NACZELNY DYREKTOR
ARCHIWÓW PAŃSTWOWYCH
Paweł Pietrzyk

Warszawa, dnia 28 maja 2024 r.

WYSTĄPIENIE POKONTROLNE

Znak kontroli	DOA.084.2.2024
Nazwa i adres jednostki kontrolowanej	Archiwum Państwowe w Bydgoszczy ul. Mieczysława Karłowicza 17 85-092 Bydgoszcz
Temat kontroli	Wybrane aspekty dotyczące bezpieczeństwa teleinformatycznego w Archiwum Państwowym w Bydgoszczy
Tryb kontroli	Zwykły
Podstawa prawna kontroli	1. Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (tj. Dz. U. z 2020 r. poz. 224). 2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2023 r., poz. 57). 3. Plan Kontroli Naczelnego Dyrektora Archiwów Państwowych na rok 2024.
Zakres kontroli	Ocena wybranych aspektów dotyczących bezpieczeństwa teleinformatycznego zawartych w Krajowych Ramach Interoperacyjności oraz realizacji obowiązków nałożonych na podmioty publiczne w ramach krajowego systemu cyberbezpieczeństwa
Okres objęty Kontrolą	01.01.2023 r. – 29.02.2024 r. z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowany obszar działalności
Próba poddana kontroli	Dokumentacja wytworzona przez Archiwum Państwowe w Bydgoszczy z kontrolowanego obszaru oraz przeprowadzenie testu konfiguracji usługi Microsoft Active Directory oraz zapory sieciowej – Firewall

Data rozpoczęcia i zakończenia czynności kontrolnych	11.03.2024 r. – 26.04.2024 r.
Imię, nazwisko i stanowisko służbowe kontrolera	1. [redacted], główny specjalista w Departamencie Organizacji Archiwów Naczelnej Dyrekcji Archiwów Państwowych, kierownik zespołu kontrolerów, upoważnienie nr 4/2024 z dnia 8 marca 2024 r. 2. [redacted], główny specjalista w Departamencie Informatyzacji Archiwów Naczelnej Dyrekcji Archiwów Państwowych, członek zespołu kontrolnego, upoważnienie nr 5/2024 z dnia 8 marca 2024 r. 3. [redacted], główny specjalista w Departamencie Informatyzacji Archiwów Naczelnej Dyrekcji Archiwów Państwowych, członek zespołu kontrolnego, upoważnienie nr 6/2024 z dnia 8 marca 2024 r.
Kierownictwo jednostki kontrolowanej	Pan Eugeniusz Borodij, powołany na stanowisko Dyrektora Archiwum Państwowego w Bydgoszczy dnia 1.01.2005 r.
Wykaz aktów prawnych regulujących przedmiot kontroli	1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2023 r. poz. 57 z późn. zm.). 2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2023 r. poz. 913 z późn. zm.) – dalej ustawa KSC. 3. 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 (tj. Dz.U. z 2017 r. poz. 2247) – dalej rozporządzenie KRI.
Ogólna ocena kontroli	**Ocena negatywna**

W toku kontroli stwierdzono

I. Opracowanie, wprowadzenie, stosowanie oraz przegląd wymaganej przez rozporządzenie KRI dokumentacji oraz systemu z zakresu bezpieczeństwa informacji (§ 20 ust. 1 rozporządzenia KRI).

W Archiwum Państwowym w Bydgoszczy (dalej AP w Bydgoszczy) opracowano, ustanowiono i wprowadzono system zarządzania bezpieczeństwem informacji (dalej SZBI) zarządzeniem *Nr 4 Dyrektora Archiwum Państwowego w Bydgoszczy z dnia 5 kwietnia 2019 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Archiwum Państwowym w Bydgoszczy* (dalej Zarządzenie SZBI). System ten regulował kluczowe dla zarządzania bezpieczeństwem obszary w celu zapewnienia poufności, dostępności i integralności informacji *(dowód: akta kontroli str. od 7 do 10)*.

Z przekazanej przez Dyrektora AP w Bydgoszczy przy pismach znak: AG.0900.1.2024 z dnia 30.01.2024 r. (dalej wyjaśnienia z dnia 30.01.2024 r.) i 22.03.2024 r. (dalej wyjaśnienia z dnia 22.03.2024 r.) dokumentacji wynika, iż w I połowie 2023 r. dokonano przeglądu dokumentacji SZBI z zaznaczeniem, iż kolejna aktualizacji będzie konieczna po przeniesieniu jednostki do nowego budynku. W wyjaśnieniach z dnia 22.03.2024 r. Dyrektor AP Bydgoszcz wskazał, iż *„W 2023 r. z uwagi na spiętrzenie zadań i zwolnieniem z pracy (...), jak również przejście do pracy w NDAP z dniem 31 lipca 2022 (...), który pełnił rolę audytora wewnętrznego w AP w Bydgoszczy nie zostały zrealizowane pkt 5, 6, 7 i 8 § 6 Zarządzenia Nr 4. (...) Działania korygujące i zmieniające zostały przełożone na czas po zakończeniu całkowitego przeniesienia się do nowej lokalizacji" (dowód: akta kontroli str. od 147 do 154).*

Zgodnie z § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

System SZBI powinien być monitorowany i poddawany przeglądom w wyniku czego powinien być doskonalony, co powinno znaleźć odzwierciedlenie w dokumentacji systemu. Działania w ramach SZBI powinny być podejmowane w sposób ciągły i tym samym powinien być on stale doskonalony. W związku z tym, konieczne jest jego monitorowanie i poddawanie cyklicznym przeglądom, w celu zdiagnozowania obszarów wymagających usprawnienia, co z kolei powinno znaleźć odzwierciedlenie w dokumentacji systemu.

W AP w Bydgoszczy w okresie poddanym kontroli nie zrealizowano zadań wskazanych w pkt 5-8 § 6 Zarządzenia SZBI, tj.:

- przygotowania planu i monitorowania realizacji audytów wewnętrznych,
- przygotowywania i nadzoru nad realizacją szkoleń i programów uświadamiających dotyczących bezpieczeństwa informacji,
- przygotowania przeglądów zarządzania,

– monitorowania realizacji działań korygujących oraz planu postępowania z ryzykiem.

Na podstawie złożonych przez Dyrektora AP w Bydgoszczy w toku kontroli wyjaśnień oraz przekazanej dokumentacji należy stwierdzić, iż w okresie badanym jednostka kontrolowana dokonała przeglądu dokumentacji SZBI natomiast nie dokonała monitoringu, przeglądu, utrzymania i doskonalenia systemu SZBI, co **uznano za nieprawidłowość**.

Biorąc powyższe pod uwagę opracowanie, wprowadzenie, stosowanie oraz przegląd wymaganej przez rozporządzenie KRI dokumentacji z zakresu bezpieczeństwa informacji **oceniono pozytywnie pomimo stwierdzonych nieprawidłowości.**

II. Opracowanie wewnętrznych regulacji opisujących sposób zarządzania ryzykiem bezpieczeństwa informacji, przeprowadzenie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz opracowanie planu postępowania z ryzykiem (§ 20 ust. 2 pkt 3 rozporządzenia KRI).

W AP w Bydgoszczy została opracowana *Instrukcja zarządzania ryzykiem* oraz *Metodyka szacowania ryzyka* stanowiące załączniki do Polityki Bezpieczeństwa Informacji *(dowód: akta kontroli str. od 49 do 57)*. W roku 2023 została przeprowadzona analiza ryzyka utraty integralności, dostępności lub poufności informacji. Nie była ona jednak kompleksowa, ponieważ nie obejmowała wszystkich aktywów będących w posiadaniu kontrolowanej jednostki, **co uznano za uchybienie**. Nie wdrożono podziału aktywów na istotne i krytyczne. Regulacje nie określały także podziału pomiędzy środkami przetwarzania informacji w zakresie komórek organizacyjnych, a aktywami odnoszącymi się do środków przetwarzania informacji wykorzystywanych do zapewnienia usług teleinformatycznych *(dowód: akta kontroli str. od 74 do 84)*.

Zgodnie z § 5 Instrukcji zarządzania ryzykiem ryzyko o istotności do 9 punktów było ryzykiem akceptowalnym, co oznacza brak obowiązku podejmowania przez jednostkę kontrolowaną działań ograniczających jego istotność. W odniesieniu do ryzyka o istotności od 10 do 25 punktów zaplanowane do wdrożenia działania zaradcze, ograniczające ich istotność do poziomu akceptowalnego, zostały zawarte w analizie ryzyka. Informacje o zmaterializowaniu się ryzyka zamieszczono również w powyższym dokumencie.

AP w Bydgoszczy opracowało *Plan ciągłości działania*, a jako jego cel wskazano minimalizację zakłóceń w realizacji działalności statutowej w związku z dysfunkcją systemu informatycznego *(dowód: akta kontroli str. od 19 do 24)*. Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2024 r. wskazał, iż *„w kontrolowanym okresie nie przeprowadzono testów ciągłości działania" (dowód: akta kontroli str. od 147 do 154)*, **co uznano za uchybienie**.

Biorąc powyższe pod uwagę powyższą kategorię **oceniono pozytywnie pomimo stwierdzonych uchybień.**

III. Opracowanie i wprowadzenie dokumentacji zarządzania sprzętem i oprogramowaniem oraz aktualizacja rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB - § 20 ust. 2 pkt 2 rozporządzenia KRI).

Zespół kontrolny pismem znak: DOA.084.2.2024 z dnia 11 marca 2024 r. zwrócił się do kierownika kontrolowanej jednostki z zapytaniem: *Czy opracowano i wdrożono dokumentację zarządzania sprzętem i oprogramowaniem, w tym: rejestr zasobów informatycznych, procedury prowadzenia rejestru zasobów informatycznych, procedury przydzielania, zwrotu sprzętu i oprogramowania, procedury korzystania z zasobów informatycznych przez użytkowników oraz jaki jest sposób aktualizacji rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB)?*

W odpowiedzi na powyższe Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2024 r. wskazał, że *„Wdrożony jest zakres opisany w procedurach Procedury i Zasady bezpieczeństwa informacji, które są załącznikiem do dokumentu polityki bezpieczeństwa"*. Jednocześnie poinformował, iż *„Rejestr zasobów IT obejmuje rejestr sprzętu IT, licencji oraz stosowanego oprogramowania – realizowany m.in. w oparciu o oprogramowanie NVision oraz spisy prowadzone w arkuszu kalkulacyjnym" (dowód: akta kontroli str. od 147 do 154).*

Po dokonaniu analizy przekazanej dokumentacji stanowiącej załączniki do Polityki bezpieczeństwa informacji zatwierdzonej przez Dyrektora AP w Bydgoszczy dnia 4.04.2019 r. zespół kontrolny stwierdził, iż jedyne regulacje dotyczące zarządzania sprzętem teleinformatycznym są zawarte w *Procedurach i zasadach bezpieczeństwa informacji* w rozdziale *Nadzór nad urządzeniami teleinformatycznymi* oraz *Przeglądy i konserwacje systemu informatycznego i aplikacji (dowód: akta kontroli str. od 25 do 48)*. Pierwszy z nich zawiera cztery n/w punkty:

1. Każde urządzenie jest oznaczone i posiada unikalny numer inwentaryzacyjny.
2. Zabroniona jest zmiana lokalizacji urządzeń teleinformatycznych i drukujących bez zgody działu IT.
3. Zabronione jest przekazywanie urządzeń teleinformatycznych i drukujących innym osobom bez zgody działu IT.
4. Zasady zabezpieczenia elektronicznych nośników informacji.

Natomiast AP w Bydgoszczy nie posiadało regulacji wewnętrznych opisujących sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB), procedury prowadzenia rejestru zasobów informatycznych, procedury przydzielania, zwrotu sprzętu i oprogramowania, procedury korzystania z zasobów informatycznych przez użytkowników, **co uznano za nieprawidłowość.**

Biorąc powyższe pod uwagę opracowanie i wprowadzenie dokumentacji zarządzania sprzętem i oprogramowaniem oraz aktualizacji rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB) **oceniono pozytywnie pomimo stwierdzonych nieprawidłowości**.

IV. Opracowanie i wprowadzenie regulacji wewnętrznych opisujących zarządzanie uprawnieniami użytkowników do pracy w systemach teleinformatycznych oraz bezzwłocznego odbierania uprawnień byłym pracownikom w systemach teleinformatycznych (§ 20 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI).

AP w Bydgoszczy posiadało regulacje dotyczące *Nadawanie uprawnień do przetwarzania danych osobowych i rejestrowania tych danych w systemie informatycznym*, *Procedurę odbierania uprawnień do przetwarzania danych osobowych* oraz *Procedurę rozpoczęcia, zawieszenia i zakończenia pracy w systemie teleinformatycznym (dowód: akta kontroli str. od 25 do 48)*.

Zespół kontrolny pismem znak: DOA.084.2.2024 z dnia 11.03.2024 r. zwrócił się do Dyrektora AP w Bydgoszczy z zapytaniem: *Czy w kierowanej przez niego jednostce była prowadzona i udokumentowana okresowa weryfikacji nadanych uprawnień użytkowników do pracy w systemach teleinformatycznych*? W odpowiedzi Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2024 r. stwierdził, iż *„Weryfikacja jest prowadzona na bieżąco. Upoważnienia do przetwarzania danych osobowych są przechowywane w teczkach osobowych pracowników" (dowód: akta kontroli str. 147 do 154).* Zespół kontrolny nie otrzymał odpowiedzi na pytanie czy w AP w Bydgoszczy prowadzony jest rejestr wydanych upoważnień.

Dyrektor AP w Bydgoszczy w odpowiedzi na pytanie zespołu kontrolnego: *Czy w okresie kontrolowanym prowadzone były działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrycia nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie*? wskazał w w/c piśmie, że *„Takie działania były prowadzone w I połowie 2023 do końca czerwca. Z uwagi na trwające prace przeprowadzkowe odbyły się one tylko pod koniec I i II kwartału 2023 roku. Nie stwierdzono w tym zakresie żadnych incydentów"*. Odnosząc się do powyższego należy podkreślić, iż kontrola obejmowała okres od 1.01.2023 r. do 29.02.2024 r. natomiast z uzyskanych wyjaśnień wynika, iż w okresie od lipca 2023 r. do końca lutego 2024 r. w AP w Bydgoszczy nie weryfikowało działań dokonywanych w zasobach teleinformatycznych w postaci wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesu czy nadzorowania samego siebie, **co uznano za nieprawidłowość.**

Dyrektor AP w Bydgoszczy, pomimo zapytania zespołu kontrolnego w piśmie znak: DOA.084.2.2024 z dnia 11.03.2024 r., nie przekazał w toku kontroli zestawienia zawierającego daty rozwiązania umowy o pracę lub wygaśnięcia umowy/zlecenia użytkowników systemów teleinformatycznych oraz odebrania tym użytkownikom uprawnień do korzystania z systemów. W wyjaśnieniach z dnia 22.03.2024 r. wskazał *„Ze względu na likwidację systemu Active Directory w siedzibie przy ul. Dworcowej i konieczność postawienia tego systemu w nowej siedzibie, dane nie zachowały się" (dowód: akta kontroli str. od 147 do 154)*. W związku z czym zespół kontrolny bazując tylko na informacjach przekazanych przez kierownika jednostki kontrolowanej w w/c piśmie, iż *„W okresie kontrolnym zwolnionych*

zostało 9 osób. Uprawnienia były odbierane w przeciągu 3-4 dni od daty zwolnienia. Wyjątkiem było zwolnienie (...) w dniu 27 lipca 2023 r. z zachowaniem trzymiesięcznego okresu wypowiedzenia bez obowiązku świadczenia pracy. Przed wręczeniem wypowiedzenia zmieniono w trybie pilnym wszystkie znane mu hasła administratora do systemów informatycznych AP w Bydgoszczy oraz hasło dostępowe do dostępu zdalnego do sieci Archiwum" nie mógł w sposób wiarygodny dokonać oceny szybkości odbierania uprawnień byłym pracownikom w systemach informatycznych o której mowa w § 20 ust. 2 pkt 5 rozporządzenia KRI.

W wyjaśnieniach z dnia 22.03.2024 r. Dyrektor AP w Bydgoszczy poinformował, iż *„Zmiany uprawnień użytkowników w kontrolowanym okresie nie były dokonywane" (dowód: akta kontroli str. od 147 do 154).*

Biorąc pod uwagę działalność AP w Bydgoszczy w zakresie opracowania i wprowadzenia regulacji wewnętrznych opisujących zarządzanie uprawnieniami użytkowników do pracy w systemach teleinformatycznych oraz bezzwłocznego odbierania uprawnień byłym pracownikom, **oceniono pozytywnie pomimo stwierdzonych nieprawidłowości.**

V. Opracowanie i wprowadzenie regulacji wewnętrznych dotyczących przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych oraz przeprowadzanie szkoleń (§ 20 ust. 2 pkt 6 rozporządzenia KRI).

AP Bydgoszczy posiadało regulacje wewnętrzne pn. *Szkolenia użytkowników* zawarte w dokumencie pt. *Procedury i zasady bezpieczeństwa*. Zgodnie z ich zapisami każdy użytkownik przed dopuszczeniem do pracy w systemie informatycznym przetwarzającym dane osobowe lub w wersji papierowej winien zapoznać się z zakresem ochrony danych osobowych w postaci elektronicznej i papierowej. W wyznaczonych okresach, każdy pracownik musi wziąć udział w szkoleniu z zakresu zasad ochrony danych osobowych *(dowód: akta kontroli str. od 25 do 48).*

Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2024 r. wskazał, iż *„Prowadzone są szkolenia stanowiskowe. Ponadto szkolenie dla 12 osób, w tym nowo przyjętych przeprowadził w dniu 27 października 2023 r. Inspektor Ochrony Danych" (dowód: akta kontroli str. od 147 do 154).*

Czynności związane z zapewnieniem pracownikom wiedzy nt. nowych zagrożeń, adekwatnych zabezpieczeń, skutków ewentualnych incydentów bezpieczeństwa informacji, innych niż dane osobowe, nie były wystarczające. Obowiązujące w AP w Bydgoszczy regulacje pn. *Szkolenia użytkowników* ograniczały zakres obowiązkowych szkoleń tylko do ochrony danych osobowych oraz nie wprowadzały obowiązku cykliczności różnych form szkoleń z zakresu wskazanego w § 20 ust. 2 pkt 6 rozporządzenia KRI, **co uznano za uchybienie.**

Powyższą kategorię zespół kontrolny **ocenił pozytywnie pomimo stwierdzonych uchybień.**

VI. Opracowanie, wprowadzenie oraz stosowanie regulacji wewnętrznych zawierających zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość (§ 20 ust. 2 pkt 8 rozporządzenia KRI).

W AP w Bydgoszczy podejmowano działania zapewaniające bezpieczną pracę na odległość. Opracowano i wdrożono dokument pt. *Procedury i zasady bezpieczeństwa informacji*, w której zawarto regulacje pn. *Warunki pracy zdalnej* wskazujące m.in. wymagane zabezpieczenia podczas pracy zdalnej *(dowód: akta kontroli str. od 25 do 48)*. Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2024 r. poinformował, iż w okresie kontrolowanym nie wykonywano pracy zdalnej. W związku z czym zespół kontrolnym nie mógł dokonać oceny prawidłowości wykorzystywanych rozwiązań uwierzytelniających.

Biorąc powyższe pod uwagę działalność jednostki kontrolowanej w powyższym obszarze **należy ocenić pozytywnie.**

VII. Opracowanie, wprowadzenie oraz stosowanie regulacji wewnętrznych w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji (§ 20 ust. 2 pkt 13 rozporządzenia KRI).

AP w Bydgoszczy posiadało regulacje wewnętrzne pn. *Incydenty bezpieczeństwa – zgłaszanie naruszeń*, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji *(dowód: akta kontroli str. od 25 do 48)*. Zgodnie z przekazanym Rejestrem Incydentów w roku 2023 wykryto dwa takie przypadki *(dowód: akta kontroli str. od 85 do 86)*. Jeden z wykrytych incydentów klasyfikował się do katalogu zdarzeń wymagających zgłoszenia do właściwego CSiRT. Jednostka kontrolowana w sposób prawidłowy i terminowy zrealizowała obowiązek wynikający z art. 22 ust. 1 pkt 2 ustawy o Krajowym systemie cyberbezpieczeństwa.

Za uchybienie uznano brak przeprowadzenia analizy przyczyn wystąpienia wykrytych incydentów naruszenia bezpieczeństwa informacji w celu doskonalenia stosowanych zabezpieczeń oraz wskazanie działań korygujących zmierzających do eliminacji ich wystąpienia w przyszłości.

Biorąc powyższe pod uwagę działalność jednostki kontrolowanej w powyższym obszarze **oceniono pozytywnie pomimo stwierdzonych uchybień**.

VIII. Opracowanie, wprowadzenie regulacji wewnętrznych, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie bezpieczeństwa informacji oraz przeprowadzania cyklicznych audytów wewnętrznych (§ 20 ust. 2 pkt 14 rozporządzenia KRI).

AP w Bydgoszczy posiadało wewnętrzne regulacje pn. *Procedura audytu wewnętrznego*, w której określono cele audytowe, sposób ich realizacji oraz obowiązkowe elementy *(dowód: akta kontroli str. od 25 do 48).*

W wyjaśnieniach z dnia 30.01.2024 r. Dyrektor AP w Bydgoszczy wskazał, iż *„W okresie od 01.01.2023 r. do dnia 30.01.2024 r. nie został przeprowadzony audyt wewnętrzny z zakresu bezpieczeństwa informacji. Pracownik odpowiedzialny za to zagadnienie (...), został przeniesiony do Naczelnej Dyrekcji Archiwów Państwowych i na jego miejsce nie został powołany inny pracownik. Powodem braku wyznaczenia nowego pracownika było niedopatrzenie spowodowane duża ilością prac związanych z odbiorami nowo wybudowanego budynku, przygotowywaniem postępowań przetargowych na przeprowadzkę zasobu i mienia oraz zakup i dostawę wyposażenia nowego obiektu Archiwum" (dowód: akta kontroli str. od 4 do 6).*

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w m.in. przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W związku z czym, nieprzeprowadzenie w AP w Bydgoszczy wymaganego przepisami prawa corocznego audytu wewnętrznego **uznano na nieprawidłowość**.

Biorąc pod uwagę powyższe działania kontrolowanej jednostki oceniono **pozytywnie pomimo stwierdzonych nieprawidłowości.**

IX. Opracowanie, wprowadzenie oraz stosowanie regulacji wewnętrznych w których określono zasady tworzenia, przechowywania kopii zapasowych danych i systemów podmiotu publicznego (§ 20 ust. 2 pkt 12 lit. b rozporządzenia KRI).

Kontrolowana jednostka posiadała regulacje dotyczące tworzenia kopii zapasowych pt. Procedura tworzenia kopii zapasowych. Kopie zapasowe były przechowywane w innej lokalizacji niż miejsce ich wytwarzania.

Dyrektor AP w Bydgoszczy w piśmie znak: AG.0900.1.2024 z dnia 5.04.2024 r. (dalej wyjaśnienia z dnia 5.04.2024 r.) poinformował, że *„Kopie bezpieczeństwa są tworzone i testowane. (...) Nasza polityka bezpieczeństwa w obecnej postaci nie przewiduje sporządzenia raportów z przeprowadzania testów odtworzenia backupów zabezpieczanych systemów" (dowód: akt kontroli str. od 218 do 221).*

Zgodnie z regulacjami zawartymi w rozdziale *Przeglądy i raporty* Administrator Systemów Informatycznych raz na rok sporządza raport dla Administratora Danych osobowych, który zawiera: wyniki przeglądu systemu do wykrywania i usuwania oprogramowania złośliwego na wszystkich stanowiskach komputerowych, wyniki przeglądu

i testów UPS'ów, wyniki przeglądu kopii zapasowych *(dowód: akta kontroli str. od 25 do 48)*. Zespół kontrolny w piśmie znak: DOA.084.1.2024 z dnia 11.03.2024 r. zwrócił się do Dyrektora AP w Bydgoszczy o przekazanie takiego raportu. W odpowiedzi w wyjaśnieniach z dnia 22.03.2024 r. kierownik jednostki kontrolowanej wskazał, iż *„Zgodnie z polityką bezpieczeństwa ASI nie ma w obowiązkach przekazywania raportów"*. Uzupełniając powyższą informację w wyjaśnieniach z dnia 5.04.2024 r. Dyrektor AP w Bydgoszczy stwierdził, iż *„W związku z zaistniałą sytuacją tj. koniecznością zwolnienia dwóch osób z działu IT co było równoznaczne z likwidacją komórki IT oraz relokacją serwerowni i systemów IT* do nowej lokalizacji powiązanej z rekonfiguracją całej architektury IT *do nowych warunków, nie sporządzono takiego raportu" (dowód: akta kontroli str. od 218 do 221).* Brak niniejszego raportu **uznano za uchybienie**.

Biorąc pod uwagę powyższe działania kontrolowanej jednostki **oceniono pozytywnie pomimo stwierdzonych uchybień.**

X. Opracowanie, wprowadzenie oraz stosowanie regulacji wewnętrznych w których ustalono zasady postępowania z informacjami zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem (§ 20 ust. 2 pkt 11 KRI).

AP w Bydgoszczy posiadało regulacje dotyczące minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji *(dowód: akta kontroli str. od 25 do 48)* tj.:

- Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności,
- Polityka kluczy,
- Przetwarzanie danych osobowych w obszarach bezpiecznych,
- Zasady zabezpieczenia dokumentów i wydruków,
- Zasady ochrony danych osobowych, nieinformatycznych,
- Zasady niszczenia dokumentów,
- Zastępstwa, urlopy i udostępnianie danych,
- Nadzór nad urządzeniami teleinformatycznymi,
- Zabezpieczenie elektronicznych nośników informacji,
- Warunki pracy zdalnej,
- Przeglądy i konserwacje systemu informatycznego i aplikacji.

W analizie ryzyka za rok 2023 nie zidentyfikowano natomiast ryzyka związanych z kradzieżą urządzeń mobilnych, **co uznano na uchybienie**.

Za uchybienie uznano również brak procedury opisującej działania związane z utylizacją sprzętu informatycznego i nośników danych.

Biorąc pod uwagę powyższe działania kontrolowanej jednostki **oceniono pozytywnie pomimo stwierdzonych uchybień.**

XI. Opracowanie, wprowadzenie oraz stosowanie regulacji wewnętrznych w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowanych zabezpieczeń (§ 20 ust. 2 pkt 12 oraz ust. 4 KRI).

Pozytywnie należy ocenić zabezpieczenia serwerowni, które spełniały wysokie standardy oraz fakt, przechowywania kopii zapasowych w innym pomieszczeniu niż są wytwarzane. AP w Bydgoszczy zapewniło właściwe parametry środowiskowe w serwerowni oraz dokonywało cyklicznych pomiarów ich wartości.

Za nieprawidłowość uznano niezapewnienie w okresie kontrolowanym przez AP w Bydgoszczy odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych.

Za nieprawidłowość uznano również brak określenia w umowach zawartych w okresie kontrolowanym z firmą [redacted] dot. utrzymania infrastruktury IT kar umownych za niewłaściwe lub nienależyte wykonanie przedmiotu umowy przez Wykonawcę.

W związku z podjętymi przez AP w Bydgoszczy działaniami kategorię **oceniono pozytywnie pomimo stwierdzonych nieprawidłowości.**

XII. Opracowanie, wprowadzenie oraz stosowanie regulacji wewnętrznych zawierających zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych zgodnie z § 21 rozporządzenia KRI.

Zespół kontrolny w piśmie znak: DOA.084.2.2024 z dnia 11.03.2024 r. zwrócił się z zapytaniem do Dyrektora AP w Bydgoszczy: *Czy w kierowanej przez niego jednostce wprowadzono regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów)*? Ponadto, w niniejszym piśmie poproszono o opisanie w jaki sposób w AP w Bydgoszczy dokonuje się przeglądania logów oraz o przekazanie przykładowego dokumentu potwierdzającego ten proces z co najmniej trzech dni z okresu od 1.12.2023 r. do 29.02.2024 r.

W odpowiedzi, w wyjaśnieniach z dnia 22.03.2023 r., Dyrektor AP w Bydgoszczy poinformował, iż w kontrolowanej jednostce nie wprowadzono regulacji wewnętrznych zawierających zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych, zgodnie z § 21 rozporządzenia KRI. Jednocześnie podkreślił, iż *„logi przeglądane są regularnie – jednakże w obecnej polityce bezpieczeństwa nie jest uwzględniona taka procedura" (dowód: akta kontroli str. od 147 do 154).* Zespół kontrolny nie uzyskał odpowiedzi na pytanie w jaki sposób w AP w Bydgoszczy dokonywane są przeglądy logów oraz nie otrzymał przykładowego dokumentu potwierdzającego ten proces.

Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2023 r. wskazał również, iż *„w obecnej polityce bezpieczeństwa nie została uwzględniona procedura prowadzenia*

i dostępu do dzienników systemowych oraz okresu i sposobu ich przechowywania" (dowód: akta kontroli str. od 147 do 154).

Zgodnie z § 21 ust. 1 rozporządzenia KRI rozliczalność *w* systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów *w* dziennikach systemów (logach). Z kolei ust. 2 stanowi, iż informacje *w* dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany *w* przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

Należy stwierdzić, iż AP w Bydgoszczy nie opracowało regulacji zawierających zasady prowadzenia i wykorzystania dzienników systemowych (logów), w tym określających zakres danych podlegających dokumentowaniu w dziennikach, co stanowi naruszenie § 21 rozporządzenia KRI i **uznano za nieprawidłowość.**

Biorąc powyższe pod uwagę ten obszar działalności jednostki kontrolowanej **oceniono pozytywnie pomimo stwierdzonych nieprawidłowości**.

XIII. Przeprowadzenia testu konfiguracji usługi Microsoft Active Directory oraz zapory sieciowej – Firewall.

Dyrektor AP w Bydgoszczy w wyjaśnieniach z dnia 22.03.2024 r. poinformował, iż *„AP Bydgoszcz nie może przesłać testów dot. Microsoft AD, gdyż usługa ta w styczniu 2024 r. została dezaktywowana z uwagi na rozpoczęcie procesu przenoszenia infrastruktury do nowej lokalizacji. Aktualnie trwa proces uruchamiania tej usługi w nowej lokalizacji archiwum – ul. Karłowicza" (dowód: akta kontroli str. od 147 do 154).* W związku z czym zespół kontrolny nie dokonał oceny konfiguracji usługi Microsoft Active Directory.

Za nieprawidłowość uznano natomiast niepoprawne skonfigurowanie przez AP w Bydgoszczy w okresie kontrolowanym zapory sieciowej – Firewall. Należy jednak podkreślić, iż w trakcie kontroli Dyrektor AP w Bydgoszczy podjął działania w celu wyeliminowania zgłaszanych w jej toku przez zespół kontrolny słabości w funkcjonowaniu zapory sieciowej – Firewall o czym poinformował w piśmie znak: AG.0900.1.2024 z dnia 25.04.2024 r. tj. *„4 kwietnia poleciłem firmie [redacted] dokonanie takich zmian konfiguracji na Firewall `u, aby były one zgodne z wymogami Naczelnej Dyrekcji Archiwów Państwowych" (dowód: akta kontroli str. 225).*

Biorąc pod uwagę działania AP w Bydgoszczy niniejszą kategorię **oceniono pozytywnie pomimo stwierdzonych nieprawidłowości.**

XIV. Realizacja obowiązków wynikających z Rozdziału 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Zgodnie z art. 21 ustawy KSC podmiot publiczny, o którym mowa w art. 4 pkt 7–15, czyli m.in. jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[1], realizujący zadanie publiczne

[1] tj. Dz. U. z 2023 r. poz. 1270 z późn. zm.

zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Natomiast zgodnie z art. 22 ust. 1 pkt 5 dane kontaktowe wyznaczonej osoby powinny zostać przekazane do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (dalej: CSIRT). Zadania i właściwość poszczególnych CSIRTów określa szczegółowo Rozdział 26 KSC. Zgodnie z art. 26 ust. 6 pkt 1 lit a i b tej ustawy koordynacja obsługi incydentów zgłaszanych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, czyli m.in. jednostki budżetowe, a także jednostki podległe organom administracji rządowej lub przez nie nadzorowane należy do zadań do CSIRT NASK.

Z wyjaśnień Dyrektora AP w Bydgoszczy oraz przesłanych dokumentów wynika, że w kontrolowanej jednostce wprawdzie wyznaczono osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, jednak zgłoszenia osoby wyznaczonej dokonano do CSIRT GOV a nie do właściwego dla archiwów państwowych, tj. CSIRT NASK. W wyjaśnieniach z dnia 22.03.2024 r. Dyrektor AP w Bydgoszczy stwierdził, iż wysłanie zgłoszenia do niewłaściwego CSIRT-u to *„pomyłka osoby wysyłającej”,* **co uznano za uchybienie.**

Kontrolowana jednostka w sposób prawidłowy i terminowy zgłosiła wykryty incydent naruszenia bezpieczeństwa informacji do właściwego CSIRT.

W związku z powyższym realizację przez AP w Bydgoszczy obowiązków wynikających z Rozdziału 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa **oceniono pozytywnie pomimo stwierdzonych uchybień**.

Podsumowanie

Biorąc pod uwagę oceny cząstkowe, **negatywnie oceniono** działalność Archiwum Państwowego w Bydgoszczy w zakresie wybranych aspektów dotyczących bezpieczeństwa teleinformatycznego.

Kierownik jednostki kontrolowanej w piśmie znak: AG.0900.1.2024 z dnia 21.05.2024r. poinformował, że nie wnosi zastrzeżeń do projektu wystąpienia pokontrolnego.

Wnioski i zalecenia pokontrolne

Biorąc pod uwagę powyższe ustalenia i oceny, na podstawie art. 46 ust. 3 pkt 1 i 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz. U. z 2020 r. poz. 224), proszę o realizację następującego zaleceń i wniosków pokontrolnych:

1. Wykonanie zadań wskazanych w pkt 5-8 § 6 zarządzenia Nr 4 Dyrektora Archiwum Państwowego w Bydgoszczy z dnia 5 kwietnia 2019 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Archiwum Państwowym w Bydgoszczy, tj.:

– przygotowanie planu i monitorowanie realizacji audytów wewnętrznych,

- przygotowywanie i nadzór nad realizacją szkoleń i programów uświadamiających dotyczących bezpieczeństwa informacji,
- przygotowanie przeglądów zarządzania,
- monitorowanie realizacji działań korygujących oraz planu postępowania z ryzykiem.

2. Przeprowadzenie analizy ryzyka zgodnie z normą wskazaną w § 20 ust. 3 pkt 2) rozporządzenia KRI, tj. PN-ISO/IEC 27005.
3. Przeprowadzenie testów ciągłości działania zgodnie z obowiązującym w AP Bydgoszcz *Planem ciągłości działania.*
4. Opracowanie i wprowadzenie regulacji wewnętrznych opisujących sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB), procedury prowadzenia rejestru zasobów informatycznych, procedury przydzielania, zwrotu sprzętu i oprogramowania, procedury korzystania z zasobów informatycznych przez użytkowników.
5. Przeprowadzenie i udokumentowanie monitoringu dostępu do zasobów teleinformatycznych, w tym przeglądu w celu wykrycia nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie.
6. Wprowadzenie zmian w regulacji pn. Szkolenia użytkowników poprzez dostosowanie jej zapisów do § 20 ust. 2 pkt 6 rozporządzenia KRI.
7. Przeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
8. Sporządzenie przez Administratora Systemów Informatycznych raportu wskazanego w regulacji pt. *Przeglądy i raporty*.
9. Zamieszczanie w umowach dot. utrzymania infrastruktury IT kar umownych za niewłaściwe lub nienależyte wykonanie przedmiotu umowy przez Wykonawcę.
10. Opracowanie i wprowadzenie do stosowania regulacji zawierających zasady prowadzenia i wykorzystania dzienników systemowych (logów), w tym określających zakres danych podlegających dokumentowaniu w dziennikach zgodnie z § 21 rozporządzenia KRI.
11. Poprawne skonfigurowanie zapory sieciowej – Firewall oraz wyeliminowanie jej słabości wskazanych przez zespół kontrolny w toku kontroli.
12. Uruchomienie i poprawne skonfigurowanie usługi Microsoft Active Directory.
13. Ponowne przeprowadzenie testu konfiguracji usługi Microsoft Active Directory i zapory sieciowej – Firewall oraz przesłanie raportu z jego przeprowadzenia.

Na podstawie art. 49 ww. ustawy proszę o poinformowanie mnie o sposobie realizacji zaleceń i wniosków pokontrolnych w terminie do dnia **2.09.2024 r.**

Pouczenie

Zgodnie z art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

dr Paweł Pietrzyk

Potwierdzenie zgodności kopii z dokumentem elektronicznym:

Znak pisma dokumentu:	DOA.084.2.2024
Identyfikator dokumentu:	1145686
Nazwa dokumentu:	WYSTĄPIENIE POKONTROLNE AP BYDGOSZCZ PN. WYBRANE ASPEKTY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO.DOCX
Suma kontrolna SHA256 dokumentu:	759418697e1db9e95e8f7a6da9bc54531a0152779dc3fa3db3b40bf05cf53a05

Wydrukował(a): [redacted]

Data wydruku: 2024-05-29 06:42:04

.....

Podpisy dokumentu:

Paweł Pietrzyk

Data podpisu: 2024-05-28 20:58:43

Rodzaj podpisu: Kwalifikowany podpis elektroniczny

Numer certyfikatu: 491137481763416838

Wystawca certyfikatu: Enigma Systemy Ochrony Informacji Sp. z o.o.