnego.
[8] Wybór próby nastąpił metodą doboru celowego, przy uwzględnieniu następujących kryteriów: istotność systemu dla działalności Ministerstwa; nakłady finansowe na system; podmiotowy zakres stosowania; zasięg terytorialny systemu (krajowy, lokalny); liczba użytkowników systemu.
[9] Ustawa z 5 grudnia 2014 r. (Dz. z 2020 r. poz. 1348, t. j. ze zm.).
[10] Wprowadzoną zarządzeniem nr 1 Dyrektora Generalnego Ministerstwa Rodziny, Pracy i Polityki Społecznej z dnia 9 stycznia 2020 r. *w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w obszarze IT MRPiPS*.
[11] 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.). Wejście w życie 31 maja 2012 r.

Od 9 stycznia 2020 r. w MRiPS obowiązywała *Polityka Bezpieczeństwa Informacji w obszarze IT* (dalej: PBI IT lub Polityka IT). Regulowała ona szereg zagadnień wspierających proces zapewnienia BI przetwarzanych w systemach informatycznych. Określała m.in. strategię bezpieczeństwa IT, zadania Departamentu Informatyki (dalej: DI), ogólne zasady ochrony i zabezpieczeń, naruszenia i postępowanie w przypadkach podejrzenia naruszeń PBI IT, ogólne zasady bezpieczeństwa fizycznego i środowiskowego, bezpieczeństwa komputerów przenośnych i pracy na odległość, bezpieczeństwa sprzętu i okablowania, w tym naprawy sprzętu, zarządzania systemami i sieciami, zasady tworzenia kopii zapasowych, korzystania z Internetu, Intranetu i poczty elektronicznej, zasady kontroli i monitorowania dostępu do systemu oraz zagadnienia dot. rozwoju i utrzymania systemu.

Zagadnienia te należy w szczególności uzupełnić o obszary dot. przeglądów *SZBI*; analizy ryzyka; audytu BI; bazy konfiguracji CMDB; wskazania wśród budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych[12] nie tylko nieruchomości, w których zlokalizowano urządzenia IT[13], a wszystkich, w których są przetwarzanie informacje, w tym pomieszczeń użytkowanych na potrzeby przechowywania dokumentacji; określenia całościowego celu strategicznego oraz zobowiązania do ciągłego doskonalenia całego *SZBI*[14].

Wyjaśniono[15], że elementy polityki BI ze względu na wielkość i złożoność obszaru zostały wprowadzone w życie w wielu regulacjach wewnętrznych, dotyczących bezpośrednio lub pośrednio tego obszaru. Zaznaczyć należy, że część wskazanych powyżej obszarów nie została uregulowana. Ponadto poszczególne regulacje wewnętrzne nie zawierały celów bezpieczeństwa informacji i zobowiązania do ciągłego doskonalenia. Ministerstwo szacowało[16], że wdrożenie kompleksowej dokumentacji *SZBI* będzie możliwe w perspektywie 6 miesięcy od zapoznania się z ostatecznymi wynikami kontroli.

Ustanowienie *SZBI,* który zapewnia poufność, dostępność i integralność informacji wymaga wdrożenia kompleksowych regulacji wewnętrznych gwarantujących sprawność jego działania. Dlatego MRiPS powinno zintensyfikować prace nad ich przygotowaniem uwzględniając wszystkie obszary BI. *SZBI* powinien być stale doskonalony, dlatego termin wprowadzenia całościowych regulacji nie powinien być uzależniony od zapoznania się z ostatecznymi wynikami kontroli. Jednostka powinna niezwłocznie podjąć niezbędne działania w tym zakresie.

2. W PBI IT wprowadzono liczne regulacje wspierające proces zarządzania infrastrukturą informatyczną. Wymaga ona dalszych aktualizacji / doprecyzowania, co uzasadnione jest nie tylko zmieniającym się otoczeniem, w tym zmianami organizacyjnymi Ministerstwa, ale także potrzebą precyzyjnego, niebudzącego wątpliwości interpretacyjnych odniesienia się do zagadnień, które określała.

PBI IT nie została zaktualizowana po przekształceniu Ministerstwa i odłączeniu działu administracji rządowej *praca*. Wyjaśniono[17] że, przekształcenie to miało charakter porządkujący i pozostawało bez wpływu na kluczowe aspekty regulujące bezpieczeństwo informatyczne.

W ocenie Ministerstwa należało jedynie dokonać zmian w załączniku nr 5[18] do Polityki IT poprzez usunięcie wniosku o nadanie / odebranie dostępu do Systemu Obsługi Wniosków i Administracji (SOWA) oraz w załączniku nr 22 poprzez usunięcie z *Wykazu Gestorów zbiorów i zasobów IT* systemów, które zostały przekazane do ówczesnego Ministerstwa Rozwoju, Pracy i Technologii[19].

Nie można się z tym zgodzić, bowiem oprócz wskazanych zagadnień PBI IT wymagała aktualizacji i zmiany, w szczególności w zakresie:

- ról dla głównych osób zaangażowanych w BI. PBI IT wprowadzała w słowniku pojęć funkcję *Arbitra* i Inspektora Bezpieczeństwa Teleinformatycznego (Inspektora IBT), które w tym miejscu zostały pozostawione omyłkowo (role te w rzeczywistości nie występowały).

[12] Załącznik nr 3 do PBI IT.
[13] Wyjaśnienia z 1 lipca 2021 r., znak: DI.III.081.5.13.2021.PW.
[14] Zgodnie z normą PN-EN ISO/IEC 27001 minimalnymi wymogami w zakresie ustanowienia polityki BI jest wdrożenie takiego dokumentu, który zawiera cele bezpieczeństwa informacji (nie tylko bezpieczeństwa informatycznego) lub tworzy ramy do ustanowienia bezpieczeństwa informacji oraz zawiera zobowiązanie do ciągłego doskonalenia całego *SZBI*.
[15] Pismo z 10 czerwca 2021 r., znak: BKA-II.081.23.10.2021.IK.
[16] Wyjaśnienia z 11 sierpnia 2021 r., znak: BKA-II.081.23.29.2021.IK.
[17] Pismo z 10 czerwca 2021 r., znak: BKA-II.081.23.5.2021.IK.
[18] *Wzór wniosku o dostęp do zasobów informatycznych MRPiPS.*
[19] Aktualnie Ministerstwo Rozwoju i Technologii.

Natomiast w załączniku nr 15[20] wprowadzono rolę Administratora Sieci Informatycznej, która nie była zdefiniowana w PBI IT, gdyż jak wyjaśniono[21] była tożsama z funkcją głównego specjalisty ds. sieciowej infrastruktury teleinformatycznej (GS ds. ICT). W załączniku nr 12[22] wprowadzono rolę Administratora Środowiska Wirtualnego, której nie wskazano w części PBI IT przedstawiającej wykaz ról związanych z zapewnieniem bezpieczeństwa;

- postanowień § 20 ust. 12 części II załącznika nr 1 wskazującego, że w przypadku nośników zawierających informacje niejawne są stosowane procedury określające postępowanie z informacjami niejawnymi, podczas gdy Pełnomocnik ds. Ochrony Informacji Niejawnych nie posiadał odrębnej procedury[23];
- funkcjonowania Komitetu Sterowania Bezpieczeństwem Informacji, który został zniesiony[24] 18 listopada 2019 r.;
- zarządzania incydentami, w tym m.in. ze względu na wprowadzenie 3 różnych definicji incydentów [szerzej pkt 14 *Wystąpienia*];
- stosowanego narzędzia do przekazywania wniosków o nadanie uprawnień. PBI IT[25] wskazywała niewykorzystywane narzędzie do ich przesyłania, tj. samoobsługowy system rejestracji zgłoszeń (http://serwis/maximo/ui/login), który był użytkowany do 9 marca 2021 r., natomiast nie określała wykorzystywanego od 2016 r. systemu eDok;
- doprecyzowania pomieszczeń wchodzących w skład strefy bezpieczeństwa. W PBI IT[26] wskazano ogólnie, że w skład strefy bezpieczeństwa wchodzą m.in. węzły dystrybucyjne. Ministerstwo posiadało 12[27] takich pomieszczeń, jednak przyjmowano, że spośród nich tylko główny punkt dystrybucyjny wchodzi w skład strefy bezpieczeństwa[28]. Ponadto w przypadku pozostawienia wszystkich węzłów dystrybucyjnych w strefie bezpieczeństwa, należy wyposażyć je w dodatkowe zabezpieczenia, m.in. związane z kontrolą dostępu;
- doprecyzowania § 26 ust. 3 części II załącznika nr 1 – w przepisie tym wskazano, że *wszystkie zmiany w systemie mogą być wprowadzane jedynie w oparciu o procedury tworzone osobno i zatwierdzone jednorazowo przez Dyrektora Departamentu Informatyki.* Zatem przepis ten można zinterpretować w ten sposób, że w przypadku każdej zmiany tworzone są procedury jej wdrożenia, które podlegają zatwierdzeniu przez Dyrektora DI. W praktyce wymóg ten realizowany był poprzez opracowanie *Procedury rozwoju* stanowiącej załącznik do umowy utrzymania w sprawności i rozwoju systemu, a następnie podpisanie umowy, tj. zatwierdzenie tej *Procedury*;
- zdefiniowania pojęcia *informacji wrażliwej i systemu wrażliwego*. PBI IT posługuje się tymi pojęciami, jednakże w słowniku terminów i skrótów nie określono, że są one rozumiane w myśl przepisów RODO[29], jako szczególna kategoria danych osobowych oraz system przetwarzający te dane. Wyjaśniono[30], że jest to pojęcie prawne, powszechnie stosowane, dlatego nie definiowano go ponownie. Wskazać jednak należy, że RODO posługuje się nieco odmiennym pojęciem *danych wrażliwych*. Ponadto niezależnie od tego, w celu zapewnienia przejrzystości regulacji, zasadnym jest doprecyzowanie pojęć, by nie budziły wątpliwości interpretacyjnych, w szczególności poprzez wskazanie, że dane pojęcie jest rozumiane w myśl określonych przepisów prawa;
- zmiany zasad przeprowadzania klasyfikacji informacji. Wdrożono procedurę *Klasyfikacji informacji w MRPiPS*[31], jednakże wprowadzała ona jedynie 2 klauzule wrażliwości: *informacje wewnętrzne* oraz *informacje jawne*. Taki podział informacji jest niewystarczający do spełnienia celu, tj. zapewnienia przypisania informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Jednostki. Wskazać należy, że zgodnie z normą PN-EN ISO/IEC 27001[32], informacje powinny być sklasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. Wyjaśniono[33], że nie wdrożono i nie przyjęto do stosowania powyższej normy, dlatego klasyfikacja informacji jest prowadzona zgodnie z wprowadzoną procedurą. Zaznaczyć jednak należy, że § 20 ust. 3 Rozporządzenia KRI wskazuje na spełnienie

[20] *Postępowanie w przypadku wyłączenia zasilania*.
[21] Pismo z 10 czerwca 2021 r., znak: BKA-II.081.23.5.2021.IK.
[22] *Funkcjonowanie środowiska testowego w MRPiPS.*
[23] Wyjaśnienia z 10 czerwca 2021 r., znak: BKA-II.081.23.5.2021.IK.
[24] Zarządzeniem nr 11 Dyrektora Generalnego z dnia 18 listopada 2019 r. w sprawie zniesienia Komitetu Sterującego Bezpieczeństwem Informacji w obszarze IT.
[25] Załącznik nr 5 do PBI IT.
[26] § 7 ust. 6 części II załącznika nr 1 do PBI IT.
[27] Zgodnie z *Wykazem serwerowni i punktów dystrybucyjnych w MRiPS*.
[28] Wyjaśnienia z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[29] 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.).
[30] Pismo z 27 lipca 2021 r., znak: BKA-II.081.23.20.2021.IK.
[31] Załącznik nr 21 do PBI IT.
[32] Pkt. A.8.2 załącznika A normy.
[33] Pismo z 27 lipca 2021 r., znak: BKA-II.081.23.20.2021.IK.

wymagań dot. *SZBI*, jeśli system ten został opracowany na podstawie powyższej normy. Zatem Jednostka powinna uwzględniać obowiązki w niej określone.

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

3. [nadzór Kierownictwa i analiza/przegląd *SZBI*] Nadzór nad *SZBI* był rozproszony i nie wszystkie obszary systemu zostały nim objęte, w szczególności dotyczące przeglądów *SZBI*, analizy ryzyka, audytu BI oraz bazy konfiguracji CMDB. Nie wyznaczono osoby sprawującej nadzór nad całościowym funkcjonowaniem *SZBI*[34], a odpowiedzialności, zadania i kompetencje powierzono wybranym kierownikom komórek organizacyjnych.

W latach 2019-2020 przygotowano projekty zmian organizacyjnych, które m.in. skupiałyby kwestię nadzoru nad funkcjonowaniem *SZBI* w jednej komórce organizacyjnej, ale ze względu na inne priorytety Kierownictwa Ministerstwa, prac nie kontynuowano[35].

Nie można zgodzić się, że nadzór nad wszystkimi obszarami *SZBI* został przypisany wybranym kierownikom komórek organizacyjnych. Obszary dot. przeglądów *SZBI*, analizy ryzyka, audytu BI, bazy konfiguracji CMDB, nie zostały uregulowane. Zatem nadzór i zadania dot. ich realizacji również nie zostały przypisane żadnej osobie / komórce organizacyjnej.

4. Brak zbiorczych informacji, które są kluczowe w procesie zarządzania, nie wspierał Ministerstwa we wdrażaniu *SZBI*. Nie przeprowadzono całościowej analizy aktualnego stanu BI, umożliwiającej opracowanie planu/strategii rozwoju *SZBI.* Kierownictwo Ministerstwa nie posiadało zatem instrumentów do weryfikacji podejmowanych działań służących wdrażaniu tego systemu.

MRPiPS, a następnie MRiPS podejmowało działania w zakresie doskonalenia *SZBI*, z uwzględnieniem informacji przekazanych w piśmie Szefa KPRM[36] dot. najważniejszych i najczęściej powtarzających się nieprawidłowości w obszarze *SZBI*, jednak bez analizy stanu BI nie można stwierdzić, czy były one odpowiedzią na najpilniejsze potrzeby Jednostki.

Podjęte działania służące poprawie BI, w szczególności dot. zweryfikowania: realizacji zaleceń poaudytowych, procedury nadawania ról i uprawnień oraz wewnętrznych zasad informowania o incydentach, spójności i kompletności systemu tworzenia kopii zapasowych, postanowień umownych i ewentualnego uzupełnienia ich o klauzule dot. bezpieczeństwa, dostępności, praw autorskich, warunków SLA i tajemnicy, zabezpieczeń techniczno-organizacyjnych dostępu do stref chronionych, rozliczalności działań administratorskich oraz wdrożenia mechanizmów bezpieczeństwa związanych z pracą zdalną. Działania te nie zostały jednak poprzedzone analizą stanu BI, dlatego nie można ocenić, czy stanowiły one realizację najpilniejszych potrzeb Ministerstwa.

Wyjaśniono[37], że analiza stanu BI realizowana jest w sposób rozproszony, na podstawie poszczególnych procedur. Dotychczas nie przyjęto rozwiązania, zgodnie z którym analiza miałaby objąć jednocześnie wszystkie aspekty funkcjonowania *SZBI*. Podejmowanie działań usprawniających oraz wyznaczanie kierunków rozwoju *SZBI* wynika z pojawiających się nowych rozwiązań prawnych, organizacyjnych, a narzędzia nadzorcze projektowane i wdrażane są w regulacjach wewnętrznych. Zaznaczono[38] także, że inicjatywy i wprowadzane zmiany w tym obszarze zależały m.in. od poszczególnych członków kierownictwa, w tym dyrektora generalnego.

Skuteczne wdrażanie *SZBI* wymaga diagnozy istniejących rozwiązań. Pozwoliłaby ona na opracowanie planu/strategii wdrażania *SZBI*, określającego m.in. planowane działania, termin ich wdrożenia oraz osoby odpowiedzialne za ich realizację. Identyfikacja słabości i opracowanie planu/strategii przyczyniłyby się do skuteczniejszego zarządzania obszarem BI, bowiem dokument taki umożliwiłby także hierarchizację działań do podjęcia. Ułatwiłoby

[34] Pisma z 10 czerwca 2021 r., znak: BKA-II.081.23.5.2021.IK.
[35] Pismo z 11 sierpnia 2021 r., znak: BKA-II.081.23.29.2021.IK.
[36] Pismo z 5 sierpnia 2019 r., znak: COA.WK.588.1.2019.MF, *Informacja o najważniejszych i najczęściej powtarzających się nieprawidłowościach stwierdzonych w wyniku kontroli przeprowadzonych przez KPRM w zakresie wykorzystania systemów teleinformatycznych do realizacji zadań publicznych.*
[37] Wyjaśnienia z 11 sierpnia 2021 r., znak: BKA-II.081.23.29.2021.IK.
[38] Wyjaśnienia z 15 czerwca 2021 r., znak: BKA-II.081.23.7.2021.IK.

to analizę i ocenę wdrażanych rozwiązań. Kierownictwo Ministerstwa posiadałoby również narzędzie zarządcze do podejmowania adekwatnych decyzji.

5. [analiza ryzyka] W MRiPS realizowano czynności dot. szacowania ryzyka, jednak były one prowadzone na potrzeby kontroli zarządczej. Identyfikowano ryzyka w stosunku do zadań, podczas gdy celem analizy ryzyka BI, powinna być w pierwszej kolejności ocena ryzyk związanych z utratą integralności, dostępności lub poufności. Ponadto analizą ryzyka powinny być objęte wszystkie aktywa jednostki. Z tego powodu nie można uznać, że działania te stanowiły spełnienie wymogów § 20 ust. 2 pkt 3 *Rozporządzenia KRI*. Brak przeprowadzenia analizy ryzyka BI skutkował tym, że nie opracowano też planu postępowania z ryzykiem. Jednostka zaznaczyła, że w maju br. powołano zespół ds. zarządzania ryzykiem[39] i kwestie BI będą przedmiotem jego prac.

> W Ministerstwie nie wdrożono regulacji dot. zarządzania ryzykiem BI. Szacowanie ryzyka wykonywane było przez poszczególne komórki na podstawie *zarządzenia w sprawie kontroli zarządczej*[40]. Regulacja ta nie mogła stanowić podstawy do sporządzenia kompleksowej analizy ryzyka BI, ponieważ wynika to z przyjętej w niej metodologii identyfikacji oraz szacowania ryzyka. Zgodnie z tym zarządzeniem komórki zobowiązane są do identyfikacji ryzyka w odniesieniu do realizowanych zadań oraz ochrony danych osobowych[41]. Identyfikowane są ryzyka związane ze zmianami w organizacji, zagrażające wizerunkowi, o charakterze finansowym, korupcyjnym, legislacyjnym, dot. zasobów ludzkich. Ocena ryzyk w odniesieniu do 6[42]z 10 systemów teleinformatycznych dot. tylko ochrony danych osobowych.
>
> Natomiast celem analizy ryzyka BI jest odniesienie jej do wszystkich aktywów jednostki (nie tylko danych osobowych) oraz dokonanie oceny ryzyk związanych z utratą integralności, dostępności lub poufności informacji. Wyjaśniono[43], że w MRiPS nie ma regulacji, która wprost nakazuje przeprowadzić analizę ryzyka BI jako odrębnego obszaru działania Jednostki.
>
> W związku z wymogiem audytora Ministerstwa Finansów przy certyfikacji Systemu Centralnego FEAD wdrożono *Metodykę zarządzania ryzykiem w zakresie bezpieczeństwa informacji SC FEAD* i na jej podstawie przeprowadzono analizę ryzyka tego systemu[44]. Jednak działania te nie były podejmowane na potrzeby *SZBI*, a wynikały z obowiązków Programu Operacyjnego Pomoc Żywnościowa 2014-2020. Analizę ryzyka i metodykę zawarto w PBI IT, co wynikało z wymagań audytora Ministerstwa Finansów oraz specyfiki tego Programu.

Analiza ryzyka BI jest jednym z najistotniejszych elementów ustanowienia *SZBI*. Pozwala na proaktywne zarządzanie bezpieczeństwem informacji, w tym przeciwdziałanie zagrożeniom oraz ograniczanie skutków w przypadku zmaterializowania się ryzyk. Z tego powodu proces ten powinien być cykliczny, a dodatkowe działania powinny być podejmowane w sytuacjach zmieniającego się otoczenia.

6. [audyt] W Ministerstwie przeprowadzono audyt BI, skupiając się na badaniu bezpieczeństwa infrastruktury teleinformatycznej. Tym samym nie objęto badaniem wszystkich obszarów bezpieczeństwa informacji. Rozszerzenie jego zakresu zapewniłoby pełną identyfikację słabości *SZBI* i wspierałoby Jednostkę w ich eliminacji.

> Czynności eksperckie[45] dot. *badania bezpieczeństwa infrastruktury teleinformatycznej*. wykonała firma zewnętrzna. Dotyczyły one w szczególności ogólnej analizy komunikacji sieciowej z poziomu Internetu, skanowania portów[46], prób detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z Internetu, skanowania podatności na aktywnych hostach z badanej sieci publicznej, zewnętrznego testowania serwerów http. Audyt ten nie objął zatem wszystkich obszarów *SZBI*[47].

---

[39] Prace rozpoczęły się w czerwcu.
[40] Zarządzenie nr 10 Ministra Rodziny i Polityki Społecznej z dnia 10 marca 2021 r. w sprawie kontroli zarządczej w MRiPS oraz obowiązków jednostek podległych i nadzorowanych w ramach kontroli zarządczej.
[41] Przy czym oceny zidentyfikowanego ryzyka w obszarze danych osobowych również dokonuje się pod względem wpływu na realizację celów i zadań z uwzględnieniem kryteriów wskazanych w zarządzeniu.
[42] CSIZS, EKSMOoN, PIU Emp@tia, Rejestr Żłobków, SI KDR, RJPS.
[43] Pismo z 9 lipca 2021 r., znak: BKA-II.081.23.14.2021.IK.
[44] Metodyka oraz przeprowadzona na jej podstawie analiza ryzyka stanowiły załącznik nr 25 do PBI IT.
[45] *Sprawozdanie z przeprowadzenia czynności eksperckich* z 2 grudnia 2020 r., sporządzone przez firmę Grant Thornton Sp. z o.o. Sp. k.
[46] Próby wykrycia usług sieciowych/urządzeń sieciowych dostępnych z poziomu Internetu.
[47] M.in. przeglądów *SZBI*, analizy ryzyka, posiadania aktualnych informacji w zakresie sprzętu i oprogramowania, zarządzania uprawnieniami, organizacji szkoleń, pracy na odległość, umów w zakresie serwisu i rozwoju systemów informatycznych /teleinformatycznych, zarządzania incydentami, tworzenia i testowania kopii zapasowych, projektowania, wdrażania, wprowadzania zmian systemów teleinformatycznych, zabezpieczeń organizacyjno-technicznych dostępu do informacji, rozliczalności działań użytkowników, tworzenia planów ciągłości działania oraz realizacji usług elektronicznych.

Wyjaśniono[48], że audyt wewnętrzny w pełnym zakresie nie został zrealizowany, ponieważ w *Planie audytu wewnętrznego na 2021 r.* znalazło się 19 obszarów ryzyka, a na samodzielnych stanowiskach audytu wewnętrznego zatrudnionych jest 3 audytorów wewnętrznych. Powołano się także na wspólne stanowisko Ministerstwa Administracji i Cyfryzacji oraz Ministerstwa Finansów[49] wskazujące, że nie należy automatycznie przypisywać zadania audytu w zakresie bezpieczeństwa informacji komórce audytu wewnętrznego.

W *Planie audytów wewnętrznych na 2021 r.* uwzględnione zostało zadanie zapewniające pn. *Systemy informatyczne*, jednakże jego szczegółowy zakres zostanie określony w programie zadania audytowego. Realizacja audytu planowana jest w IV kw. 2021 r.

Realizacja audytu w niepełnym zakresie utrudnia osiągnięcie celu audytu, w tym nie pozwala na skuteczną identyfikację potencjalnych słabości lub zagrożeń bezpieczeństwa informacji.

7. Prawidłowo monitorowano stopień wykonania rekomendacji audytu i częściowo je wdrożono. Konieczna jest również realizacja zalecenia audytu przeprowadzonego w 2019 r., które nie zostało wykonane, tj. uzupełnienie dokumentu pn. *Tryb kompleksowego i cyklicznego badania podatności w obrębie infrastruktury informatycznej MRPiPS*.

W Ministerstwie w 2019 r. przeprowadzono audyt wewnętrzny Bezpieczeństwa teleinformatycznego MRPiPS[50]. Realizacja zaleceń tego audytu była monitorowana i podlegała także ocenie w toku czynności eksperckich przeprowadzonych w 2020 r. W wyniku przeprowadzonego w 2019 r. audytu sformułowano 2 zalecenia. Pierwsze dot. określenia trybu kompleksowego i cyklicznego badania podatności w obrębie infrastruktury informatycznej. Kolejne – wdrożenia cyklicznych działań w zakresie skanowania, których celem miało być badanie aktualnego stanu bezpieczeństwa w związku z pojawianiem się nowych zagrożeń. Ponadto rekomendowano by wyniki tych testów poddawać szczegółowej analizie, a w razie konieczności podejmować działania usprawniające badany obszar.

MRiPS wdrożyło drugie zalecenie, tj. sporządzano raporty z badania podatności systemów. Podatności, które zostały w nich wskazane były usuwane przez wykonawców umów zajmujących się utrzymaniem systemów, a następnie ponawiano testy podatności.

Pierwsze zalecenie wdrożono częściowo. Opracowano dokument *Tryb kompleksowego i cyklicznego badania podatności w obrębie infrastruktury informatycznej MRPiPS*, jednak, w ocenie czynności eksperckich, składał się on z 10 punktów, nie był datowany, właściciel dokumentu nie został oznaczony, na dokumencie nie było akceptacji uprawnionej osoby i przyjęcia do użytkowania. Dokument zawierał w treści szczątkowe informacje na temat kluczowych kroków składających się na podstawowy proces zarządzania podatnościami[51]. Ekspert zalecił podjęcie dalszych działań w celu kompletnego wdrożenia zalecenia.

Dokument został zatwierdzony przez Dyrektora DI 11 stycznia 2021 r. i przyjęty do wykonywania przez pracowników. Nie został on jednak uszczegółowiony zgodnie z zaleceniem, tj. dodano do jego treści tylko możliwość badania podatności bezpieczeństwa teleinformatycznego także innymi narzędziami niż dotychczas stosowane oraz zmieniono cykliczność badania podatności (z raz na kwartał na raz na pół roku). Wyjaśniono[52], że zalecenie zostało potraktowane przez DI, jako dotyczące realizacji wskazanej procedury na poziomie wykonawczym, a zatwierdzony dokument zawiera główne czynności administratorów wykonujących badanie podatności systemów.

Ocena czynności eksperckich dotyczyła opracowanego dokumentu. Zatem podejmowane działania w obszarze badania podatności, pomimo że wspierają proces zapewnienia BI, nie są wystarczające do realizacji zalecenia audytu. Opracowanie przejrzystej dokumentacji dot. bezpieczeństwa informacji zapewnia sprawność działania *SZBI* i stanowi istotny jego element.

8. **[baza CMDB]** Ministerstwo prowadziło inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji. Do spełnienia wymogów § 20 ust. 2 pkt 2

[48] Wyjaśnienia z 6 lipca 2021 r., znak; BKA-II.081.23.10.2021.IK.
[49] Wspólne stanowisko Departamentu Informatyki MAiC oraz Departamentu Audytu Sektora Finansów Publicznych MF, opublikowane pod adresem: https://mf-arch2.mf.gov.pl/web/bip/ministerstwo-finansow.
[50] Badanie bezpieczeństwa infrastruktury IT z wykorzystaniem specjalistycznego narzędzia do badania podatności.
[51] Dot. *przygotowania systemów do skanowania podatności, skanowanie podatności, definiowanie planu naprawczego, wdrożenie planu naprawczego, ponownego skanowania podatności.*
[52] Pismo z 13 lipca 2021 r., znak: DI.III.081.5.16.2021.PW.

Rozporządzenia KRI wymagane jest ujęcie w ewidencjach / rejestrach wszystkich aktywów informatycznych i wskazanie relacji pomiędzy elementami konfiguracji.

MRiPS w zakresie inwentaryzacji sprzętu i oprogramowania dysponowało: wykazem serwerowni, wykazem sprzętu komputerowego[53], wykazem urządzeń mobilnych oraz ewidencjami aktywów informacyjnych przetwarzających informacje w sposób cyfrowy[54]. Dokumenty te nie obejmowały jednak wszystkich zidentyfikowanych aktywów informatycznych (np. drukarek, urządzeń wielofunkcyjnych, pendrive'ów, modemów, sprzętu do wideokonferencji). Ponadto nie zawierały danych o oprogramowaniu (w wykazie sprzętu komputerowego wskazano jedynie system operacyjny) i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji.

W opinii[55] Ministerstwa wdrożenie dedykowanego narzędzia kompleksowej, relacyjnej bazy danych CMDB, jest jednym z możliwych rozwiązań ale nie jedynym. Kierując się koniecznością zapewnienia redukcji kosztów wybrano inny sposób gromadzenia tych informacji, przy jednoczesnym spełnieniu warunku zapewnienia ich autentyczności, rozliczalności, niezaprzeczalności i niezawodności. Zdaniem Kontrolowanego Rozporządzenie KRI nie wskazuje na obowiązek prowadzenia i aktualizacji bazy konfiguracji CMDB jako sposobu realizacji zawartych w nim wymagań.

W *Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych*[56] w pkt. 2.3. *Inwentaryzacja sprzętu i oprogramowania informatycznego* wskazano, że spełnienie powyższego wymogu oznacza w praktyce posiadanie rejestru zasobów teleinformatycznych (zwanego bazą konfiguracji CMDB). Powinien on zawierać 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.

Przekazane ewidencje / rejestry wymagają uzupełnienia o powyższe elementy dla zapewnienia zgodności z wymogami Rozporządzenia KRI. Nie jest kwestionowany brak dedykowanego specjalistycznego narzędzia do zarządzania infrastrukturą IT, a fakt, że przyjęte przez Ministerstwo rozwiązania nie zapewniają pełnych informacji w tym zakresie. Wybór konkretnego rozwiązania dot. sposobu prowadzenia i aktualizacji inwentaryzacji sprzętu i oprogramowania informatycznego leży w gestii każdej Jednostki. Nie jest ona zobowiązana do korzystania z dedykowanego narzędzia.

Brak kompletnego rejestru aktywów informatycznych uniemożliwia przeprowadzenie rzetelnej analizy ryzyka i przygotowanie planu postępowania z ryzykiem.

9. PBI IT odnosiła się do zarządzania infrastrukturą informatyczną, określając obowiązek ewidencji zasobów informacyjnych, do których należały także aktywa informatyczne. Uzupełnienia wymaga wskazanie sposobu i zakresu gromadzonych danych.

W PBI IT[57] wprowadzono obowiązek ewidencji aktywów informacyjnych przetwarzających informacje w sposób cyfrowy. Za aktywa informacyjne uznano[58] wszelkie zasoby będące informacją i nośnikiem informacji istotne z puntu widzenia Ministerstwa, do których Jednostka posiada prawo majątkowe, m.in. papier, nośniki elektroniczne, bazy danych, komputery osobiste (notebooki, laptopy), systemy informatyczne, systemy operacyjne, serwery, archiwa tradycyjne i cyfrowe. Ewidencje te były prowadzone przez komórki organizacyjne.

Słabością tych regulacji był jednak brak postanowień dot. sposobu i zakresu gromadzonych danych, w szczególności w odniesieniu do aktywów informatycznych. Wyjaśniono[59], że nie wprowadzono regulacji określających wymagania dot. prowadzenia i aktualizacji bazy konfiguracji CMDB, bowiem Ministerstwo nie wykorzystuje narzędzia jakim jest hurtownia danych CMDB.

[53] Zakres danych zestawienia sprzętu komputerowego: rodzaj, nazwa, pełna nazwa, nr inwentarzowy, nr fabryczny, nazwisko i imię, dep./biuro, lokalizacja, wartość, data zakupu lub przekazania, system operacyjny (zakupiony), system zainstalowany.
[54] Ewidencje prowadzone przez poszczególne komórki MRiPS. Kontroli poddano ewidencje z 7 komórek organizacyjnych, tj.: z Departamentu Analiz Ekonomicznych; Departamentu Informatyki; Departamentu Polityki Rodzinnej; Departamentu Prawnego; Biura Administracyjnego; Biura Ministra; Biura Pełnomocnika Rządu do Spraw Równego Traktowania.
[55] Pismo z 11 sierpnia 2021 r., znak: BKA-II.081.23.29.2021.IK.
[56] Z 15 grudnia 2015 r., strona 23. Opublikowane na: https://mc.bip.gov.pl/wytyczne/wytyczne-dla-kontroli-dzialania-systemow-teleinformatycznych-uzywanych-do-realizacji-zadan-publicznych.html.
[57] § 8 ust. 1 część I załącznika nr 1 do PBI IT.
[58] Słownik terminów i skrótów w części I załącznika nr 1 do PBI IT.
[59] Pismo DI.III.081.5.13.2021.PW z 1 lipca 2021 r.

Wybór konkretnego sposobu prowadzenia i aktualizacji inwentaryzacji sprzętu i oprogramowania informatycznego należy do MRiPS. Natomiast przyjęte rozwiązania / zasady powinny zostać określone w regulacjach wewnętrznych. Zapewniłoby to wsparcie dla osób zaangażowanych w ten proces w efektywnej realizacji zadań.

10. [uprawnienia] W Ministerstwie wdrożono regulacje wspierające proces nadawania uprawnień i zapewniające przejrzystość działań w tym obszarze. Wymagają one jedynie aktualizacji w zakresie narzędzia wykorzystywanego do przesyłania i rejestrowania wniosków o nadanie / zmianę uprawnień. Przyjęte natomiast rozwiązania dotyczące odbierania uprawnień nie gwarantują ich skuteczności, przez co niespełniony pozostaje wymóg § 20 ust. 2 pkt 5 Rozporządzenia KRI. Odbieranie uprawnień następuje ze znacznym opóźnieniem w odniesieniu od momentu zakończenia stosunku pracy.

> PBI IT regulowała proces nadawania uprawnień. Kierownik komórki, w której zatrudniony był pracownik określał zakres uprawnień, ograniczając je do niezbędnego minimum, potrzebnego na danym stanowisku. Wnioski elektroniczne były przekazywane do DI, a uprawnienia nadawane przez administratorów poszczególnych systemów. Regulacja ta wprowadzała także wzory wniosków. Zawarto w niej odwołanie do niewykorzystywanego narzędzia służącego do ich przesyłania, tj. samoobsługowego systemu rejestracji zgłoszeń (http://serwis/maximo/ui/login), który użytkowano do 9 marca 2021 r. PBI IT nie określała natomiast używanego od 2016 r. systemu eDok, który służył jako podstawowe narzędzie do ich przekazywania. Wyjaśniono[60], że wszystkie wnioski były przesyłane i rejestrowane w systemie eDok. Użytkownicy korzystali z systemu http://serwis/maximo/ui/login sporadycznie. Zadeklarowano, że postanowienia PBI IT w tym zakresie zostaną zmienione przy najbliższej aktualizacji dokumentu.
>
> Podstawą odebrania uprawnień był wniosek o odebranie / cofnięcie uprawnień. Zgodnie z PBI IT powinien on niezwłocznie zostać przesłany do DI przez komórkę, w której zatrudniony był pracownik. Uprawnienia cofane były w dniu otrzymania takiego wniosku w eDok przez administratora systemu. Przyjęta zasada, ze względu na brak wyznaczenia terminu przekazania takiego wniosku, nie gwarantowała niezwłocznego odebrania uprawnień, w przypadkach zakończenia świadczenia pracy. Wskazano[61], że każdy pracownik w związku z ustaniem zatrudnienia obowiązany jest do niezwłocznego zwrotu i rozliczenia się ze sprzętu, co musi zostać potwierdzone na karcie obiegowej. Wg MRiPS dla pracowników DI było to równoznaczne z koniecznością odebrania uprawnień pracownikowi.
>
> W okresie maj-czerwiec 2021 r. stosunek pracy w Jednostce zakończyło 18[62] pracowników. Tylko w 2 przypadkach odebranie uprawnień nastąpiło z dniem zakończenia zatrudnienia albo przed tym dniem. W pozostałych 7 przypadkach uprawnienia cofnięto w terminie do 3 dni roboczych od zakończenia zatrudnienia, w 3 przypadkach do 9 dni roboczych, natomiast w pozostałych 6 opóźnienie w zakresie cofnięcia uprawnień było znaczne i wyniosło od 43 do 62 dni roboczych. Zatem mimo obowiązku rozliczenia się ze sprzętu, uprawnienia nie były niezwłocznie cofane.

Wdrożone działania w zakresie cofania uprawnień nie zapewniły niezwłocznego ich odebrania, co wymaga wdrożenia skutecznego rozwiązania.

11. W trzech badanych systemach uprawnienia nadawano prawidłowo, zgodnie z kompetencjami pracowników oraz uprawnieniami wykonawców umów dotyczących utrzymania i rozwoju danego systemu. Funkcjonalności systemów pozwalały na nadanie różnego ich zakresu, a zasada ograniczenia uprawnień do niezbędnego minimum potrzebnego do realizacji zadań była stosowana. Pracownikom zablokowano dostęp do elementów narzędziowych systemów, co zapobiegało wprowadzaniu w nich niepożądanych zmian. W przypadku wykonawców umów mieli oni dostęp jedynie do „swojego" systemu, ponieważ były one od siebie rozdzielone na poziomie sieci.

> Uprawnienia do 3 badanych systemów w pełnym zakresie nadawane były wyłącznie osobom odpowiedzialnym za administrowanie systemami, natomiast pozostałym zostały ograniczone do niezbędnego minimum potrzebnego do realizacji zadań. Badane systemy gromadziły także

[60] Pismo z 28 lipca 2021 r., znak: DI.III.081.5.26.2021.PW.
[61] Pismo z 28 lipca 2021 r., znak: DI.III.081.5.26.2021.PW.
[62] Łącznie z pracownikami przeniesionymi w trybie art. 64 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. u. z 2021 r. poz. 1233, tj.), w przypadku których jako datę zakończenia stosunku pracy uznano ostatni dzień, w którym członek ksc figurował jako pracownik MRiPS.

informacje o zakresach nadanych uprawnień, niezależnie od złożonych wniosków przechowywanych w eDok. W przypadku tych systemów utworzone zostało także awaryjne konto techniczne administratora centralnego, do którego login i hasło zostało zdeponowane w zabezpieczonym miejscu.

Dostępem do elementów narzędziowych systemów dysponowali wyłącznie pracownicy Wydziału Przetwarzania Danych oraz wykonawca umowy odpowiedzialny za utrzymanie i rozwój danego systemu. Wdrażane przez wykonawcę zmiany były nadzorowane przez ASI danego systemu przy współpracy z pracownikami Wydziału Przetwarzania Danych.

Wykonawcy umów dot. utrzymania i rozwoju danego systemu składali wniosek o nadanie uprawnień dla swojego personelu realizującego przedmiot umowy wraz z oświadczeniami tych osób o zapoznaniu się i zobowiązaniu do przestrzegania zasad, reguł i postanowień zawartych w Wyciągu z PBI IT. Na tej podstawie tworzone były dla nich konta. We wniosku wskazywany był okres, na jaki ma być utworzone konto – maksymalny to czas trwania umowy. W umowach wskazywana była również miesięczna gwarancja, zatem w tym okresie, w przypadkach awarii, wykonawca mógł także uzyskać dostęp do systemu. Systemy były od siebie rozdzielone na poziomie sieci, zatem wykonawca miał dostęp tylko do „swojego" systemu. Dostęp do niego następował za pomocą szyfrowanego połączenia VPN.

12. Dokumentowania wymagają analizy aktywności użytkowników oraz kontrola spójności treści wniosków nadanych uprawnień z ich faktycznym zakresem w trzech badanych systemach.

Regulacje[63] MRiPS wprowadzały obowiązek okresowej kontroli spójności treści wniosków określających zakres uprawnień z ich zakresem nadanym w systemach. Wyjaśniono[64], że kontrole takie odbywają się częściej niż raz w roku w związku ze zmianami w strukturze organizacyjnej komórek Ministerstwa oraz zmianami w systemach. W ocenie Ministerstwa[65] dokumentowanie procesu kontroli spójności byłoby działaniem nadmiarowym.

Ponadto PBI IT[66] dla administratorów systemów wprowadzała obowiązek weryfikacji uprawnień nadanych użytkownikom przynajmniej raz w ciągu dwóch lat. Weryfikacja ta w stosunku do 3 badanych systemów polegała na analizie aktywności użytkowników. Jeżeli użytkownik nie logował się do systemu w okresie dłuższym niż rok, jego konto było blokowane. Z procesu tego nie były sporządzane formalne dokumenty, z wyjątkiem statystki usuniętych kont. Wskazano, że przyjęcie tej zasady pozwala na zapewnienie większej efektywności działań pracowników DI oraz pozwala zapewnić na racjonalnym poziomie zatrudnienie i ponoszone przez MRiPS koszty osobowe.

Nie można zgodzić się, że dokumentowanie czynności podejmowanych w ramach kontroli spójności byłoby działaniem nadmiarowym. Nadawanie właściwych uprawnień wspiera zapewnienie BI, dlatego czynności kontrolne w tym zakresie powinny być dokumentowane. Dokumentowanie jest również ważne z perspektywy nadzoru oraz efektywnego doskonalenia procesu nadawania uprawnień. W odniesieniu do prowadzonych analiz aktywności użytkowników nie można zgodzić się, że sporządzenie wykazu z danymi nt. usuniętych kont raz w roku wymagałoby zwiększenia zatrudnienia i ponoszenia dodatkowych kosztów osobowych.

13. Zarządzanie hasłami w badanych systemach było realizowane prawidłowo, tj. stosowano zasady złożoności hasła, jego okresowej zmiany oraz ochrony przed udostępnieniem. Zasadnym byłoby wdrożenie rozwiązań w zakresie blokowania dostępu do konta ASI badanych systemów po określonej liczbie prób błędnego logowania. Praktyka nadawania identyfikatorów pozwalała na ustalenie użytkowników, choć uzasadnionym byłoby wprowadzenie jednolitych zasad w zakresie ich tworzenia.

Badane systemy[67] wymuszały złożoność hasła, okresową jego zmianę, natomiast w przypadku pierwszego logowania zmianę hasła nadanego przez administratora. Określono czas aktywności sesji, po upływie którego systemy rozłączały się, a dostęp do nich wymagał ponownego logowania. Dodatkowo CSIZS i PIU Emp@tia zapamiętywały 5 ostatnich haseł, zapobiegając ich ponownemu wykorzystaniu. SI KDR nie miał takiej funkcjonalności. Uniemożliwiał tylko ponowne wykorzystanie bieżącego hasła. Systemy te nie posiadały

[63] Postanowienia końcowe załącznika nr 5 do PBI IT.
[64] Pismo z 28 lipca 2021 r., znak: DI.III.081.5.26.2021.PW.
[65] Pismo z 28 lipca 2021 r., znak: DI.III.081.5.26.2021.PW.
[66] § 22 ust. 23 część II załącznika nr 1 do PBI IT.
[67] PIU Emp@tia, SI KDR, CSIZS.

funkcjonalności blokowania dostępu po kilku nieudanych próbach logowania, tj. SI KDR blokował taki dostęp po 5 nieudanych próbach, jednak blokada następowała na 10 minut i po upływie tego czasu użytkownik posiadał ponowną możliwość logowania. Tej funkcji nie miały CSIZS i PIU Emp@tia[68].

Wyjaśniono[69], że w zakresie CSIZS MRiPS rozważy wprowadzenie funkcjonalności blokady dostępu dla administratorów po określonej liczbie błędnych prób logowania. Zasadnym jest jednak wprowadzenie takich rozwiązań dla wszystkich systemów.

MRiPS nie wdrożyło jednolitych zasad nadawania identyfikatora użytkownika. W przypadku badanych systemów nazwa użytkownika nie mogła tylko zawierać spacji ani być tożsama z już istniejącą. Każdy użytkownik posiadał niepowtarzalny identyfikator dostępności do systemu, ale sposób jego ustalania był różny. Z reguły składał się on z imienia i nazwiska, imienia i pierwszej litery nazwiska bądź pierwszej litery imienia i nazwiska użytkownika. Wyjątkiem było jedno konto w CSIZS i PIU Emp@tii, gdzie identyfikator skonstruowano w sposób odmienny, jednak identyfikacja użytkownika możliwa była przez zapisy zawarte w profilu konta.

14. [incydenty] MRiPS opracowało regulacje dotyczące zarządzania incydentami określające zasady ich zgłaszania oraz klasyfikacji wg trzech poziomów, a także zakres zadań osób zaangażowanych w ten proces.

Obszar ten wymaga jednak udoskonalenia, w szczególności ze względu na wprowadzenie 3[70] odmiennych definicji incydentu oraz wskazanie[71] nieaktualnych kanałów ich zgłaszania.

Zasadnym byłoby również wdrożenie postanowień dot. zakresu danych, jakie mają być zamieszczane w rejestrze incydentów, monitorowania, wykrywania i analizowania incydentów i ataków, w tym wyszukiwania powiązań oraz szacowania słabości zabezpieczeń, określenia maksymalnego czasu obsługi incydentów dla poszczególnych ich poziomów (poziom niski, średni i wysoki), zasad gromadzenia materiału dowodowego (poziom niski i średni) oraz, w uzasadnionych sytuacjach, mechanizmów umożliwiających monitorowanie rozmiarów i kosztów incydentów.

Dobrą praktyką było przekazywanie pracownikom informacji zwrotnej dot. zamknięcia incydentu. Kwestia ta ma zostać uwzględniona przy aktualizacji PBI IT[72].

Przyjęcie 3 odmiennych definicji incydentu w PBI IT nie zapewniało przejrzystości. Mogło również budzić wątpliwości interpretacyjne, jakie zdarzenia należy uznać za incydent. Jak wyjaśniono[73], zróżnicowanie to wynikało ze skierowania regulacji do różnych grup adresatów, o różnym poziomie kompetencji informatycznych. Zadeklarowano jednak, że dokument zostanie ujednolicony przy jego najbliższej aktualizacji.

PBI IT wskazuje użytkownikom tylko jeden aktualny kanał zgłaszania incydentów, tj. wewnętrzny nr telefonu. Podany w niej samoobsługowy system zgłoszeń (http://serwis/maximo/ui/login) wykorzystywany był do 9 marca 2021 r. i został zastąpiony nowym rozwiązaniem pn. ServiceDesk Plus. Natomiast na skutek zmiany struktury Ministerstwa[74] nastąpiła także zmiana adresu mejlowego (wskazano incydent@mrpips.gov.pl, podczas gdy aktualny to incydent@mrips.gov.pl). Wyjaśniono[75], że stosowne postanowienia PBI IT zostaną zmienione przy jej najbliższej aktualizacji.

PBI IT zawierała także procedurę gromadzenia materiału dowodowego w sytuacji zgłoszenia zdarzeń w zakresie bezpieczeństwa IT, jednak bez wskazania dla jakiego poziomu incydentów ma być ona uruchamiana. Wyjaśniono[76], że dot. ona incydentów i ataków wysokiego poziomu. Wynika z tego, że do pozostałych poziomów (niski, średni) zasady nie zostały opracowane. Wskazano, że doprecyzowanie tej kwestii nastąpi przy najbliższej aktualizacji PBI IT.

Natomiast pozostałe elementy wskazane powyżej, o które należałoby rozszerzyć PBI IT, zdaniem Ministerstwa[77] *nie mogą być skodyfikowane w sposób szczegółowy dla każdego incydentu dotyczącego bezpieczeństwa, jaki może w przyszłości nastąpić.* Dodano również,

[68] Za pośrednictwem CSIZS można zalogować się także do PIU Emp@tii.
[69] Pismo z 11 sierpnia 2021 r., znak: BKA-II.081.23.29.2021.IK.
[70] Pierwsza definicja incydentu znajduje się w części I *Pojęcia i przepisy regulujące PBI (IT)* zał. nr 1, druga w zał. nr 13 do PBI IT określającym procedurę zgłaszania incydentów związanych z bezpieczeństwem informacji oraz trzecia w zał. nr 19 do PBI IT określającym procedurę zgłaszania incydentów i ataków związanych z cyberbezpieczeństwem.
[71] Pkt 2 załącznika nr 13 do PBI IT.
[72] Pismo z 22 lipca 2021 r., znak: DI.III.081.5.24.2021.PW.
[73] Pismo z 22 lipca 2021 r., znak: DI.III.081.5.24.2021.PW.
[74] Tj. odłączenia działu *praca*.
[75] Pismo z 28 lipca 2021 r., znak: DI.III.081.5.26.2021.PW.
[76] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.26.2021.IK.
[77] Pismo z 22 lipca 2021 r., znak: DI.III.081.5.24.2021.PW.

że *kategoryczne wskazanie czasów obsługi incydentów, groziłoby raczej sparaliżowaniem działań osób rozwiązujących problem ze względu na groźbę przekroczenia terminów, niż motywowała ich do skutecznego działania.*

Zgodzić należy się, że tworzenie złożonych regulacji dla każdego z potencjalnych zagrożeń jest niecelowe. Natomiast ramowe uregulowanie poszczególnych kwestii ma na celu wskazanie właściwych norm postępowania i wsparcie w efektywnej realizacji zadań. Wyznaczenie maksymalnego czasu na obsługę poszczególnych kategorii incydentów nie jest działaniem mającym *paraliżować* czynności osób do tego wyznaczonych, a zapewniającym bezpieczeństwo informacji. Niezwłoczne usunięcie danego incydentu może bowiem znacząco wpłynąć na ograniczenie jego skutków.

15. Realizowano obowiązek rejestracji incydentów, zarówno tych pochodzących od pracowników, jak i z CSIRT.GOV.PL. Katalog gromadzonych informacji w rejestrach wymaga rozszerzenia w szczególności o dane osób zgłaszających, przyjmujących i obsługujących incydent/atak, wskazanie do jakiego poziomu został on zakwalifikowany oraz daty i godziny zamknięcia jego obsługi. Zamieszczenie danych osób uczestniczących w procesie zarządzania incydentem zapewniłoby rozliczalność działań, natomiast wskazanie jego poziomu i czasu zamknięcia pozwoliłoby na ocenę skuteczności zastosowanych rozwiązań. Niewątpliwie ocena ta ma wpływ na dobór właściwych zabezpieczeń, dlatego działania w tym zakresie powinny być dokumentowane.

Ministerstwo prowadziło dwa rejestry incydentów. W jednym rejestrowane były incydenty zgłaszane przez pracowników – w badanym okresie odnotowano ich 289. Natomiast w drugim ewidencjonowano incydenty pochodzące z CSIRT.GOV.PL i zarejestrowano ich 27. Zgodnie z wyjaśnieniami[78], w okresie kontrolowanym nie odnotowano zdarzeń, które zakwalifikowano jako incydenty wysokiego poziomu, poza jednym, w którym stwierdzono naruszenie danych osobowych. Przypadek ten został udokumentowany.

Rejestr incydentów zgłaszanych przez pracowników zawierał informacje skąd wpłynęło zgłoszenie, temat, datę i godzinę zgłoszenia oraz sposób rozwiązania incydentu. Z kolei rejestr incydentów pochodzących z CSIRT.GOV.PL. wskazywał nazwę, datę i opis incydentu oraz podjęte działania i wnioski. Zakres informacji, jakie powinny zostać odnotowane w rejestrze nie został uregulowany w PBI IT. W ocenie MRiPS nieokreślenie tej kwestii nie wpływa na rzetelność rejestrów oraz gromadzenia w nich istotnych informacji. Dodano również[79], że przyjęty zakres danych związanych ze zgłoszonymi zdarzeniami, które zawiera obecnie rejestr, jest wystarczający dla dokumentowania działań pracowników DI w tym zakresie. Zadeklarowano, że działania związane z analizą rejestrów w celu doskonalenia stosowanych zabezpieczeń były realizowane, choć działań tych nie dokumentowano[80].

Brak dokumentowania analiz rejestru incydentów uniemożliwia ocenę skuteczności podjętych działań, które są istotne w procesie doskonalenia *SZBI*. Brak czasu zamknięcia incydentu nie pozwala na uzyskanie informacji, w przypadku których incydentów wystąpiły największe problemy z ich usunięciem i w stosunku do których należy wzmocnić zabezpieczenia. A niewskazanie poziomu incydentu ma wpływ na ocenę adekwatności podjętych działań.

16. **[szkolenia]** Wynikający z regulacji wewnętrznych obowiązek organizacji szkoleń w zakresie bezpieczeństwa informacji dla pracowników nie rzadziej niż raz na 2 lata, nie został spełniony. Od cyklu szkoleń e-learningowych zrealizowanych w marcu i kwietniu 2019 r., w wyniku których przeszkolono znaczną część pracowników (438), ten okres minął. Na dzień 27 maja 2021 r. powyższy wymóg został spełniony jedynie w odniesieniu do 4 z 463 pracowników MRiPS. Wpływ na to miała sytuacja epidemiologiczna.

W 2019 r. MRPiPS przeprowadziło następujące szkolenia:

- cykl szkoleń e-learningowych pn. *Bezpieczny pracownik w cyberprzestrzeni* dla 438 pracowników (marzec-kwiecień);
- *Bezpieczeństwo aplikacji mobilnych* dla 1 pracownika (październik);

[78] Pismo z 22 lipca 2021 r., znak: DI.III.081.5.24.2021.PW.
[79] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.26.2021.IK.
[80] Wyjaśnienia z 22 lipca 2021 r., znak: DI.III.081.5.24.2021.PW.

- *Audyt systemów bezpieczeństwa informacji* dla 1[81] pracownika (listopad);
- *Informatyka śledcza – computer forensics* dla 3 pracowników (listopad).

W badanym okresie (tj. w grudniu 2020 r.) zrealizowano natomiast szkolenie pn. *Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001* dla 2[82] osób. Wymóg odbycia szkolenia nie rzadziej niż raz na 2 lata spełniało 4 pracowników, tj. 3 osoby uczestniczące w szkoleniu *Informatyka śledcza* oraz 1 pracownik biorący udział w szkoleniu *Bezpieczeństwo aplikacji mobilnych*. Wyjaśniono[83], że ze względu na sytuację epidemiologiczną przygotowania do organizacji szkoleń były opóźnione.

Forma szkoleń powinna być dostosowana do sytuacji epidemiologicznej, ponieważ szkolenia w zakresie BI mają istotne znaczenie, zwłaszcza w pracy zdalnej, która zwiększa ryzyko zagrożeń.

17. W Ministerstwie wprowadzono wymóg zapoznania się przez każdego pracownika, stażystę, praktykanta, wolontariusza lub podmiot zewnętrzny z Wyciągiem z PBI IT[84], z wyłączeniem dyrektorów komórek organizacyjnych i pracowników DI, którzy zobowiązani byli do zapoznania się z całym dokumentem. Czynności te były dokumentowane poprzez złożenie przez te osoby oświadczenia o zapoznaniu się z treścią regulacji i zobowiązaniu się do przestrzegania zasad, reguł i postanowień w niej zawartych. Zasadnym byłoby wdrożenie wymogu zapoznania się z całą Polityką IT. Jest to uzasadnione wskazaniem w części załączników[85] obowiązków i odpowiedzialności pracowników, z którymi powinni się oni zapoznać.

Wszystkie osoby poddane kontroli (46[86] z 463 (10%) pracowników[87], 2 stażystów oraz 1 wolontariusz (100%)[88]) złożyły oświadczenia o zapoznaniu się z PBI IT / Wyciągiem z PBI IT.

Przyjęcie dwóch rodzajów dokumentów (Wyciąg z PBI IT i PBI IT), jak wyjaśniono[89], wynikało z różnego zakresu odpowiedzialności poszczególnych grup pracowniczych. Przyjęto zasadę, że od dyrektorów oraz pracowników DI wymaga się wyższego poziomu odpowiedzialności, a zatem również większego poziomu znajomości regulacji. Dla pozostałych pracowników przygotowany został Wyciąg z PBI IT, który zawiera najistotniejsze jej elementy. Niezależnie od postanowień PBI IT, każdy pracownik MRiPS miał dostęp do bazy regulacji wewnętrznych i mógł zapoznać się z przepisami całego zarządzenia wprowadzającego PBI IT. Ponadto pracownicy Ministerstwa byli informowani drogą mejlową o procedurze zgłaszania incydentów.

Zamieszczenie PBI IT w bazie regulacji wewnętrznych było słusznym działaniem, jednak rodzi ryzyko, że nie każdy pracownik zapozna się z jej treścią z własnej inicjatywy. Dodatkowo w treści oświadczenia o zapoznaniu się z Wyciągiem z PBI IT pracownik potwierdzał, że zobowiązuje się do przestrzegania zasad, reguł i postanowień w nim zawartych. Jeśli sam dodatkowo zapozna się z całą regulacją, to i tak złożone zobowiązanie nie będzie dotyczyło wszystkich zasad.

18. **[umowy]** Umowy zawierały postanowienia gwarantujące odpowiedni poziom bezpieczeństwa informacji i należyte zabezpieczenie interesów Ministerstwa. Najważniejsze z nich dot.: parametrów świadczonych usług (parametrów SLA), obowiązku przeniesienia na rzecz MRiPS autorskich praw majątkowych do wytworzonych w ramach umowy dzieł, kar umownych na wypadek niewykonania lub nienależytego wykonania umowy oraz warunków

[81] Osoba biorąca udział w tym szkoleniu na dzień 27 maja 2021 r. nie była już pracownikiem MRiPS.
[82] Osoby biorące udział w tym szkoleniu na dzień 27 maja 2021 r. nie były już pracownikami MRiPS.
[83] Pismo z 30 lipca 2021 r., znak: BKA-II.081.23.23.2021.IK.
[84] Załącznik nr 2 do PBI IT.
[85] W szczególności dot. zał. nr 5 (pracownicy zobowiązani do przestrzegania praw dostępu do informatycznego systemu MRPiPS oraz bezpośredni przełożeni zaangażowani w proces dostępu do zasobów IT), zał. nr 8 (użytkownicy urządzeń mobilnych), zał. nr 9 (użytkownicy i przełożeni pracowników w zakresie zdalnego dostępu), zał. nr 10 (wszyscy pracownicy w zakresie podjęcia decyzji co do zniszczenia dokumentów lub informacji zwykłych oraz nieuprawnionego lub celowego zniszczenia nośników/sprzętu/dokumentów), zał. nr 11 (każdy kto otrzymał do użytku urządzenie do podpisu elektronicznego), zał. nr 13 (każda osoba, w celu zgłoszenia incydentu), zał. nr 14 (pracownicy, którzy otrzymali dostęp do komputera nieobecnego pracownika), zał. nr 15 (pracownicy w zakresie obowiązku wylogowania się z systemów informatycznych, wyłączenia z zasilania stacji roboczych oraz pozostałego sprzętu biurowego), zał. nr 18 (pracownicy w zakresie zgłaszania podejrzenia naruszenia i obowiązków w tej sytuacji), zał. nr 19 (pracownicy w zakresie zgłaszania incydentów i ataków), zał. nr 20 (pracownicy Departamentu Polityki Rodzinnej w zakresie pozyskiwania i zawierania umów z Partnerami KDR, przekazywania informacji o Partnerach oraz koordynowania pracy urzędów wojewódzkich), zał. nr 21 (pracownicy w zakresie poprawnego przetwarzania informacji), zał. 23-25 (pracownicy Departamentu Pomocy i Integracji Społecznej w zakresie zarządzania Systemem Centralnym FEAD).
[86] Dobór oświadczeń składanych przez pracowników korpusu służby cywilnej odbył się w oparciu o metodę losową ze stałym interwałem n+10. Wybrano 37 spośród 372 pracowników (10%), rozpoczynając od poz. nr 1 z przekazanego wykazu pracowników. W przypadku pracowników zatrudnionych poza korpusem służby cywilnej zastosowano dobór celowy uwzględniający charakter stanowiska, tj. wytypowano stanowiska mające dostęp do systemu informatycznego MRiPS.
[87] Zatrudnionych na 27 maja 2021 r.
[88] Wszystkie osoby świadczące pracę w Ministerstwie na dzień sporządzania zestawienia (27 maja 2021 r.).
[89] Pismo z 27.07.2021 r., znak: BKA-II.081.23.20.2021.IK.

rozwiązania umowy[90]. Regulowały także procedury odbioru przedmiotu umowy poprzez obowiązek rozliczenia umów dopiero po zatwierdzeniu protokołu odbioru. Wskazywały osoby odpowiedzialne za sprawowanie bieżącego nadzoru i upoważnione do kontaktów. Zobowiązywały do zapoznawania się z Wyciągiem z PBI IT wszystkich wykonawców mających dostęp do zasobów informatycznych Ministerstwa.

Zasadnym byłoby rozszerzenie postanowień umów o kwestię odszkodowania ze strony wykonawcy w przypadku niezastosowania się do procedur lub świadomego działania wpływającego na osłabienie systemu bezpieczeństwa oraz dot. bezstronności wykonawców. Dodatkowo w przypadku 3 z 11 umów (27%) nie wskazano postanowień dot. poufności, a w 4 (36%) nie określono mechanizmów umożliwiających Ministerstwu kontrolę lub audyt wykonawcy w zakresie przestrzegania przez niego zasad BI.

> W badanym okresie obowiązywało 57[91] umów w zakresie serwisu i rozwoju sprzętu oraz oprogramowania. Kontroli poddano 11[92] z nich (19%)[93].
>
> W 10[94] z 11 badanych umów (91%) zasady odpowiedzialności odszkodowawczej nie odnosiły się wprost do szkód powstałych wskutek świadomego działania wpływającego na osłabienie systemu bezpieczeństwa lub niezastosowania się przez wykonawcę do procedur obowiązujących w MRiPS. W przypadku 1[95] umowy dot. kupna-sprzedaży komputerów przenośnych nie było konieczności wskazania takich postanowień. Jak wyjaśniono[96] klauzule stosowane przez MRiPS w umowach obejmują wszelkie rodzaje szkód, a więc również te powstałe z wyżej wymienionych przyczyn.

Uwzględnianie w zawieranych umowach postanowień, które precyzyjnie określą odpowiedzialność za szkody powstałe wskutek powyższych działań umożliwi Ministerstwu sprawne dochodzenie ewentualnych roszczeń.

> Żadna z 11 badanych umów nie uwzględniała postanowień dot. zachowania przez wykonawcę bezstronności przy realizacji umowy. Wyjaśniono[97], że w przypadku badanych umów nie zachodzi ryzyko wykonania prac w sposób stronniczy.

Nie można się z tym zgodzić, bowiem możliwość oddziaływania na bezstronność wykonawców istnieje w przypadku każdej umowy dot. serwisu i rozwoju sprzętu i oprogramowania informatycznego. Natomiast wprowadzenie mechanizmów zapewnienia bezstronności minimalizuje ryzyko braku obiektywizmu i wystąpienia konfliktu interesów.

> W 3[98] z 11 (27%) badanych umów nie zawarto postanowień zobowiązujących do zachowania w tajemnicy informacji uzyskanych w związku z ich realizacją lub nie zobowiązano do złożenia oświadczenia o poufności. Jak wyjaśniono[99], takie zabezpieczenia wymagane są od wykonawców, którzy w ramach realizacji przedmiotu umowy mają dostęp do zasobów infrastruktury informatycznej centrum przetwarzania danych.

Zapewnienie poufności nie powinno ograniczać się tylko do informacji, które są przechowywane w centrum przetwarzania danych. Zabezpieczenie takie powinno mieć zastosowanie w zakresie wszystkich informacji jakimi dysponuje MRiPS.

> W odniesieniu do 4[100] umów serwisowych, w przypadku których zasadnym było wprowadzenie mechanizmów kontroli lub audytu wykonawcy, wskazano[101], że wprowadzanie takich mechanizmów nie było konieczne, a weryfikacja prawidłowości działań po stronie wykonawcy może odbywać się

[90] Z wyjątkiem jednej umowy o dzieło (nr DI.WI.3.2021 Hostlab Olczak i Wspólnicy Sp. J.), która nie wymagała takich postanowień. Uzasadnione było to jej krótkim terminem realizacji (2 miesiące) i wprowadzeniem zabezpieczeń w postaci kar umownych.
[91] Zestawienie 56 umów obowiązujących w MRiPS na serwis i rozwój systemów, w tym oprogramowania (przekazane przy piśmie z 2 czerwca 2021 r., znak: BKA-II.081.23.3.2021.IK) oraz 1 umowa nr DI/WI/1/2019 z 21 lutego 2019 r. dot. naprawy, konserwacji i czyszczenia urządzeń IT (przekazana przy piśmie z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK).
[92] Umowy: nr 28.DI.PN.2019.2020 Integrated Solutions Sp z o.o.; nr 32.DI.PN.2019.2020 S&T Poland Sp. z o.o; nr 13.DI.PN.2018 IT Solution Factor Sp. z o.o.; nr 18.DI.PN.2020 IT Solution Factor Sp. z o.o.; nr 17.DI.PN.2020 Softiq Sp. z o.o.; nr 11.DI.PN.2019 Softiq Sp. z o.o.; nr 25.DI.PN.2020.2021 Softiq Sp. z o.o.; nr 18.DI.PN.2016 Sygnity S.A; nr DI.WI.3.2021 Hostlab [redacted] i Wspólnicy Sp. J; nr 34.DI.PN.2020 SLX Sp. z o.o.; nr 30.DI.PN.2020 MBA System Sp. z o.o.
[93] Próbę do badania dobrano metodą celową uwzględniając: wartość umowy, zasadność jej zawarcia, istotność przedmiotu umowy dla badanego obszaru oraz czy przedmiot umowy dotyczy wybranych do badania 3 systemów (CSIZS, PIU Emp@tia, SI KDR).
[94] Umowy: nr 28.DI.PN.2019.2020 Integrated Solutions Sp z o.o.; nr 32.DI.PN.2019.2020 S&T Poland Sp. z o.o; nr 13.DI.PN.2018 IT Solution Factor Sp. z o.o.; nr 18.DI.PN.2020 IT Solution Factor Sp. z o.o.; nr 17.DI.PN.2020 Softiq Sp. z o.o.; nr 11.DI.PN.2019 Softiq Sp. z o.o.; nr 25.DI.PN.2020.2021 Softiq Sp. z o.o.; nr 18.DI.PN.2016 Sygnity S.A; nr DI.WI.3.2021 Hostlab [redacted] i Wspólnicy Sp. J; nr 34.DI.PN.2020 SLX Sp. z o.o.
[95] Umowa nr 30.DI.PN.2020 MBA System Sp. z o.o.
[96] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW.
[97] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW.
[98] Umowy: nr 18.DI.PN.2020 IT Solution Factor Sp. z o.o. (wsparcie techniczne producenta dla oprogramowania kopii zapasowej); nr DI.WI.3.2021 Hostlab [redacted] i Wspólnicy Sp. J (przygotowanie serwisu internetowego nt. programów realizowanych przez MRiPS); nr 34.DI.PN.2020 SLX Sp. z o.o. (dostawa wraz z instalacją i konfiguracją zestawu do wideokonferencji).
[99] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW.
[100] Umowy: nr 28.DI.PN.2019.2020 Integrated Solutions Sp z o.o.; nr 32.DI.PN.2019.2020 S&T Poland Sp. z o.o; nr 13.DI.PN.2018 IT Solution Factor Sp. z o.o.; nr 18.DI.PN.2020 IT Solution Factor Sp. z o.o.
[101] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW oraz pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.27.2021.IK.

w ramach ewentualnych postępowań odszkodowawczych. Dodano[102] również, że odpowiednie klauzule zostaną opracowane i będą wprowadzane do treści umów, kiedy będzie to uzasadnione ich przedmiotem.

Zamieszczenie w umowach postanowień dot. uprawnień kontrolnych umożliwiłoby Ministerstwu podejmowanie dodatkowych działań, w szczególności w sytuacjach powzięcia informacji nt. nieprzestrzegania przez wykonawców zasad BI obowiązujących w Jednostce.

19. Obowiązujące w MRiPS regulacje nie obejmowały wszystkich zagadnień, jakie powinny być uwzględniane przy sporządzaniu umów dot. serwisu i rozwoju sprzętu i oprogramowania informatycznego. Odnosiły się one jedynie się do wymagań stawianych przez przepisy prawa zamówień publicznych[103], finansów publicznych[104] oraz ochrony danych osobowych[105]. Zatem zasadne byłoby opracowanie katalogu niezbędnych postanowień dotyczących ochrony informacji.

W przedmiocie zawierania umów cywilnoprawnych[106] regulacje nie określały obowiązku wskazania w umowach dot. serwisu i rozwoju sprzętu i oprogramowania informatycznego postanowień w zakresie:

- poufności;
- bezstronności;
- parametrów SLA;
- mechanizmów kontroli i audytu wykonawcy;
- odpowiedzialności i odszkodowania ze strony wykonawcy w przypadku niezastosowania się do procedur lub świadomego działania wpływającego na osłabienie systemu bezpieczeństwa;
- kwestii obowiązku obecności (lub jego braku) wyznaczonego pracownika MRiPS przy realizacji przedmiotu umowy dla zapewnienia nadzoru nad jej wykonaniem, jeśli jest to uzasadnione jej charakterem;
- konieczności określenia osób odpowiedzialnych za sprawowanie bieżącego nadzoru nad ich realizacją lub upoważnionych do kontaktów;
- uwzględniania opisu i poziomu dostępu do urządzeń przetwarzających informacje lub do pomieszczeń, w których informacje są przechowywane.

Wyjaśniono[107], że przyjęto reguły określające zestaw minimalnych, ale jednocześnie niezbędnych klauzul, które są wymagane przez prawo zamówień publicznych oraz finanse publiczne. Zdaniem Ministerstwa[108] wprowadzanie nadmiarowych klauzul, nieadekwatnych dla konkretnego przedmiotu zamówienia może skutkować ponoszeniem zawyżonych i nieuzasadnionych kosztów realizacji przedmiotu zamówienia.

Wprowadzenie katalogu postanowień nie oznacza automatyzmu w zakresie ich przenoszenia do treści umów. Katalog ma stanowić pomocnicze narzędzie, które będzie zapobiegać pominięciu istotnych zabezpieczeń w umowach.

20. Przyjęte rozwiązania dot. obowiązku zachowania poufności informacji odnosiły się jedynie do części wykonawców. PBI IT zawężała obowiązek składania oświadczeń dot. poufności do osób, które wykonywały prace lub usługi w zakresie obsługi informatycznej lub teleinformatycznej, obsługi nośników danych, w tym utylizacji tych nośników. Natomiast przyjęta praktyka dodatkowo ograniczała realizację tego obowiązku do wykonawców umów, którzy mieli dostęp do zasobów infrastruktury informatycznej centrum przetwarzania danych.

Spośród 11 badanych umów, obowiązek złożenia oświadczenia o poufności, zgodnie z postanowieniami PBI IT[109] dot. 10[110] umów. Nie został on zrealizowany w przypadku

[102] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.27.2021.IK.
[103] Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129, ze zm.).
[104] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2021 r. poz. 305, ze zm.).
[105] 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.) oraz ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781, t. j.).
[106] Zarządzenie nr 7 Dyrektora Generalnego MRPIPS z dnia 23 maja 2018 r. w sprawie zamówień publicznych; zarządzenie nr 3 Dyrektora Generalnego MRPiPS z dnia 11 stycznia 2019 r. zmieniające zarządzenie w sprawie zamówień publicznych; zarządzenie Dyrektora Generalnego MRPiPS z dnia 26 listopada 2019 r. zmieniające zarządzenie w sprawie zamówień publicznych; zarządzenie Dyrektora Generalnego MRIPS z dnia 20 maja 2021 r. w sprawie zamówień publicznych.
[107] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW.
[108] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW.
[109] Załącznik nr 6 do PBI IT.
[110] Z wyłączeniem umowy nr 30.DI.PN.2020, której przedmiot dot. zakupu laptopów.

5[111] umów, gdyż jak wyjaśniono[112] oświadczenia pobierano jedynie od wykonawców, którzy mieli dostęp do zasobów infrastruktury informatycznej centrum przetwarzania danych. Dodano, że stosowne przepisy PBI IT wymagają doprecyzowania i zostaną zmodyfikowane.

Obowiązek zachowania poufności informacji powinien dotyczyć wszystkich wykonawców.

21. [praca na odległość] Pozytywnie należy ocenić działania zapewniające bezpieczną pracę na odległość. PBI IT zawierała ogólne postanowienia w tym zakresie, a w okresie epidemii opracowano *Zasady polecania i świadczenia pracy zdalnej* (dalej: *zasady pracy zdalnej*)[113]. Na urządzeniach mobilnych stosowano zabezpieczenia chroniące informacje na nich przetwarzane, w szczególności przez odpowiednią konfigurację stacjonarnego komputera służbowego, do którego następowało połączenie zdalne, uwierzytelnianie użytkownika, bezpieczne szyfrowane połączenie VPN oraz np. zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, oprogramowanie antywirusowe, systemy kontroli dostępu.

PBI IT zawierała postanowienia dot. komputerów przenośnych i pracy na odległość, przyznawania urządzeń zdalnego dostępu[114], zasad uzyskiwania zdalnego dostępu do sieci dla usługodawcy zewnętrznego[115]. *Zasady pracy zdalnej* określały m.in. zlecanie pracy zdalnej i sporządzanie harmonogramów dot. osób ją wykonujących, sprzętu informatycznego i bezpiecznego dostępu do zasobów MRiPS, obowiązki pracowników oraz organizację pracy zdalnej. Przewidywały też możliwość wykonywania pracy zdalnej na sprzęcie prywatnym pracownika.

Sprzęt prywatny był wykorzystywany, gdy nie było innej możliwości. Służył on wyłącznie do zestawienia połączenia VPN i uruchomienia pulpitu zdalnego. Pracownik wykonując pracę zdalną wykorzystywał oprogramowanie, które zainstalowano i skonfigurowano na jego służbowym komputerze stacjonarnym. Dostęp do zasobów / systemów następował nie z komputera zdalnego (prywatnego) lecz z komputera znajdującego się w sieci MRiPS.

Zasadą było, że pracownicy korzystający zdalnie ze sprzętu służbowego posiadali skonfigurowane urządzenia, aby zapewniały one dostęp do zasobów i uprawnień, jakie zostały przydzielone pracownikowi w przypadku świadczenia pracy w trybie stacjonarnym. Osoby korzystające ze sprzętu prywatnego otrzymywały dostęp do poczty elektronicznej i systemu obiegu dokumentów, a udzielenie szerszego zakresu następowało na podstawie wniosku kierownika komórki, w której zatrudniony był pracownik, po zatwierdzeniu przez Dyrektora DI.

Praca zdalna była ewidencjonowana, tj. prowadzono wykazy pracowników pracujących na prywatnym, jak i służbowym sprzęcie ze wskazaniem okresu jej realizacji.

22. Wdrożono narzędzia umożliwiające monitorowanie użytkowników świadczących pracę zdalnie w celu wykrycia nieuprawnionych działań, czynności te nie były jednak dokumentowane.

Zgodnie z PBI IT[116] kluczowe systemy informatyczne powinny być monitorowane w celu wykrycia w nich nieuprawnionych działań. W procedurze *Dostęp zdalny do zasobów MRiPS*[117] przewidziano, że *korzystanie z połączenia zdalnego wiąże się z wyrażeniem zgody na monitorowanie działań użytkownika w sieci MRiPS*[118]. Ze wszystkich połączeń użytkowników zbierano logi w urządzeniu VPN oraz z systemów typu IPS. Narzędzia zapewniające bezpieczeństwo[119], m.in. dokonują badania treści pakietów transmitowanych z i do wewnętrznej sieci MRiPS, a w przypadku naruszenia bezpieczeństwa prezentują alerty. W przypadku braku alertu stan taki traktowany jest jako równoznaczny z brakiem wystąpienia naruszeń i zagrożeń BI. Monitoring realizowany jest w ramach bieżących zadań i codziennych czynności pracowników odpowiedzialnych za jego prowadzenie. Z czynności tych nie jest sporządzana osobna dokumentacja papierowa. Wskazano, że w badanym okresie nie doszło do sytuacji cofnięcia użytkownikowi zdalnego dostępu.

[111] Umowy: nr 28.DI.PN.2019.2020 Integrated Solutions Sp z o.o.; nr 13.DI.PN.2018 IT Solution Factor Sp. z o.o.; nr 18.DI.PN.2020 IT Solution Factor Sp. z o.o.; nr DI.WI.3.2021 Hostlab [redacted] i Wspólnicy Sp. J; nr 34.DI.PN.2020 SLX Sp. z o.o.
[112] Pismo z 19 lipca 2021 r., znak: DI.III.081.5.18.2021.PW.
[113] Zasady z 26 sierpnia 2020 r. (obowiązujące od 1 września 2020 r.) oraz z 26 lutego 2021 r. (obowiązujące od 1 marca 2021 r.).
[114] § 9 części II PBI IT wraz z procedurą dot. zasad przyznawania urządzeń zdalnego dostępu użytkownikom MRPiPS (załącznik nr 8 do PBI IT).
[115] § 19 ust. 11-13 części II PBI IT wraz z procedurą dot. dostępu zdalnego do systemów teleinformatycznych MRPiPS (załącznik nr 9 do PBI IT).
[116] § 24 części II PBI IT.
[117] Pkt 3 procedury. Procedura stanowi załącznik do *Zasad pracy zdalnej*.
[118] Filtrowanie treści, filtrowanie nagłówków pakietów, możliwość odcięcia użytkownika od zasobów MRiPS w przypadku naruszenia bezpieczeństwa informatycznego lub informacji MRiPS. Ponadto pkt 5 postanowień końcowych procedury określał, że *zdalny dostęp może być zawsze i w każdej chwili odrzucony z ważnych względów (przykładowo: zbyt długa bezczynność, transfer niedozwolonych plików, zachowanie niezgodne z PBI)*.
[119] W szczególności Next Generation Firewall, Intrusion Prevention System, oprogramowanie antywirusowe, system kontroli dostępu do sieci (NAC), blokowanie dostępu po pięciu nieudanych próbach.

23. [kopie zapasowe] Działania w zakresie wykonywania i testowania kopii zapasowych były wykonywane prawidłowo. Zostały one dostosowane do potrzeb Ministerstwa i wspierały jednostkę w zarządzaniu tym obszarem. Wprowadzono też odpowiednie regulacje w PBI IT[120], a ich uszczegółowienie nastąpiło w dokumentacji Systemu backupu Commvault[121] oraz w *Polityce kopii zapasowych MRPiPS*[122].

Do zarządzania kopiami wykorzystywane było oprogramowanie Commvault[123], które zapewniało ich ewidencję. Kopie tworzone były dla wszystkich systemów teleinformatycznych. Każdy system posiadał indywidualnie zdefiniowaną częstotliwość ich sporządzania, w zależności od poziomu jego istotności. W przypadku trzech badanych systemów pełna kopia zapasowa tworzona była raz w tygodniu, a następnie codziennie sporządzano kopie przyrostowe. Przechowywano je przez okres 30 dni, w cyklu utrzymania 4 kopii pełnych. System backupu weryfikował poprawność utworzenia kopii i w przypadku ich nieprawidłowego zapisu wysyłał mejlem do uprawnionych pracowników *Raport niepowodzeń*. Na jego podstawie podejmowano dalsze działania w celu usunięcia przyczyn zaraportowanych błędów. W uzasadnionych sytuacjach podejmowane też były działania związane z odtworzeniem kopii. Wykonywano je również w przypadkach problemów zgłaszanych przez pracowników. Każde działanie związane z odtworzeniem kopii odnotowywano w *Raporcie odtwarzania zasobów backupu*[124].

24. [projektowanie, eksploatacja oraz wdrażanie zmian w systemach] MRiPS posiadało regulacje wewnętrzne w zakresie projektowania, wdrażania i eksploatacji systemów teleinformatycznych oraz przeprowadzania zmian w systemach. Zawierały ogólne postanowienia, natomiast szczegółowe wymogi zawierane były w specyfikacji danego systemu teleinformatycznego. Rozwiązanie takie, ze względu na różnorodność systemów, pozwoliło na określenie indywidualnych wymogów do każdego z nich.

W badanym okresie nie wdrażano nowych systemów. PBI IT[125] w zakresie projektowania i odbioru systemu zawierała postanowienia dot.: obowiązku określania w umowach kwestii własności oprogramowania i praw autorskich[126], przechowywania kodu źródłowego, obowiązku opracowania przez dostawcę oprogramowania zarówno dokumentacji technicznej, jak i użytkowej, konieczności odseparowania środowiska produkcyjnego od innych środowisk oraz zakazu prowadzenia prac rozwojowych w tym środowisku, zasad przeprowadzania testów. Wskazywała także na konieczność współpracy komórki wdrażającej system z DI w celu spełnienia nie tylko wymogów technicznych, ale również bezpieczeństwa.

25. Proces wdrażania zmian w trzech badanych systemach był przejrzysty. Słabością było nałożenie obowiązków w PBI IT, które w praktyce nie były przestrzegane. Dotyczyło to obowiązku rejestracji zmian. Ponadto nie dokumentowano przeprowadzonych analiz zasadności wdrożenia zmiany, ryzyka, wykonalności, kosztu, zysku, wpływu na pozostałe części sytemu oraz możliwości weryfikacji tej zmiany.

W badanym okresie w 3 kontrolowanych systemach wprowadzono 24 zmiany, tj. 13 w CSIZS, 6[127] – SI KDR, 5 – PIU Emp@tia. Przebiegły one zgodnie z *Procedurami rozwojowymi*[128]. Ministerstwo przekazywało do wykonawcy umowy listę zmian, jakie chciałoby wdrożyć w systemie. Następnie wykonawca sporządzał projekt wstępnych zmian wraz z określeniem liczby roboczogodzin potrzebnych do ich wykonania[129] oraz plan testów akceptacyjnych[130]. Dokumenty zatwierdzał ASI danego systemu. Po przekazaniu przez wykonawcę nowej wersji systemu sporządzany był protokół przekazania wersji. Była ona testowana przez Wydział Testów i Homologacji, a po pozytywnym przebiegu testów, ASI sporządzał protokół odbioru wersji systemu. Wykonawcy systemów zobowiązani byli do przekazania kodów źródłowych, które przechowywane były w zabezpieczonym miejscu. *Procedury rozwoju* regulowały także proces zapytania projektowego.

---

[120] § 18 cz. II załącznika nr 1 PBI IT.
[121] Wersja 3.0 z 1 czerwca 2021 r.
[122] Zlecona do realizacji przez Dyrektora DI 1 października 2020 r.
[123] W wersji 11.20.36.
[124] Przykładowy *Raport odtwarzania zasobów backupu* stanowi załącznik nr 3 do protokołu oględzin tworzenia oraz testowania kopii zapasowych przeprowadzonych 1 lipca 2021 r.
[125] § 15 załącznika nr 1 do PBI IT.
[126] Ze wskazaniem, że jeśli to możliwe Ministerstwo powinno być właścicielem praw autorskich.
[127] W ramach 1 zmiany wersji systemu 2.11.0 dokonano 2 zmian prawnych. Jedna dot. dostosowania systemu do zmienionych wzorów wniosków oraz momentu aktywowania Karty Dużej Rodziny (KDR2020_25), natomiast druga – dostosowania systemu do przejścia z obsługi funkcjonalności integracji z mKDR na integrację z mObywatel (KDR2020_26).
[128] Stanowiącymi zał. do umów, tj.: zał. nr 1 do umowy nr 17/DI/PN/2020 (dot. CSIZS); zał. nr 1 do umowy 11/DI/PN/2019 (dot. SI KDR); zał. nr 2 do umowy nr 18/DI/PN/2016 (dot. PIU Emp@tia umowa obowiązywała do 24 listopada 2020 r.) oraz zał. nr 1 do umowy nr 25/DI/PN/2020/2021 (dot. PIU Emp@tia umowa obowiązywała od 7 kwietnia 2021 r.).
[129] Zmiany zostały podzielone na 3 kategorie: zmiany prawne (dostosowanie do zmian prawa mających wpływ na działanie systemu), zmiany funkcjonalne (dostosowanie systemu do potrzeb i wymagań użytkowników) oraz zmiany wynikające z aktualizacji platformy narzędziowo sprzętowej. W przypadku zmian prawnych wykonawca nie był zobowiązany do określania liczby roboczogodzin potrzebnych na wykonanie tej zmiany, bowiem rozliczane były one ryczałtowo.
[130] Stanowi on załącznik do projektu wstępnego.

Zgodnie z PBI IT wnioski o zmianę powinny być rejestrowane oraz analizowane pod kątem zasadności wdrożenia zmiany, ryzyka, wykonalności, kosztu, zysku, wpływu na pozostałe części sytemu oraz możliwości weryfikacji tej zmiany[131]. Analiza taka była prowadzona podczas akceptacji projektu wstępnego[132]. Zdaniem DI zatwierdzenie tego projektu jest potwierdzeniem pozytywnego wyniku tej analizy i było to wystarczające, dlatego nie wymagało dodatkowego dokumentowania[133].

Nie można zgodzić się z Kontrolowanym, ponieważ dokumentacja dot. zatwierdzenia projektu wstępnego nie zawierała informacji pozwalających na ustalenie, czy analiza w powyższym zakresie została przeprowadzona i jaki był jej wynik.

W odniesieniu do obowiązku rejestrowania zmian wskazano[134], że wykaz zmian znajduje się treści *Raportów z realizacji przedmiotów umów*[135]. Dokumentacja utrzymania systemu jest prowadzona dla systemu i są w niej przechowywane wykazy wszystkich zmian. Zdaniem MRiPS, spełnia to wymóg prowadzenia rejestru zmian, bowiem w ten sposób zapewnia się pełną wiedzę pracownikom DI, co jest podstawowym celem prowadzenia jakichkolwiek rejestrów[136].

Raporty z realizacji przedmiotów umów dają pełną informację nt. wdrażanych zmian w systemach, ale nie można ich uznać za rejestr zmian określony w regulacji wewnętrznej. W przypadku SI KDR oraz CSIZS *Raporty z realizacji przedmiotu umów* zawierały tylko informacje nt. zmian wersji wdrożonych w 3 miesięcznym okresie rozliczeniowym. Zatem, aby ustalić pełny zakres zmian jakie zostały wprowadzone w tych systemach, należałoby zapoznać się ze wszystkimi raportami[137]. W przypadku PIU Emp@tia w badanym okresie nastąpiła zmiana Wykonawcy. Tym samym raport nowego wykonawcy zawierał informacje nt. zmian systemu zrealizowanych jedynie przez niego.

26. Pozytywnie należy ocenić monitorowanie systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności, w szczególności wobec wzrostu liczby systemów teleinformatycznych, ilości przetwarzanych danych oraz liczby użytkowników.

Zgodnie z *Procedurami administrowania oraz usuwania awarii i błędów*[138] trzech badanych systemów, ich wykonawcy zobowiązani byli do monitorowania w sposób ciągły wydajności, dostępności, niezawodności oraz sprawności i bezpieczeństwa działania poszczególnych komponentów danego systemu, w tym przeprowadzania testów wydajnościowych na żądanie MRiPS, a także monitorowania przyrostu danych, ilości wolnej przestrzeni dyskowej, długości aktualnego okna backupowego.

W badanym okresie przeprowadzono testy wydajnościowe PIU Emp@tia oraz CSIZS, które potwierdziły, że systemy działają stabilnie. Podkreślono[139] także, że są one eksploatowane od wielu lat i przechodzą tzw. *testy bojowe* podczas rozpoczynania się każdego okresu świadczeniowego. Wówczas w ciągu kilku dni przetwarzają klika milionów wniosków, a ostatnich kilka okresów przebiegało bez problemów wydajnościowych.

MRiPS przeprowadziło także inne analizy jakościowo-ilościowe, m.in. dot. błędnych wniosków bankowych w ramach świadczenia 500+, statystyki dot. liczby wniosków o świadczenie 500+ oraz inne świadczenia, w tym liczby wydanych decyzji, statystyki wymiany danych pomiędzy gminami i urzędami wojewódzkimi oraz raporty wywołanych usług przez urzędy wojewódzkie.

Sprawny proces monitorowania systemów teleinformatycznych umożliwia podjęcie niezwłocznych działań w przypadku wystąpienia sytuacji niepożądanych, tym samym w istotny sposób może przyczynić się do ograniczenia ich skutków i zwiększyć bezpieczeństwo informacji w nich przetwarzanych.

27. [zabezpieczenia techniczno-organizacyjne dostępu do informacji] W MRiPS obowiązywały regulacje wewnętrzne dot. minimalizowania wystąpienia ryzyka kradzieży lub

[131] § 26 ust. 2 części II zał. nr 1 do PBI IT – *Wnioski o dokonanie zmiany składane są w formie pisemnej oraz rejestrowane, analizowane pod kątem zasadności, ryzyka, wykonalności, kosztu, zysku z przeprowadzenia danej zmiany, wpływu na pozostałe części systemu informatycznego, a także pod kątem możliwości późniejszej weryfikacji tej zmiany.*
[132] Pismo z 20 lipca 2021 r., znak: DI.III.081.5.19.2021.PW.
[133] Pismo z 5 sierpnia 2021 r., znak: DI.III.081.5.35.2021.PW.
[134] Pismo z 20 lipca 2021 r., znak: DI.III.081.5.19.2021.PW.
[135] Raporty sporządzane przez wykonawców za dany okres rozliczeniowy.
[136] Pismo z 5 sierpnia 2021 r., znak: DI.III.081.5.35.2021.PW.
[137] Np. ostatni raport SI KDR obejmujący okres 3 marca – 2 czerwca 2021 r. zawiera informację nt. 4 wersji systemu zatwierdzonych w okresie za jaki sporządzono raport, a nie wszystkich wprowadzonych zmian do systemu.
[138] Stanowiącymi zał. do umów, tj.: nr 2 do umowy nr 17/DI/PN/2020 (dot. CSIZS); nr 2 do umowy 11/DI/PN/2019 (dot. SI KDR); nr 3 do umowy nr 18/DI/PN/2016 (dot. PIU Emp@tia) oraz nr 2 do umowy nr 25/DI/PN/2020/2021 (dot. PIU Emp@tia).
[139] Pismo z 20 lipca 2021 r., znak: DI.III.081.5.19.2021.PW.

utraty informacji, w tym określające zasady ochrony fizycznej. Jednakże wymagały one aktualizacji i uzupełnienia. Prace w tym zakresie zostały wstrzymane, w szczególności z uwagi na istotne zmiany zasad kontroli ruchu spowodowane odłączeniem działu administracji rządowej – *praca*[140].

Wdrożono *Instrukcję kontroli ruchu osobowego i materiałowego oraz organizacji ruchu pojazdów i przydziału miejsc parkingowych* (dalej: *Instrukcja kontroli ruchu osobowego*)[141]. Wskazywała ona m.in. dokumenty uprawniające do wejścia na teren Jednostki oraz zasady ich wydawania, zasady kontroli osób i dokumentów przy wejściu, zasady ruchu i przebywania osób na terenie MRiPS oraz zasady ruchu pojazdów i przydziału miejsc parkingowych. Regulacja ta ze względu na wprowadzone zmiany organizacyjne wymagała aktualizacji / uzupełnienia, w szczególności w zakresie:

- zmiany komórki odpowiedzialnej za wykonywanie identyfikatorów oraz kart wstępu. Na skutek zmiany regulaminu organizacyjnego MRPiPS[142] zadanie to 1 sierpnia 2020 r. przeszło z Biura Ministra do Biura Administracyjnego;
- określenia zasad dot. pomieszczeń plombowanych, w tym wprowadzenia obowiązku ich ewidencji;
- wskazania zasad zarządzania kluczami, w tym dostępu do poszczególnych pomieszczeń;
- wdrożenia dodatkowej kategorii kart *agent ochrony* od 1 lipca 2020 r. na skutek zawarcia umowy[143] na fizyczną ochronę osób i mienia;
- doprecyzowania, w których lokalizacjach prowadzona jest kontrola polegająca na przejściu przez stacjonarny detektor do wykrywania metali oraz kontrola bagażu. Działania te są bowiem podejmowane tylko w 2 budynkach Ministerstwa, a nie wszystkich obiektach;
- obowiązku ewidencji wejść zstępnych pracowników.

Ponadto usługi profesjonalnej całodobowej ochrony fizycznej osób i mienia w obiektach MRiPS świadczone były przez wyspecjalizowaną firmę w ramach zawartej umowy[144], która regulowała szczegółowe wymogi w tym zakresie.

28. Wdrożono rozwiązania zapewniające rejestrację ruchu osobowego na terenie Ministerstwa, w tym pozwalające na jego kontrolę. Wprowadzenie różnych rodzajów kart dostępu dla poszczególnych grup interesantów ułatwiało tę kontrolę. Uregulowania wymagają przejazdy samochodami pracowników Uniwersytetu Warszawskiego przez parking MRiPS. Zasadnym byłoby również odnotowywanie wejść dzieci pracowników na teren budynku.

Dostęp do obiektów odbywał się na podstawie magnetycznych kart dostępu. Wdrożono 6[145] rodzajów takich kart dla różnych grup interesantów. Wszystkie karty podlegały obowiązkowi rejestracji, w tym przypisaniu ich do konkretnej osoby, zatem dysponowano informacjami pozwalającymi na ustalenie, kto i kiedy przemieszczał się po obiektach Ministerstwa.

Do sporządzania kart, nadawania uprawnień oraz kontroli dostępu wykorzystywany był system informatyczny, który umożliwiał nadanie uprawnień do wybranych miejsc oraz gromadził dane ze wszystkich przejść. Pozwalał też na generowanie raportów nt. zdarzeń konkretnego pracownika[146] bądź zdarzeń na konkretnym przejściu. Rejestrował także zdarzenia nieuprawnionych prób dostępu, tj. użycia karty dostępu na przejściu, do którego pracownik nie posiadał uprawnień. W przypadku pracowników kończących pracę w MRiPS blokada dostępu następowała ostatniego dnia pracy, przy zdawaniu identyfikatora.

Z przejazdów przez parking Ministerstwa korzystali pracownicy Uniwersytetu Warszawskiego (dalej: UW). Spowodowane to było zablokowaniem wjazdu na ich parking przez roboty rozbiórkowe oraz budowlane.

Wyjaśniono[147], że potwierdzono listę samochodów i użytkowników korzystających z tego przejazdu, jak również przekazano ją pracownikom ochrony. Wskazano także, że w związku

[140] Wyjaśnienia z 6 lipca 2021 r., znak: BKA-II.081.23.12.2021.IK.
[141] Wprowadzona zarządzeniem nr 2 Dyrektora Generalnego MRPiPS z dnia 13 marca 2017 r.
[142] Zarządzenie nr 22 Ministra RPiPS z dnia 31 lipca 2020 r. w sprawie ustalenia regulaminu organizacyjnego MRPiPS.
[143] Umowa nr 10/BA/US/2020/1 z 18 czerwca 2020 r.
[144] Umowa nr 10/BA/US/2020/1 z 18 czerwca 2020 r.
[145] Wśród nich były: 1. identyfikatory dla pracowników; 2. karty wstępu GOŚĆ – dot. osób jednorazowo wchodzących do Ministerstwa; 3. karta wstępu WYKONAWCA – dot. osób wykonujących cykliczne prace w założonym czasie (np. osoby sprzątające); 4. karta wstępu STAŻYSTA – dot. osób, które świadczą usługi nieodpłatnie (wolontariusze, praktykanci, stażyści); 5. karta wstępu KARTA WSTĘPU – dot. pracowników jednostek podległych i nadzorowanych; 6. karta wstępu AGENT OCHRONY – dot. pracowników ochrony.
[146] Przeszukiwanie zdarzeń danych osób w systemie możliwe jest na podstawie wielu różnych kryteriów, między innymi po generowanym przez System indywidualnych numerach systemowych, nazwisku, numerach kadrowych.
[147] Wyjaśnienia 6 lipca 2021 r., znak: BKA-II.081.23.12.2021.IK.

z przejęciem nieruchomości MRiPS przez Ministerstwo Rozwoju, Pracy i Technologii przekazano nowemu jej użytkownikowi informacje o konieczności pilnego uregulowania i ewidencjonowania tych przejazdów. Mając na uwadze ponowne przejęcie działu *praca*, tym samym ponowne przejęcie tej nieruchomości, MRiPS powinno uregulować kwestie korzystania z parkingu przez pracowników UW.

Na teren Ministerstwa nie miały wstępu osoby niepełnoletnie, z wyjątkiem dzieci pracowników. Wejścia te nie były rejestrowane w *Książce kontroli ruchu osobowego* i nie była wydawana karta wstępu. Tym samym nie posiadano pełnych informacji nt. osób przebywających w danym dniu na terenie Ministerstwa.

Wyjaśniono[148], że dzieci pracowników mogą wejść na teren MRiPS wyłącznie pod nadzorem pracownika. Najczęściej nie posiadają one dowodów tożsamości, a jedynymi osobami mogącymi potwierdzić ich tożsamość są pracownicy. Wskazać należy, że możliwość wejść dzieci pracowników nie budzi wątpliwości, natomiast Ministerstwo powinno posiadać informacje w tym zakresie, w szczególności na wypadek sytuacji nadzwyczajnych np. związanych z ewakuacją.

29. Plombowanie pomieszczeń w celu zwiększenia bezpieczeństwa informacji w nich przetwarzanych było właściwe. Zasadnym byłoby wprowadzenie obowiązku ich ewidencji.

W MRiPS w sytuacjach tego wymagających, plombowano pomieszczenia. Nie prowadzono jednak ich ewidencji / wykazu. Po zaplombowaniu pomieszczenia klucze do niego przechowywano w plombowanych woreczkach na recepcji, a ich pobranie / zdanie podlegało obowiązkowi rejestracji. Wydanie / zdanie kluczy w stosunku do pozostałych pomieszczeń nie było ewidencjonowane. Wyjaśniono[149], że chodziło o takie zabezpieczenie tych pomieszczeń, aby wszystkie czynności w nich wykonywane były realizowane w obecności uprawnionego pracownika, np. sprzątanie, naprawy, konserwacje klimatyzatorów, itp.

Plombowanie pomieszczeń zwiększało bezpieczeństwo informacji, jednak brak ich ewidencji nie zapewniał szybkiego dostępu do informacji potrzebnych w sytuacjach podejmowania określonych działań w zakresie tych pomieszczeń oraz pozbawiał Ministerstwo informacji nt. zasadności / celowości zastosowania tego rodzaju zabezpieczenia.

30. Pracownicy recepcji nie posiadali pełnych informacji, kto jest uprawniony do pobrania kluczy i do jakich konkretnie pomieszczeń, w tym pomieszczeń plombowanych, co zwiększało ryzyko nieuprawnionego dostępu. *Baza danych o pomieszczeniach zajmowanych przez pracowników* nie zawierała informacji w odniesieniu do sal konferencyjnych i pomieszczeń technicznych, jak również nie były w niej zaznaczone pomieszczenia plombowane.

Klucze wydawane i przyjmowane były przez pracownika recepcji[150]. W przypadku wątpliwości co zasadności pobrania kluczy pracownik recepcji mógł zweryfikować takie żądanie przez dostęp do *Bazy danych o pomieszczeniach zajmowanych przez pracowników* prowadzonej w programie *IBM Lotus Notes.* Nie była to jednak pełna informacja, ponieważ baza ta nie zawierała informacji kto ma dostęp do pobrania kluczy do sal konferencyjnych, pomieszczeń technicznych. Ponadto baza ta wskazywała użytkowników danego pomieszczenia, a nie odnosiła się do dostępu do niego przez przełożonych. Wyjaśniono[151], że MRiPS rozważa dokonanie zmian w tych zakresach w *Instrukcji kontroli ruchu osobowego.*

31. Wprowadzono regulacje w zakresie utylizacji/zbycia dokumentacji, sprzętu i nośników danych. W szczególności zawierały one rozwiązania dot. obowiązku trwałego usunięcia danych w przypadkach zbycia / przekazania zasobów IT. Doprecyzowania wymaga jednak zakres stosowania procedury *Niszczenia dokumentacji papierowej oraz nośników informacji pochodzących z systemów informatycznych MRPiPS.*

Za zbycie i utylizację sprzętu odpowiedzialne było Biuro Administracyjne, a za usunięcie danych DI. PBI IT[152] określała zasady w tym zakresie, natomiast warto zwrócić uwagę na zasadność precyzyjnego określenia zakresu stosowania procedury *Niszczenia dokumentacji papierowej oraz nośników informacji pochodzących z systemów*

[148] Wyjaśnienia 6 lipca 2021 r., znak: BKA-II.081.23.12.2021.IK.
[149] Wyjaśnienia 6 lipca 2021 r., znak: BKA-II.081.23.12.2021.IK.
[150] Pracownik firmy zewnętrznej realizujący usługi na podstawie umowy nr 10/BA/US/2020/1 z 18 czerwca 2020 r.
[151] Pismo z 3 sierpnia 2021 r., znak: BKA-II-081.23.26.2021.IK.
[152] § 20 ust. 8-13 zał. nr 1 i zał. nr 10 do PBI IT *Niszczenie dokumentacji papierowej oraz nośników informacji pochodzących z systemów informatycznych MRPiPS.*

informatycznych MRPiPS[153]. PBI IT[154] wskazywała, że ma ona zastosowanie tylko do informacji wrażliwych pod kątem poufności, podczas gdy w praktyce dotyczyła ona także pozostałych informacji[155]. Zasadne było także określenie zasad dot. utylizacji / zbycia sprzętu i nośników danych w zarządzeniach w sprawie: powołania i funkcjonowania komisji oceny przydatności do dalszego użytkowania składników majątkowych w MRiPS[156]; powołania i funkcjonowania komisji do spraw zbycia zbędnych lub zużytych składników majątku ruchomego MRiPS[157]; powołania i funkcjonowania komisji likwidacyjnej w MRiPS[158].

W badanym okresie nie utylizowano sprzętu ani nośników danych, dokonano natomiast nieodpłatnego przekazania sprzętu informatycznego gminie (komputer, urządzenie wielofunkcyjne, UPS). Działania w tym zakresie przebiegły zgodnie z wdrożonymi regulacjami. Dokonano oceny przydatności tego sprzętu[159], a następnie zdecydowano[160] o nieodpłatnym jego przekazaniu, bez zastrzeżenia obowiązku zwrotu. Sprzęt został przekazany na podstawie protokołu[161]. Nie było konieczności usunięcia z niego danych, bowiem wykorzystywany był on przez gminę od 2015 r. na podstawie zawartej umowy użyczenia[162].

32. W przypadku naprawy sprzętu informatycznego zapewniono bezpieczeństwo informacji, w szczególności przez wymontowanie nośnika danych.

W badanym okresie doszło do naprawy 3 notebook-ów, komputera oraz zasilaczy sieciowych. W przypadku 2 notebooków oraz komputera naprawy zrealizowano w siedzibie DI w obecności pracownika Wydziału Systemów Teleinformatycznych i Obsługi Informatycznej[163]. W przypadku 1 naprawy notebooka realizowanej poza siedzibą MRiPS, wymontowano z niego twardy dysk.

33. [zabezpieczenia organizacyjno-techniczne systemów] Pozytywnie należy ocenić zabezpieczenia organizacyjno-techniczne dostępu do serwerowni. Wyposażenie oraz wdrożone rozwiązania w zakresie monitorowania środowiska jej pracy spełniały wysokie standardy, a przyjęte środki ochrony w istotny sposób przyczyniały się do zapewnienia BI. Właściwym działaniem było także wydzielenie pomieszczenia backupu do odrębnej lokalizacji. Ministerstwo powinno jednak rozważyć wzmocnienie zabezpieczeń pomieszczenia backupu oraz jednego z wyjść ewakuacyjnych.

Pomieszczenie serwerowni posiadało szereg zabezpieczeń, w tym: system kontroli dostępu, system zasilania gwarantowanego UPS, instalację wentylacyjną, system klimatyzacji, system kontroli dostępu, system sygnalizacji włamań i napadu, system telewizji przemysłowej CCTV, system gaszenia gazem SUG[164], system wczesnego wykrywania pożaru, czujniki zalania, system zarządzania budynkiem BMS – Building Managment System.

Pomieszczenie backupu wyposażono w systemy zapewniające jego bezpieczeństwo i dostęp jedynie upoważnionym pracownikom. Przyjęte rozwiązania pozwoliły na kontrolę osób w nim przebywających. Nie zainstalowano w nim sytemu gazowego gaszenia pożaru, jednakże wyposażono je w czujniki wykrywania zadymienia oraz gaśnice do sprzętu elektronicznego. Pomimo istniejącego ryzyka zalania, pomieszczenie to nie zostało wyposażone w czujki zalania. Znajdowały się w nim okna, które nie posiadały dodatkowych zabezpieczeń. Wyjaśniono[165], że do backupu wybrano najlepiej dostosowane do tego celu pomieszczenie. Zaakceptowano ryzyko związane z brakiem wszystkich zabezpieczeń uznając, że jest ono mniejsze od ryzyka związanego z pozostawieniem tego pomieszczenia bez rozdzielania od serwerowni.

W odniesieniu do wyjścia ewakuacyjnego wskazano[166], że budynek ten podlega całodobowej ochronie. Wyłączone jest ono z bieżącego użytkowania i służy wyłącznie w czasie ewakuacji.

Pomieszczenie backupu stanowi istotne miejsce w zakresie bezpieczeństwa informacji, a wyjście ewakuacyjne prowadzi na teren ogólnodostępny, w związku z czym Ministerstwo powinno rozważyć wzmocnienie ich zabezpieczeń.

---

[153] Załącznik nr 10 do PBI IT.
[154] § 20 ust. 9 części II załącznika nr 1 do PBI IT.
[155] Wyjaśnienia z 21 lipca 2021 r., znak: BKA-II.081.23.17.2021.IK.
[156] Zarządzenie nr 2 Dyrektora Generalnego MRiPS z dnia 2 marca 2021 r., zmienione zarządzeniem nr 11 z dnia 16 kwietnia 2021 r.
[157] Zarządzenie nr 12 Dyrektora Generalnego MRiPS z dnia 22 kwietnia 2021 r.
[158] Zarządzenie nr 3 Dyrektora Generalnego MRiPS z dnia 2 marca 2021 r.
[159] Protokół *Komisji oceny przydatności do dalszego użytkowania składników majątkowych* nr 4/2021 z dnia 27 kwietnia 2021 r.
[160] Protokół *Komisji do spraw zbycia zbędnych lub zużytych składników rzeczowych majątku ruchomego* nr 1/2021 z 12 maja 2021 r.
[161] Protokół zdawczo-odbiorczy nr 1/2021 z dnia 14 maja 2021 r.
[162] Umowa nr 1797/MRPiPS/KDR/2015 z dnia 2 września 2015 r.
[163] Wyjaśnienia z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[164] SUG - Stałe Urządzenia Gaśnicze – jest to automatyczna instalacja przeciwpożarowa która samoczynnie wykrywa i sygnalizuje pożar we wczesnej jego fazie rozwoju oraz rozpoczyna akcję gaśniczą w chronionej strefie.
[165] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[166] Pismo z 6 lipca 2021 r., znak: BKA-II.081.23.12.2021.IK.

34. Ministerstwo sukcesywnie w ramach dostępnych środków wymieniało sprzęt komputerowy z systemem operacyjnym, dla którego producent nie zapewniał wsparcia w postaci poprawek bezpieczeństwa (*Windows 7*). Czynności te wymagają kontynuacji, bowiem na 76 z 771 (10%) użytkowanych komputerach nadal jest zainstalowany ten system.

> Wyjaśniono[167], że w br. planowana jest wymiana wszystkich komputerów z systemem operacyjnym Windows 7.

Brak możliwości aktualizacji oprogramowania prowadzi do znacznego wzrostu ryzyka ataków, a tym samym zagraża BI gromadzonych i przetwarzanych w Jednostce.

35. Zapewnienie bezpieczeństwa systemów wzmacniały także wdrożone działania w zakresie ochrony antywirusowej oraz antyspamowej. Zasadnym byłoby jednak uwzględnienie w regulacjach przyjętych rozwiązań antyspamowych. Proces ochrony antywirusowej został uregulowany[168].

> Oprogramowanie antywirusowe zapewniało automatyczną aktualizację na użytkowanym sprzęcie przez pracowników. Nie była wymagana interakcja użytkownika[169]. Natomiast oprogramowanie antyspamowe zapewniało ochronę poczty elektronicznej dzięki integracji wielowarstwowego systemu antyspamowego i funkcji filtrowania reputacji z programami antywirusowymi i antyszpiegowskimi. Wskazano że[170], że PBI IT zostanie przy najbliższej aktualizacji uzupełniona o postanowienia dot. ochrony poczty przed tzw. spamem.

36. **[plan ciągłości działania]** Plan ciągłości działania był w trakcie opracowania. Powołano Zespół ds. wypracowania rozwiązań zapewniających ciągłość działania, który przygotował projekt zasad oraz inwentaryzację procesów, następnie prace były kontynuowane przez Zespół ds. zarządzania ryzykiem. Planowano, że prace zakończą się w IV kw. 2021 r.

> W pierwszej kolejności prace Zespołu ds. wypracowania rozwiązań zapewniających ciągłość działania dot. ustalenia harmonogramu działań oraz aktualizacji procedury zgłaszania przypadków zachorowania przez pracowników na COVID-19. Zespół ocenił regulacje pod kątem rozwiązań służących zapewnieniu ciągłości działania.
>
> Ustalono, że w Jednostce obowiązują przede wszystkim regulacje związane z zarządzaniem kryzysowym, obronnym oraz w przypadku wystąpienia zdarzeń nadzwyczajnych, tj. pożar, powódź, atak terrorystyczny, demonstracje przed siedzibą, itp. Stwierdzono również, że zidentyfikowane procedury określają głównie zadania MRiPS w przypadku wystąpienia stanu wyjątkowego lub też służą ochronie zasobów. Zatem nie dotyczą one bezpośrednio utrzymania ciągłości działania Ministerstwa, zgodnie z przyjętą definicją zachowania ciągłości działania. Prace Zespołu zakończyły się z końcem maja 2021 r. Będą one kontynuowane przez Zespół ds. zarządzania ryzykiem.
>
> Jednym z efektów prac zespołu ds. ciągłości działania było przygotowanie projektu zasad zapewnienia ciągłości działania oraz inwentaryzacja procesów, które wspierają ciągłość działalności jednostki[171].

37. **[rozliczalność]** W celu identyfikacji działań niepożądanych prowadzono przegląd logów oraz ich analizę. Brakowało jednak całościowych regulacji wewnętrznych zawierających zasady prowadzenia i wykorzystania dzienników systemów (logów), w tym określających zakres danych podlegających dokumentowaniu w dziennikach.

> W PBI IT wskazano jedynie ogólne postanowienia dot. obowiązku stosowania indywidualnych kont w celu zachowania rozliczalności[172], systematycznego przeglądania logów[173], możliwości rekonstrukcji istotnych działań użytkowników w celu ograniczenia nadużyć[174], obowiązku posiadania dziennika administratora[175] i rejestracji istotnych/wrażliwych danych[176]. Wyjaśniono[177], że decyzja o niewdrożeniu regulacji, zawierających zasady prowadzenia i wykorzystania dzienników systemów (logów), w tym określających zakres danych

[167] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[168] § 17 części II załącznika nr 1 do PBI IT oraz § 10 części II załącznika nr 2 do PBI IT.
[169] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[170] Pismo z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[171] Wyjaśnienia z 3 sierpnia 2021 r., znak: BKA-II.081.23.25.2021.IK.
[172] § 22 ust. 6 części II załącznika nr 1 do PBI IT.
[173] § 24 ust. 5 części II załącznika nr 1 do PBI IT.
[174] § 24 ust. 11 części II załącznika nr 1 do PBI IT.
[175] § 18 ust. 11 części II załącznika nr 1 do PBI IT.
[176] § 24 ust. 9 i 10 części II załącznika nr 1 do PBI IT.
[177] Pismo z 15 lipca 2021 r., znak DI.III.081.5.16.2021.PW.

podlegających dokumentowaniu w dziennikach, została podjęta w sposób celowy. Podjęto ją ze względu na liczbę oraz różnorodność eksploatowanych i użytkowanych systemów, a także bieżące potrzeby monitoringu. Przyjęto, że zamieszczenie takich zapisów na poziomie sztywnych postanowień w regulacjach Ministerstwa spowodowałoby usztywnienie i całkowity brak reagowania na aktualne potrzeby i możliwości oraz wiedzę pozyskaną z doświadczenia nabytego w trakcie realizacji monitoringu.

Nie można zgodzić się ze stanowiskiem, że ustalenie ogólnych zasad prowadzenia i wykorzystania dzienników systemów, w tym określających minimalny zakres danych podlegających dokumentowaniu w dziennikach spowoduje usztywnienie i całkowity brak reagowania na aktualne potrzeby Jednostki. Ogólne regulacje stworzą ramy do efektywnego działania. Zakres danych podlegających dokumentowaniu w postaci zapisów w dziennikach systemów w każdej jednostce może być różny i wynikać z jej indywidualnych potrzeb, w szczególności zidentyfikowanych na etapie analizy ryzyka. Zatem minimalne wymogi w tym zakresie powinny zostać określone.

DI do monitoringu funkcjonowania zarówno środowiska systemowego, jak i poszczególnych systemów wykorzystywał narzędzia monitorowania zdarzeń i zautomatyzowanej analizy logów systemowych. System monitoringu oparty jest na mechanizmach zbierania i ewentualnej agregacji tych logów. Poszczególne dashboardy oraz wykresy zostały specjalnie zdefiniowane, po przeprowadzeniu wcześniejszej analizy, jakie mierniki i wskaźniki są dla poprawności monitoringu istotne i niezbędne. Mogą być one skalowane i na bieżąco konfigurowane, zgodnie z potrzebami osób monitorujących[178].

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

II. Wymiana informacji w postaci elektronicznej

38. [Usługi elektroniczne] Ministerstwo świadczyło usługi elektroniczne i zapewniało komunikację elektroniczną przez skrzynkę podawczą na platformie ePUAP[179]. Spełniono zatem wymogi określone w art. 16 ust. 1a ustawy o informatyzacji.

MRiPS świadczy 26 usług elektronicznych. Opublikowane zostały opisy procedur obowiązujących przy załatwianiu spraw drogą elektroniczną.

39. [Centralne Repozytorium Wzorów Dokumentów Elektronicznych (CRWDE)] W ramach realizacji 26 usług elektronicznych korzystano z 32 własnych wzorów dokumentów elektronicznych oraz 21 opracowanych i opublikowanych w CRWDE przez inny podmiot publiczny. Jednakże 6 z 32 (19%) własnych wzorów nie zostało przekazanych do CRWDE i nie opublikowano ich na stronie BIP, tym samym nie spełniono obowiązku określonego w art. 19b ust. 3 ustawy o informatyzacji.

Wyjaśniono[180], że nieprzekazanie 6 wzorów[181] do CRWDE wynikało z niedopatrzenia. Wzory te zostaną niezwłocznie przekazane.

40. [Model usługowy] Proces świadczenia usług elektronicznych przez 3 badane systemy teleinformatyczne realizowany był zgodnie z § 15 ust. 2 Rozporządzenia KRI. Zarządzanie usługami odbywało się bowiem w oparciu o udokumentowane procedury, które zostały ujęte w umowach oraz w specyfikacji technicznej systemów.

Dla 3 badanych systemów stosuje się rozwiązania oparte na modelu usługowym. Procedury obsługi, odpowiedzialność za utrzymanie usługi od strony technicznej, poziom świadczenia usługi, wskaźniki jej dostępności, a także wskaźniki dostępności i mechanizmy reagowania na ich przekroczenie ujęte są w umowach oraz w specyfikacji technicznej systemów, za pomocą których usługi elektroniczne są realizowane.

Wyjaśniono[182], że użytkowane systemy wykorzystujące elektroniczne usługi wymiany danych, budowane są w oparciu o architekturę SOA. Według MRiPS model SOA jest w pełni wdrożony i oparty o platformę integracyjną oraz dwie szyny danych ESB, gdzie wbudowany jest również system zarządzania i udostępniania usług.

---

[178] Wyjaśnienia z 15 lipca 2021 r., znak: DI.III.081.5.16.2021.PW.
[179] Dokumenty elektroniczne mogą być doręczane za pomocą ESP dostępnej na Elektronicznej Platformie Usług Administracji Publicznej (ePUAP) pod adresem:/4g447ytes7/skrytka oraz https://www.gov.pl/web/rodzina/kontakt-elektroniczna-skrzynka-podawcza https://www.gov.pl/web/gov/uslugi-dla-obywatela.
[180] Pismo z 29 lipca 2021 r., znak: BKA-II.081.23.22.2021.IK wraz z załącznikiem.
[181] Wzory: ZSR-05; ZDKR-01; ZDKR-02; ZDKR-03; ZDKR-04; RKZ-4.
[182] Pismo z 11 sierpnia 2021 r., znak: BKA-II.081.23.29.2021.IK.

41. [Współpraca systemów teleinformatycznych z innymi systemami] W badanych systemach stosowane były odwołania do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań zgodnie z § 5 ust. 3 pkt 3 Rozporządzenia KRI. Sposób komunikacji z innymi systemami, w tym wyposażenie w składniki sprzętowe i oprogramowanie umożliwiał badanym systemom wymianę danych z innymi systemami, spełniając tym samym wymogi § 16 ust. 1 tego rozporządzenia.

> CSIZS komunikuje się z systemami: Domu Maklerskiego PKO BP (dane o kwotach przyznanych świadczeń 500+); Rejestrami Państwowymi (Ministra Cyfryzacji) – PESEL (dane osobowe); Zakładu Ubezpieczeń Społecznych (dane o składkach na ubezpieczenie zdrowotne i społeczne oraz o świadczeniach z ZUS); Ministerstwa Finansów (dane o dochodach podatników); Centralną Ewidencją i Informacją o Działalności Gospodarczej (dalej: CEIDG – dane osoby prowadzącej działalność gospodarczą); Krajowym Rejestrem Sądowym (dalej: KRS – dane podmiotu prowadzącego działalność gospodarczą); Aplikacją Centralną Rynku Pracy (dane o bezrobotnych); Narodowego Funduszu Zdrowia (dane o uprawnieniach do świadczeń opieki zdrowotnej); Kasy Rolniczego Ubezpieczenia Społecznego (dane o składkach na ubezpieczenie zdrowotne); Ministerstwa Edukacji i Nauki (dane o uczniach i studentach); EKSMOoN (dane dot. orzeczeń o niepełnosprawności; systemy bankowości elektronicznej, PIU Emp@tia.
>
> PIU Emp@tia wymienia dane z CSIZS; Login.gov.pl (dane autoryzacyjne klientów chcących korzystać z usług elektronicznych); Rejestrem Żłobków oraz SI KDR w zakresie częściowego pozyskania danych służących do autouzupełnienia formularzy.
>
> SI KDR wymienia dane z systemami: PESEL; CEIDG; Systemem Informacji Oświatowej; KRS; EKSMOoN w zakresie weryfikacji i partnerów programu.

42. [Formaty danych udostępnianych przez systemy teleinformatyczne] Sposób kodowania znaków w dokumentach wysyłanych i odbieranych przez badane systemy, a także wymienianych informacji z innymi systemami w drodze teletransmisji, realizowany był zgodnie z § 17 ust. 1 Rozporządzenia KRI. Badane systemy udostępniały zasoby informacyjne, spełniając wymogi § 18 ust. 1 Rozporządzenia KRI.

> W badanych systemach obsługiwane były w szczególności formaty danych: .txt, .pdf, .xls, .csv, .jpg, .jpeg, .png, .zip, .xml, .xsd, .xsl, .xslt, .XAdES. Jednocześnie wskazano[183], że w przypadku, gdyby użytkownik (obywatel) w ramach usługi elektronicznej chciał przekazać załącznik, ma możliwość złożenia go w dowolnym formacie danych wskazanym w Rozporządzeniu KRI.

43. [Obieg dokumentów w podmiocie] Pozytywnie należy ocenić, że w Ministerstwie podstawowym sposobem dokumentowania czynności kancelaryjnych jest EZD[184], co jest zgodne z § 20 ust. 2 pkt 9 Rozporządzenia KRI. Wyjątki od tej zasady zostały udokumentowane.

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

1. Zmianę procesu ustanawiania i eksploatacji kompleksowego, spójnego systemu zarządzania bezpieczeństwem informacji uwzględniającego poufność, dostępność, integralność gromadzonych i przetwarzanych informacji, w tym:
   - ustanowienie systemu zarządzania ryzykiem zapewniającego cykliczną identyfikację ryzyk oraz opracowanie planu postępowania z ryzykiem,
   - przegląd oraz uzupełnienie procedur i regulacji wewnętrznych dotyczących *SZBI*,
   - zapewnienie systemowych rozwiązań mających na celu identyfikację wszystkich słabości tego systemu,
   - utworzenie pełnej bazy konfiguracji CMDB,

[183] Wyjaśnienia z 29 lipca 2021 r., znak: BKA-II.081.23.22.2021.IK.
[184] § 3 ust. 1 Instrukcji kancelaryjnej Ministerstwa Rodziny, Pracy i Polityki Społecznej stanowiącej załącznik nr 1 do zarządzenia nr 38 Ministra Rodziny, Pracy i Polityki Społecznej z dnia 12 grudnia 2019 r. w sprawie ustalenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt i instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego Ministerstwa Rodziny, Pracy i Polityki Społecznej.

- opracowanie planów ciągłości działania na wypadek wystąpienia zdarzeń zagrażających realizacji zadań,
- wprowadzenie skutecznych narzędzi niezwłocznego odbierania uprawnień po zakończeniu zatrudnienia.

2. Wdrożenie narzędzi i mechanizmów zarządczych zapewniających efektywny nadzór w procesie ustanawiania, eksploatacji i doskonalenia *SZBI* oraz dokonywanie okresowej ewaluacji tego procesu.

3. Prawidłowe zabezpieczenie interesów Ministerstwa w zawieranych umowach, w tym wprowadzenie przykładowego katalogu postanowień gwarantujących odpowiedni poziom ochrony i bezpieczeństwa informacji.

4. Zintensyfikowanie działań mających na celu dostosowanie form szkoleniowych do sytuacji epidemiologicznej dla zapewnienia cykliczności w procesie podnoszenia świadomości pracowników w obszarze bezpieczeństwa informacji.

5. Wyeliminowanie pozostałych problemów 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-/