MINISTER
Rodziny i Polityki Społecznej

Warszawa /elektroniczny znacznik czasu/

BKA-II.081.23.31.2021.IK

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

Szanowny Panie Ministrze,

w odpowiedzi na wystąpienie pokontrolne znak: DNK.WK.1743.1.2021.MJ dotyczące kontroli przeprowadzonej przez Kancelarię Prezesa Rady Ministrów w Ministerstwie Rodziny i Polityki Społecznej w zakresie *wykorzystania systemów teleinformatycznych do realizacji zadań publicznych w okresie od 6 października 2020 r. do 30 lipca 2021 r.* niniejszym przedstawiam informacje o sposobie wykonania zaleceń, wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Ad zalecenie nr 1

Zmiana 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,*
  W celu realizacji zalecenia Ministerstwo opracuje i wdroży stosowne procedury w obszarze IT w II kwartale 2022 r.
- *przegląd oraz uzupełnienie procedur i regulacji wewnętrznych dotyczących Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).*
  W celu realizacji zalecenia wykonany zostanie przegląd posiadanych obecnie procedur związanych z funkcjonowaniem SZBI oraz zostaną przygotowane projekty zmian i uzupełnień obecnie funkcjonujących regulacji, tak aby do końca I kwartału br. zostały wprowadzone w życie. Ponadto, zostanie przygotowany opis SZBI, który będzie miał

charakter informacyjny i będzie adresowany przede wszystkim dla nowych pracowników Ministerstwa.

- *zapewnienie systemowych rozwiązań mających na celu identyfikację wszystkich słabości tego systemu,*

W związku z prowadzoną co roku aktualizacją wyników procesu analizy ryzyka i zadaniami Zespołu ds. zarządzania ryzykiem w perspektywie najbliższego kwartału, a następnie w okresie do końca br. zostaną przygotowane i wdrożone rozwiązania, które będą miały na celu realizację niniejszego zalecenia. W I etapie prac zostanie zwrócona szczególna uwaga wszystkim komórkom organizacyjnym Ministerstwa, aby podczas procesu analizy ryzyka oceną objęto poszczególne elementy SZBI, zgodnie z zakresem ich zadań i kompetencji. Na podstawie zebranych danych, w II etapie, o ile okaże się to niezbędne, zostaną zainicjowane prace mające na celu wdrożenie systemowych rozwiązań, które pozwolą na identyfikację słabości systemu.

- *utworzenie pełnej bazy konfiguracji CMDB.*

Ministerstwo podjęło działania zmierzające do scalenia (tam gdzie będzie to możliwe) posiadanych informacji w zakresie bazy konfiguracji (CMDB). W tym celu w pierwszym etapie zostanie wdrożone narzędzie, które scentralizuje informacje o stacjach roboczych. Działania te zostaną zrealizowane w I kwartale 2022 r. W dalszej kolejności, na bazie posiadanego już rozwiązania działania scalające obejmą urządzenia mobilne. Kolejne działania będą zmierzać do scentralizowania posiadanych informacji stanowiących zasób bazy konfiguracji w zakresie infrastruktury serwerowej, a termin ich realizacji będzie uzależniony od sytuacji finansowej jednostki.

Zostaną opracowane regulacje odnoszące się do sposobu i zakresu gromadzonych w bazie CMBD danych. Planuje się, że regulacje zostaną opracowane w terminie do końca II kwartału 2022 r.

- *opracowanie planów ciągłości działania na wypadek wystąpienia zdarzeń zagrażających realizacji zadań,*

Ze względu na zmiany organizacyjne i przeniesienie części „Praca” z Ministerstwa Rozwoju, Pracy i Technologii do Ministerstwa Rodziny i Polityki Społecznej, a tym samym na konieczność uwzględnienia celów i zadań komórek organizacyjnych z ww. części budżetowej planowane jest opracowanie przedmiotowego dokumentu w II kwartale 2022 r.

- *wprowadzenie skutecznych narzędzi niezwłocznego odbierania uprawnień po zakończeniu zatrudnienia,*

W celu skutecznej realizacji procesu odbierania uprawnień po zakończeniu zatrudnienia Ministerstwo zaproponuje rozwiązania organizacyjne i techniczne poprzez opracowanie procedur powiadamiania pracowników servicedesk drogą elektroniczną o rozwiązaniu stosunku pracy z pracownikiem i odbierania uprawnień/dostępów do zasobów przez Administratorów Systemu Informatycznego. Proponowane rozwiązania zostaną uzgodnione z komórkami organizacyjnymi Ministerstwa, a po uzyskaniu ich akceptacji wdrożone do stosowania. Planuje się, że zmiany organizacyjne w tym zakresie zostaną opracowane do końca II kwartału 2022 r.

Ad zalecenie nr 2

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

Pierwszym elementem wdrożenia zalecenia będzie etap monitorowania i oceny wdrożenia zaleceń i uwag zawartych w niniejszym wystąpieniu przez Biuro Kontroli i Audytu w Ministerstwie w bieżącym roku. Na podstawie wyników analizy ryzyka, prowadzonego monitoringu wdrożenia zaleceń zostaną przygotowane propozycje rozwiązań o charakterze zarządczym, które zapewnią stały i efektywny nadzór nad SZBI. Pozwolą one na prowadzenie cyklicznej ewaluacji tego obszaru, którego składowymi będą m.in. realizowane zadania audytowe i kontrolne w tym obszarze.

Ad zalecenie nr 3

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

W ramach planowanych zamówień Departament Informatyki będzie na bieżąco uzgadniał z właściwymi komórkami organizacyjnymi MRiPS zapisy umów w zakresie wymaganym przez prawo zamówień publicznych, finansów publicznych, danych osobowych. We współpracy z właściwymi komórkami organizacyjnymi Ministerstwa zostaną wypracowane zapisy w zakresie utworzenia katalogu postanowień umownych, które obejmą postanowienia gwarantujące odpowiedni poziom ochrony i bezpieczeństwa informacji w celu prawidłowego zabezpieczenie interesów Ministerstwa w zawieranych umowach.

Ad zalecenie nr 4

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

Ministerstwo przygotowało narzędzie do realizacji szkolenia w formie e-learning w zakresie podnoszenia świadomości pracowników w obszarze bezpieczeństwa informatycznego. Szkolenie zostanie zorganizowane i przeprowadzone do końca lutego br.

Ad zalecenie nr 5

Wyeliminowanie pozostałych problemów wskazanych w Wystąpieniu.

Incydenty. *Nie sporządzano dokumentacji z działań w zakresie rejestracji i analizy incydentów, a regulacje z tego obszaru nie zostały zaktualizowane i uzupełnione.*

W ramach aktualizacji Polityki Bezpieczeństwa Informacji IT zostanie ujednolicona definicja incydentu bezpieczeństwa, zostaną wskazane aktualne kanały zgłaszania incydentów bezpieczeństwa oraz zostaną określone informacje konieczne do rejestracji i obsługi incydentu bezpieczeństwa. Planuje się dokonanie aktualizacji PBI IT w tym zakresie do końca I kwartału 2022 r.

Zapewnienie wiedzy pracownikom. *Kontynuacji wymagają działania dotyczące zwiększenia świadomości pracowników w zakresie BI.*

W ramach aktualizacji Polityki Bezpieczeństwa Informacji IT zostaną wprowadzone zapisy, które będą zobowiązywały wszystkich pracowników do zapoznania się regulacjami w zakresie procedury zgłaszania incydentów bezpieczeństwa informatycznego. Planuje się dokonanie aktualizacji PBI IT w tym zakresie do końca I kwartału 2022 r.

Rozliczalność działań. *Należy zadbać o opracowanie całościowych regulacji zawierających zasady prowadzenia i wykorzystania dzienników systemów (logów), w tym określających zakres danych podlegających dokumentowaniu w dziennikach.*

W ramach posiadanych umów na wsparcie i rozwój systemów teleinformatycznych Ministerstwo podejmie działania związane opracowaniem regulacji wewnętrznych określających zakres danych podlegających dokumentowaniu w dziennikach. Opracowanie regulacji planuje się zrealizować do końca II kwartału 2022 r. Należy jednak mieć na uwadze różnorodność każdego z eksploatowanych w MRiPS systemów teleinformatycznych, a także uwarunkowania budżetowe, niezbędne do zapewnienia infrastruktury do realizacji tych regulacji. Wobec powyższego wdrożenie regulacji w systemach będzie realizowane sukcesywnie, adekwatnie do posiadanych środków budżetowych, które pozwolą na wprowadzenie stosownych zmian w systemach.

Projektowanie, eksploatacja oraz wdrażanie zmian w systemach. *Wyeliminowanie problemów 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.*
W ramach aktualizacji PBI IT zostaną doprecyzowane zapisy dotyczące procesu wdrażania zmian w systemach teleinformatycznych, w szczególności związane z zapewnieniem chronologii wpisów w zakresie wprowadzanych do systemów zmian. Planuje się dokonanie aktualizacji PBI IT, w tym zakresie do końca I kwartału 2022 r.

Zabezpieczenia organizacyjno-techniczne dostępu do informacji. *Z powodu zmian organizacyjnych aktualizacji wymagają regulacje dotyczące minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji, z uwzględnieniem zasad ochrony fizycznej.*
W celu zwiększenia bezpieczeństwa informacji przetwarzanych w pomieszczeniach plombowanych należy wprowadzić obowiązek ewidencji tych pomieszczeń oraz zasady zarządzania kluczami, w tym zasady dostępu do danego pomieszczenia przez poszczególnych pracowników.
Zagadnienia te znajdują swoje odzwierciedlenie w nowo projektowanej *Instrukcji kontroli ruchu osobowego i materiałowego oraz organizacji ruchu pojazdów i przydziału miejsc parkingowych*, która aktualnie jest na etapie konsultacji wewnętrznych. Planowany termin wejścia w życie nowych regulacji to I kwartał 2022 r.

Zabezpieczenia organizacyjno-techniczne systemów. *Ministerstwo powinno rozważyć wzmocnienie zabezpieczeń pomieszczenia backupu oraz wyjść ewakuacyjnych.*

Drzwi wyjściowe w budynku Ministerstwa, o których mowa w wystąpieniu pokontrolnym zostaną wzmocnione, m.in. poprzez wymianę wadliwego zamka, a także instalację dodatkowego zabezpieczenia.

Wykonane zostanie wzmocnienie zabezpieczeń pomieszczenia, o którym mowa w treści wystąpienia pokontrolnego poprzez zamontowanie samozamykacza. Od 5 stycznia br. pomieszczenie nr 405 zostało wyposażone w metalową szafę, która jest używana do przechowywania taśm backupowych.
Realizacja zalecenia w pełnym zakresie planowana jest do końca 2022 r.
Zapisy dotyczące przyjętych rozwiązań antyspamowych poczty elektronicznej zostaną umieszczone w aktualizacji PBI IT.

Z poważaniem

Minister

z up. Stanisław Szwed

Sekretarz Stanu

/-podpisano kwalifikowanym podpisem elektronicznym/