NACZELNY DYREKTOR
ARCHIWÓW PAŃSTWOWYCH
Paweł Pietrzyk

Warszawa, dnia 5 czerwca 2024 r.

WYSTĄPIENIE POKONTROLNE

Znak kontroli	DOA.084.3.2024
Nazwa i adres jednostki kontrolowanej	Archiwum Państwowe w Poznaniu ul. 23 Lutego 41/43 61-744 Poznań
Temat kontroli	Wybrane aspekty dotyczące bezpieczeństwa teleinformatycznego w Archiwum Państwowym w Poznaniu
Tryb kontroli	Zwykły
Podstawa prawna kontroli	1. Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz. U. z 2020 r. poz. 224). 2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023r., 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	1.01.2023 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 Poznaniu 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, upoważnienie nr 7/2024 z dnia 8.03.2024 r., kierownik zespołu kontrolerów. 2. [redacted], główny specjalista w Departamencie Informatyzacji Archiwów Naczelnej Dyrekcji Archiwów Państwowych, upoważnienie nr 8/2024 z dnia 8.03.2024 r., członek zespołu kontrolnego. 3. [redacted], główny specjalista w Departamencie Informatyzacji Archiwów Naczelnej Dyrekcji Archiwów Państwowych, upoważnienie nr 9/2024 z dnia 8.03.2024 r., członek zespołu kontrolnego.
Kierownictwo jednostki kontrolowanej	Pan Henryk Krystek, pełniący funkcję Dyrektora Archiwum Państwowego w Poznaniu od 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 (t.j. Dz. U. z 2023 r. poz. 57 z późn. zm.). 2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.). 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 (t.j. Dz.U. z 2017 r. poz. 2247) – dalej rozporządzenie KRI.
Ogólna ocena kontroli	**Ocena pozytywna pomimo stwierdzonych nieprawidłowości**

W toku kontroli stwierdzono:

I. Opracowanie, wprowadzenie, stosowanie oraz przegląd wymaganej przez rozporządzenie KRI dokumentacji z zakresu bezpieczeństwa informacji (§ 20 ust. 1, ust. 2 rozporządzenia KRI).

Archiwum Państwowe w Poznaniu (dalej AP w Poznaniu) nie posiadało kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI). W szczególności dotyczy to braku opracowania całościowej dokumentacji, która jest warunkiem skutecznego zarządzania bezpieczeństwem informacji. Dyrektor AP w Poznaniu w piśmie znak: DNS.0900.1.2024 z dnia 30.01.2024 r. (dalej wyjaśnienia z dnia 30.01.2024 r.) wskazał, że *„Archiwum Państwowe w Poznaniu wprowadziło Politykę ochrony danych oraz Politykę bezpieczeństwa sytemu informatycznego wraz z zestawem procedur i wzorcami dokumentów. Wprowadzanie Systemu zarządzania bezpieczeństwem informacji zostało zainicjowane po powołaniu nowego inspektora ochrony danych i obecnie jest w procesie wdrażania"* (*dowód: akta kontroli Tom I str. 4*). **Powyższe uznano za nieprawidłowość**. Należy podkreślić, że dopiero wdrożenie całościowych regulacji będzie stanowiło spełnienie wymogów § 20 ust. 1 rozporządzenia KRI.

Za nieprawidłowość uznano również nieprzeprowadzenie, pomimo posiadanej procedury, przeglądu SZBI minimum 1 raz na rok w okresie poprzedzającym zatwierdzenie budżetu jednostki. Dyrektor AP w Poznaniu w piśmie znak: DNS.0900.1.2024 z dnia 22.03.2024r. (dalej wyjaśnienia z dnia 22.03.2024 r.) poinformował, iż *„W okresie kontrolowanym nie dokonano przeglądu dokumentacji SZBI, ze względu na niepowołanie Pełnomocnika ds. Bezpieczeństwa Informacji, który inicjuje i koordynuje przegląd. Ponadto APP jest w trakcie procedowania i wdrażania procedur wynikających z SZBI, dlatego nie dokonano przeglądu SZBI"* (*dowód: akta kontroli Tom II str. 3*).

Ponadto, w okresie kontrolowanym w AP w Poznaniu, z uwagi na nieobsadzenie stanowiska Pełnomocnika Bezpieczeństwa Informacji, nie zgłaszano propozycji działań korygujących SZBI. Nie składano również wniosków o dokonanie zmian w dokumentacji SZBI oraz w infrastrukturze IT, **co uznano za uchybienie**. Podjęto wyłączenie działania w celu uregulowania procesu nadawania uprawnień oraz eliminacji nieprawidłowości wynikających z wniosków z audytu KRI.

W badanym okresie w AP w Poznaniu, pomimo posiadania wdrożonych procedur, nie testowano Procedury zapewnienia ciągłości działania i odtworzenia systemu oraz nie przeprowadzono ćwiczeń działań zgodnych z zapisami dokumentu, **co uznano za uchybienie**.

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

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 okresie kontrolowanym AP w Poznaniu wprowadziło nowe procedury regulujące proces zarządzania ryzykiem, tj. Instrukcję zarządzania ryzykiem, zatwierdzoną 20.10.2023 r. oraz Metodykę szacowania ryzyka, zatwierdzoną 24.10.2023 r. *(dowód: akta kontroli Tom II str. od 283 do 292)*.

Ostatnia analiza ryzyka została przeprowadzona w dniu 30.06.2023 r. według rozwiązań zawartych w załączniku nr 5 Polityki Ochrony Danych Osobowych. Dla zagrożeń o istotności przekraczającej poziom akceptowalny opracowano Plan postępowania z ryzykiem. Przeprowadzona analiza ryzyka nie odnosiła się do wszystkich aktywów jednostki, **co uznano za uchybienie**. W okresie kontrolowanym AP w Poznaniu posiadało Koordynatora ds. ryzyka, który sporządził raport o stanie procesu zarządzania ryzykiem za rok 2023 *(dowód: akta kontroli Tom II str. od 41 do 42)*.

Jednostka kontrolowana planuje przeprowadzić analizę ryzyka wg obowiązujących odpowiednio od dnia 20.10.2023 r. i 24.10.2023 r. Instrukcji zarządzania ryzykiem i Metodyki szacowania ryzykiem w czerwcu 2024 r. lub w szczególnym wypadku zgłoszenia Dyrektorowi AP w Poznaniu przez komórki organizacyjne istotnego ryzyka.

Biorąc powyższe pod uwagę **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).

AP w Poznaniu posiadało od 3.11.2023 r. regulacje opisujące sposób zarządzania sprzętem informatycznym oraz niszczenia nośników danych, tj. *Procedurę przyjmowania, inwentaryzowania zasobów* oraz *Procedurę niszczenia nośników danych (dowód: akta kontroli Tom I str. od 314 do 317)*. W Raporcie z audytu KRI, przeprowadzonym w dniach 9.11.-8.12.2023 r., stwierdzono, że podmiot nie posiadał zinwentaryzowanego sprzętu/oprogramowania wraz z określeniem ważności danego komponentu dla całej organizacji. Jako zalecenie wskazano stosowanie procedury przyjmowania, inwentaryzowania zasobów *(dowód: akta kontroli Tom I str. od 413 do 423)*.

Dyrektor AP w Poznaniu w wyjaśnieniach z dnia 22.03.2024 r. wskazał, iż *„Ostatnia pełna inwentaryzacja wyposażenia była przeprowadzona w 2022 roku, na podstawie Zarządzenia Dyrektora Archiwum Państwowego w Poznaniu nr 7/2022 z dnia 14 października 2022 roku. Spisowi inwentaryzacyjnemu i porównaniu stanu faktycznego z ewidencją zasobu podlegało nie tylko wyposażenie IT, ale również pozostałe wyposażenie pomieszczeń biurowych (meble, biurka, fotele, urządzenia i in.). Proces inwentaryzacji przeprowadzono jeszcze w lipcu 2023 roku, w związku z pismem Naczelnej Dyrekcji Archiwów Państwowych z 26 czerwca 2023 roku znak DIA.032.1.2023. Obecnie trwa proces wdrażania nowego*

narzędzia inwentaryzującego. Został zakupiony program (...), co pozwoli nam na dokładne zweryfikowanie stanu wyposażenia IT z ewidencją. (...) Rejestr zasobów teleinformatycznych do tej pory wprowadzaliśmy ręcznie do aplikacji Wyposażenie. Obecnie wdrażamy system półautomatycznej inwentaryzacji z systemem (...)" (dowód: akta kontroli: Tom I str. od 2 do 9).

W związku z niedysponowaniem przez AP Poznań kompleksową bazą CMDB, powyższą kategorię **oceniono pozytywnie pomimo stwierdzonych uchybień.**

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 Poznaniu wprowadziło Regulamin przetwarzania informacji, zatwierdzony 6.10.2023 r., który zawiera m.in. Procedurę nadawania i odbierania uprawnień do korzystania z systemów informatycznych *(dowód: akta kontroli Tom I str. od 249 do 256).* Ponadto, w kontrolowanej jednostce obowiązywała również Procedura rozpoczęcia i zakończenia zatrudnienia, zatwierdzona 30.10.2023 r. (*dowód: akta kontroli Tom I str. od 297 do 298*) oraz Procedura nadawania upoważnień do przetwarzania danych osobowych, zatwierdzona 06.12.2023 r. (*dowód: akta kontroli Tom I str. od 271 do 272*).

W przypadku zmian zadań osób zaangażowanych w przetwarzanie danych osobowych lub rozwiązania/wygaśnięcia umowy, kontrolowana jednostka nie dokonywała w sposób niezwłoczny stosownych zmian w dostępie do systemów teleinformatycznych. Z przekazanego przez AP w Poznaniu przy wyjaśnieniach z dnia 22.03.2024 r. zestawienia dot. rozwiązania umów o pracę/wygaśnięcia umowy z użytkownikami systemów teleinformatycznych wynika, iż w badanym okresie rozwiązano umowę z 8 osobami, w tym z dwiema które nie posiadały kont w systemach. W tym samym dniu co rozwiązanie umowy uprawnienia odebrano 1 osobie, następnego dnia roboczego – 1 osobie, po dwóch dniach roboczych – 2 osobom, po miesiącu z adnotacją *„na wniosek kierownika oddziału opracowania, zastępujący dyrektora przedłużył dostęp"* – 1 osobie, po 2 miesiącach – 1 osobie *(dowód: akta kontroli Tom II str. 52),* **co uznano za uchybienie**.

W kontrolowanym okresie AP w Poznaniu prowadziło działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych.

Za uchybienie uznano natomiast brak przeprowadzenia w badanym okresie weryfikacji uprawnień osób zaangażowanych w proces przetwarzania informacji pod kątem ich adekwatności do realizowanych przez nich zadań oraz nie prowadzenie rejestru nadanych uprawnień do pracy w systemach teleinformatycznych.

Biorąc pod uwagę działania AP w Poznaniu niniejszą **kategorię oceniono pozytywnie pomimo stwierdzonych uchybień.**

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).

W AP w Poznaniu obowiązywała procedura *Plan szkoleń*, zatwierdzona 12.09.2023 r. *(dowód: akta kontroli Tom I str. od 211 do 212).* Zgodnie z jej zapisami w ramach rocznego planu szkoleń powinny zostać zrealizowane szkolenia:

- dla wszystkich pracowników: RODO - podstawy; Zasady powierzania i udostępniania danych osobowych; Podstawy analizy ryzyka; Cyberprzestępstwo (ataki komputerowe i socjotechniczne).
- dla specjalistów: Audytor wewnętrzny ISO 27001; Bezpieczeństwo sieci komputerowych (testy penetracyjne); Atakowanie i ochrona aplikacji webowych; Sposoby ochrony fizycznej i zabezpieczenia techniczne.

Wynikający z regulacji wewnętrznych obowiązek organizacji szkoleń w zakresie bezpieczeństwa informacji został spełniony. W okresie kontrolowanym pracownicy AP w Poznaniu wzięli udział w następujących szkoleniach: „Jak się chronić przed cyberatakami?" – 56 pracowników; System zarządzania bezpieczeństwem informacji – 58 pracowników; Cyberbezpieczeństwo: Nie popadajmy w paranoję, ale ... - 56 pracowników; Poznaj bezpieczeństwo Windows. Część pierwsza: usługi systemowe – 1 pracownik; Poznaj bezpieczeństwo Windows. Część druga: lokalne uwierzytelnianie i autoryzacja w systemach Windows – 1 pracownik *(dowód: akta kontroli Tom II str. od 2 do 9)*.

Działania AP w Poznaniu w zakresie zapewnienia pracownikom aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów naruszenia bezpieczeństwa informacji, **oceniono pozytywnie**.

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).

AP w Poznaniu wprowadziło zasady bezpiecznej pracy na odległość, tj. *Procedurę Pracy zdalnej*, zatwierdzoną 25.07.2023 r. *(dowód: akta kontroli Tom I str. od 424-430)* oraz *Procedurę dostępu zdalnego*, zatwierdzoną 15.01.2024 r. *(dowód: akta kontroli Tom I str. od 295 do 296).* Zgodnie z informacjami przekazanymi przez Dyrektora AP w Poznaniu w wyjaśnieniach z dnia 22.03.2024 r. w okresie kontrolowanym pracownicy nie świadczyli pracy zdalnej *(dowód: akta kontroli Tom I str. od 4 do 8)*. W związku z czym zespół kontrolny nie mógł dokonać oceny prawidłowości stosowania rozwiązań uwierzytelniających.

Biorąc pod uwagę działania AP w Poznaniu niniejszą **kategorię oceniono 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 Poznaniu opracowało regulacje dotyczące zarządzania incydentami bezpieczeństwa określające zasady ich zgłaszania oraz postępowania na wypadek ich wystąpienia, tj. *Instrukcja postępowania na wypadek wykrycia incydentu bezpieczeństwa*, zatwierdzona 06.10.2023 r. *(dowód: akta kontroli Tom I str. od 257 do 259).*

Kontrolowana jednostka prowadziła *Rejestr Incydentów (dowód: akta kontroli Tom I str. od 153 do 156)*. W okresie kontrolowanym wykryto jeden incydent naruszenia bezpieczeństwa. Zespół kontrolny ocenił, iż incydent został zgłoszony bezzwłocznie po jego wykryciu. W celu zminimalizowania jego powtórzenia w przyszłości dokonano analizy przyczyn jego wystąpienia oraz podjęto działania korygujące, których termin realizacji wyznaczono do dnia 30.04.2024 r. *(dowód: akta kontroli Tom II str. od 2 do 9).*

W związku z powyższym działania AP w Poznaniu w powyższej kategorii **oceniono pozytywnie.**

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

W AP w Poznaniu wprowadzono regulacje określające konieczność realizacji corocznego audytu bezpieczeństwa informacji, tj. *Procedura audytu wewnętrznego*, zatwierdzona 12.09.2023 r. *(dowód: akta kontroli Tom I str. od 213 do 214).* W dniach 9.11.2023 r. – 8.12.2023 r. przeprowadzono audyt KRI obejmujący wszystkie obszary SZBI zgodnie z minimalnymi wymaganiami dla systemów teleinformatycznych określonych w KRI. Na jego podstawie sporządzono w dniu 18.01.2024 r. raport, w którym zidentyfikowano 9 słabości SZBI oraz rekomendowano wdrożenie zaleceń celem ich eliminacji *(dowód: akta kontroli Tom I str. od 413 do 423).*

W związku z podjętymi przez AP w Poznaniu działaniami kategorię **oceniono pozytywnie.**

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

Działania AP w Poznaniu w zakresie wykonywania i testowania kopii zapasowych były wykonywane prawidłowo i zostały dostosowane do potrzeb jednostki oraz stanowiły wsparcie w zarządzaniu tym obszarem.

W AP w Poznaniu obowiązywała *Procedura tworzenia, testowania kopii bezpieczeństwa*, zatwierdzona 15.01.2024 r. oraz *Szczegółowy opis tworzenia kopii zapasowych i ich testowania*, zatwierdzona 18.01.2024 r. *(dowód: akta kontroli Tom I str. od 299 do 303).* Stosowana była aplikacja do tworzenia kopii zapasowych, która wysyła komunikaty o ewentualnych błędach i niepowodzeniach przy tworzeniu backupu, poza tym wyświetla komunikat na ekranie o powodzeniu operacji.

Kontrolowana jednostka testowała tworzone kopie zapasowe poprzez okresowe uruchamianie procedury ich przywracania. Zgodnie z wyjaśnieniami Dyrektora AP w Poznaniu z dnia 22.03.2024 r. kopie zapasowe na dysku przenośnym przechowywane były w zamkniętej szafie metalowej poza serwerownią. Dostęp do nich posiadały wyłącznie osoby uprawnione przez Dyrektora AP w Poznaniu, a każde wydanie i przyjęcie kopii było rejestrowane. Ponadto, kierownik jednostki kontrolowanej poinformował, iż *„dwoje pracowników zna procedurę przywracania systemu na serwerach domeny i EZD z kopii zapasowych" (dowód: akta kontroli Tom II str. od 2 do 9).*

W związku z podjętymi przez AP w Poznaniu działaniami kategorię **oceniono pozytywnie.**

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).

W Raporcie z Audytu KRI za rok 2023, przeprowadzonym w dniach 9.11.2023 r. - 8.12.2023 r., stwierdzono, że podmiot nie monitoruje faktu podłączenia zewnętrznego sprzętu do infrastruktury służbowej oraz zalecono pilne podjęcie działań naprawczych *(dowód: akta kontroli Tom I str. od 413 do 423).*

W Archiwum Państwowym w Poznaniu obowiązywała *Procedura niszczenia nośników danych,* zatwierdzona 3.11.2023 r. oraz *Procedura monitorowania systemów*, zatwierdzona 16.01.2024 r. *(dowód: akta kontroli Tom I str. od 306 do 309).*

Dyrektor AP w Poznaniu w wyjaśnieniach z dnia 22.03.2024 r. wskazał, iż *„W kontrolowanym okresie nie przeprowadzono niszczenia nośników informacji. Likwidacja zużytego, uszkodzonego i wysłużonego sprzętu IT, który zostanie zebrany i przeznaczony do utylizacji zostanie przeprowadzona w drugim kwartale 2024 roku. W kontrolowanym okresie nie dokonywano napraw nośników informacji".*

W analizie ryzyka za rok 2023 nie zidentyfikowano ryzyk związanych z kradzieżą informacji i środków przetwarzania informacji oraz urządzeń mobilnych, **co uznano na uchybienie**.

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).

W AP w Poznaniu obowiązywał dokument pt. *Przyjęte standardy technologiczne*, zatwierdzony 15.01.2024 r., który określał zasady zapewniające bezpieczeństwo sprzętu teleinformatycznego i sieci strukturalnych oraz *Procedura monitorowania systemów*, zatwierdzona 16.01.2024 r. *(dowód: akta kontroli Tom I str. od 306 do 309).*

Zespół kontrolny pozytywnie ocenił zabezpieczenia serwerowni, które spełniały wysokie standardy oraz fakt, przechowywania kopii zapasowych w innym pomieszczeniu niż są wytwarzane. W kontrolowanym okresie AP w Poznaniu monitorowało parametry środowiskowe w serwerowni oraz dokonywało cyklicznych pomiarów ich wartości.

W okresie kontrolowanym AP w Poznaniu podejmowało działania związane z aktualizacją oprogramowania oraz redukcję ryzyk poprzez wdrożenie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących bezpieczeństwa oraz aktualizację oprogramowania antywirusowego i antyspamowego.

W związku z podjętymi przez AP w Poznaniu działaniami **kategorię oceniono pozytywnie.**

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.

W AP w Poznaniu obowiązywała *Procedura przechowywania logów/dzienników zdarzeń*, zatwierdzona 2.11.2023 r. *(dowód: akta kontroli Tom I str. od 310 do 311).*
W Raporcie z Audytu KRI za rok 2023, stwierdzono, że podmiot nie wykorzystuje narzędzi, które w sposób automatyczny analizują logi pod względem wystąpienia naruszeń oraz zalecono zakup odpowiedniego systemu/oprogramowania analizującego logi pod względem ewentualnych naruszeń *(dowód: akta kontroli Tom I str. od 413 do 423)*.

Jednostka kontrolowana w okresie badanym wprowadziła *Procedurę przeglądu dzienników w tym dziennika logów*, zatwierdzoną 16.01.2024 r. Zgodnie z jej zapisami logi/zdarzenia przechowywane będą na serwerach lokalnych - minimum 2 lata *(dowód: akta kontroli Tom I str. od 312 do 313)*.

W kontrolowanym okresie AP w Poznaniu zapewniło, aby dzienniki systemowe automatycznie odnotowywały obligatoryjne działania użytkowników i obiektów systemowych *(dowód: akta kontroli Tom II str. od 2 do 9)*.

Dyrektor AP w Poznaniu w odpowiedzi na pytanie zespołu kontrolnego: *Czy w okresie kontrolowanym podejmowano działania związane z regularnym przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych?* w wyjaśnieniach z dnia 22.03.2024 r.

wskazał, iż *„Procedura przeglądania i analizowania logów podejmowana jest regularnie przez informatyka w codziennej pracy i nie są sporządzane z tych procesów raporty, ani notatki służbowe. Wyjątkiem są sytuacje anormalne, które zobowiązani jesteśmy zgłaszać do CIRT i Naczelnej Dyrekcji" (dowód: akta kontroli Tom II str. od 2 do 9)*. Brak dokumentowania przeglądania logów i ich analizy w celu identyfikacji działań niepożądanych **uznano za uchybienie.**

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

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

Wyniki przeprowadzonych w toku czynności kontrolnych testów usługi Microsoft Active Directory oraz konfiguracji zapory sieciowej Archiwum Państwowego w Poznaniu zostały omówione przez zespół kontrolerów podczas spotkania z przedstawicielami kontrolowanej jednostki, które odbyło się w dniu 18.04.2024 r. Zgłoszone przez kontrolerów w trybie roboczym uwagi i propozycje usprawnień zostały przyjęte, a kierownik kontrolowanej jednostki oświadczył, że zostaną one zrealizowane w terminie do 26.04.2024 r.

Pismem znak: DNS.0900.1.2024 z dnia 27.04.2024 r. Dyrektor AP w Poznaniu poinformował, że zgłoszone na spotkaniu uwagi dotyczące ustawień usługi Active Directory zostały uwzględnione, a ustawienia zmodyfikowane. Natomiast *„poprawki w konfiguracji urządzenia UTM zostaną dokonane w pierwszej połowie maja przez specjalistę od systemów (...)" (dowód: akta kontroli Tom II str. 167)*.

Biorąc powyższe pod uwagę działania kontrolowanej jednostki w powyższym zakresie **oceniono pozytywnie.**

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

AP w Poznaniu wypełniło obowiązek wynikający z ustawy o krajowym systemie cyberbezpieczeństwa dotyczący wyznaczenia osoby odpowiedzialnej do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Zgłoszenia dokonano w dniu 30.03.2021 r. do właściwego dla Archiwum CSiRT NASK.

Dyrektor AP w Poznaniu, w wyjaśnieniach z dnia 30.01.2024 r., przekazał Rejestr Incydentów w którym w roku 2023 zarejestrowano jeden incydent. Powyższe naruszenie bezpieczeństwa nie mieściło się w katalogu zdarzeń wymagających zgłoszenia do właściwego CSiRT-u.

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

Podsumowanie

Biorąc pod uwagę oceny cząstkowe, **pozytywnie pomimo stwierdzonych nieprawidłowości** oceniono działalność Archiwum Państwowego w Poznaniu w zakresie wybranych aspektów dotyczących bezpieczeństwa teleinformatycznego.

Kierownik jednostki kontrolowanej w piśmie znak: DNS.0900.1.2024 z dnia 24 maja 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 następujących zaleceń i wniosków pokontrolnych:

1. Opracowanie i wprowadzenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z zapisami rozporządzenia KRI oraz przesłanie tego dokumentu do NDAP.
2. Przeprowadzenie testów ciągłości działania oraz ćwiczeń działań zgodnie z zapisami Procedury zapewnienia ciągłości działania i odtworzenia systemu.
3. Przeprowadzenie analizy ryzyka zgodnie z normą wskazaną w § 20 ust. 3 pkt 2) rozporządzenia KRI, tj. PN-ISO/IEC 27005.
4. Przeprowadzenie kompleksowej inwentaryzacji sprzętu/oprogramowania wraz z określeniem ważności danego komponentu dla całej organizacji oraz prowadzenie kompleksowej bazy CMDB.
5. Bezzwłocznie dokonywanie zmian w dostępie do systemów teleinformatycznych w przypadku zmian zadań osób zaangażowanych w przetwarzanie danych osobowych lub rozwiązania/wygaśnięcia umowy.
6. Prowadzenie rejestru nadanych uprawnień do pracy w systemach teleinformatycznych.
7. Stosowanie narzędzi, które w sposób automatyczny będą analizować logi pod względem wystąpienia ewentualnych naruszeń.

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.084.3.2024
Identyfikator dokumentu:	1147390
Nazwa dokumentu:	WYSTĄPIENIE POKONTROLNE AP POZNAŃ PN. WYBRANE ASPEKTY DOT. BEZPIECZEŃSTWA TELEINFORMATYCZNEGO.DOCX
Suma kontrolna SHA256 dokumentu:	29e4e353742fdd0bfa5dec06705eb3bdc1a81f69703ec20e5ea0aec116cac611

Wydrukował(a): [redacted]

Data wydruku: 2024-06-05 15:36:26

.....

Podpisy dokumentu:

Paweł Pietrzyk

Data podpisu: 2024-06-05 15:34:09

Rodzaj podpisu: Kwalifikowany podpis elektroniczny

Numer certyfikatu: 491137481763416838

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