Warszawa, dnia 19.03.2024 r.

NACZELNY DYREKTOR
ARCHIWÓW PAŃSTWOWYCH
Paweł Pietrzyk

WYSTĄPIENIE POKONTROLNE

Znak kontroli	DOA.084.10.2023
Nazwa i adres jednostki kontrolowanej	Archiwum Państwowe w Katowicach ul. Józefowska 104 40-145 Katowice
Temat kontroli	Kontrola wybranych aspektów dotyczących bezpieczeństwa teleinformatycznego w Archiwum Państwowym w Katowicach
Tryb kontroli	Zwykły
Podstawa prawna kontroli	Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz. U. z 2020 r. poz. 224). Plan Kontroli Naczelnego Dyrektora Archiwów Państwowych na rok 2023
Zakres kontroli	Zapewnienie przez Archiwum Państwowe w Katowicach: 1. ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami (§ 20 ust. 2 pkt 7 KRI); 2. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób umożliwiający szybkie podjęcie działań korygujących (§ 20 ust. 2 pkt 13 KRI); 3. okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (§ 20 ust. 2 pkt 14 KRI).
Okres objęty Kontrolą	01.01.2023 -31.12.2023
Próba poddana kontroli	Konfiguracja usługi Microsoft Active Directory oraz zapory sieciowej – Firewall oraz zabezpieczenia fizyczne pomieszczenia serwerowni kontrolowanej jednostki. Dokumentacja dotycząca zgłaszania do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) incydentów w podmiocie publicznym w roku 2023. Dokumenty z realizowanych audytów wewnętrznych w zakresie bezpieczeństwa informacji.
Data rozpoczęcia i zakończenia	18.12.2023 – 06.03.2024

czynności kontrolnych	
Imię, nazwisko i stanowisko służbowe kontrolera	Piotr Łukawski Dyrektor DIA – kierownik zespołu kontrolnego [redacted] gł. spec. DIA [redacted] gł. spec. DIA
Kierownictwo jednostki kontrolowanej	Dyrektor Archiwum Państwowego w Katowicach Pani Sławomira Krupa
Wykaz aktów prawnych regulujących przedmiot 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 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.). 3. 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.). 4. 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).
Ogólna ocena kontroli	Ocena pozytywna pomimo stwierdzonych nieprawidłowości

W toku kontroli weryfikacji poddano następujące zagadnienia:

1. **Konfiguracja usługi Microsoft Active Directory oraz zapory sieciowej – Firewall.**

Wyniki przeprowadzonych w toku czynności kontrolnych testów usługi Microsoft Active Directory oraz zapory sieciowej Archiwum Państwowego w Katowicach zostały omówione przez kontrolerów podczas spotkania z przedstawicielami kontrolowanej jednostki, które odbyło się w dniu 12.02.2024 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 29.02.2024 r. W dniach 15.02. oraz 23.02. br. wpłynęły informacje z kontrolowanej jednostki o wprowadzeniu zmian omówionych w czasie spotkania w dniu 12.02.2024 r., dlatego działania kontrolowanej jednostki w powyższym zakresie oceniono **pozytywnie**.

Dowód: wyniki testów, notatka ze spotkania w dniu 12.02.2024 r. oraz informacje z dnia 15.02.2024 r. oraz 23.02.2024 r. – akta kontroli str. 57-136, str. 153-158, str. 167-170 oraz 173-176.

2. **Zabezpieczenia fizyczne pomieszczenia serwerowni kontrolowanej jednostki.**

W ocenie zespołu kontrolnego zabezpieczenia fizyczne pomieszczeń serwerowni użytkowanych przez Archiwum Państwowe w Katowicach są adekwatne i wystarczające dlatego działania kontrolowanej jednostki dotyczące tego zagadnienia oceniono **pozytywnie**.

Dowód: opis przekazany przez kontrolowaną jednostkę w piśmie sygn. DAG.0910.1.2023 z dnia 12.01.2024 r. – akta kontroli str. 43-48.

3. **Realizacja obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz z rozporządzenia 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, a dotyczących zgłaszania incydentów naruszenia bezpieczeństwa informacji.**

Zgodnie z art. 21 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: 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 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,

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

czyli m.in. jednostki budżetowe, a także jednostki podległe organom administracji rządowej lub przez nie nadzorowane należy do zadań do CSIRT NASK.
Z wyjaśnień Dyrektor Archiwum Państwowego w Katowicach, Pani Sławomiry Krupy 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 CSIRT NASK.
Jednocześnie zgodnie z wyjaśnieniami kierownika kontrolowanej jednostki w okresie podlegającym kontroli nie odnotowano incydentów związanych z bezpieczeństwem teleinformatycznym.
Dowód: wyjaśnienia w piśmie sygn. DAG.0910.1.2023 z dnia 12.01.2024 r. i kopie dokumentów kontrolowanej jednostki – akta kontroli str. 43-48 oraz str. 53-56.
Biorąc pod uwagę powyższe działania kontrolowanej jednostki oceniono **pozytywnie pomimo stwierdzonych uchybień**.

Odpowiadając na projekt wystąpienia pokontrolnego, pismem sygn. DAG.0910.1.2023 z dnia 14.03.2024 r., Dyrektor Archiwum Państwowego w Katowicach, Pani Sławomira Krupa poinformowała, że w dniu 12.03.2024 r. dokonano zgłoszenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego czyli do CSIRT NASK oraz przedstawiła potwierdzający ten fakt dokument.

4. **Realizacja obowiązku okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji kontrolowanej jednostki wynikającego z rozporządzenia 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.**

Zgodnie z § 20 ust. 2 pkt 14 z rozporządzenia 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, 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.

Z wyjaśnień kierownika kontrolowanej jednostki wynika, że w Archiwum Państwowym w Katowicach przeprowadzono audyt wewnętrzny bezpieczeństwa informacji w okresie pomiędzy 17 maja a 17 czerwca 2023 r. Jednocześnie Dyrektor Archiwum Państwowego w Katowicach zapewniła, że kolejny audyt został zaplanowany na I kwartał 2024 r.

W dniu 12.02.2024 r. kierownik zespołu kontrolnego wystąpił do kierownika kontrolowanej jednostki z prośbą o udzielenie informacji czy osoba, która przeprowadziła opisane wyżej czynności posiada kwalifikacje audytora wewnętrznego. W odpowiedzi kierownik kontrolowanej jednostki wyjaśnił, że *(...) do obowiązków Inspektora Ochrony Danych (zwany dalej IOD) należy prowadzenie audytów wewnętrznych w zakresie przestrzegania obowiązujących zasad i przepisów w zakresie ochrony danych osobowych. Ponadto IOD opracowuje i aktualizuje szczegółowe harmonogramy audytów wewnętrznych oraz przygotowuje raport z przeprowadzonego audytu. (...).* Do akt kontroli nie przekazano jednak dokumentu potwierdzającego fakt, że osoba przeprowadzająca audyt posiada niezbędne do tego kwalifikacje.

Dowód: wyjaśnienia kontrolowanej jednostki – akta kontroli str. 139-152 oraz str. 159-162.

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

W odpowiedzi na projekt wystąpienia pokontrolnego, pismem sygn. DAG.0910.1.2023 z dnia 14.03.2024 r., Dyrektor Archiwum Państwowego w Katowicach, Pani Sławomira Krupa poinformowała, że osoba, do zadań której należy przeprowadzanie audytów wewnętrznych w zakresie bezpieczeństwa informacji, została skierowana na szkolenie pt. *Audytor Wewnętrzny Systemu Zarzadzania Bezpieczeństwem Informacji ISO 27001,* które ma odbyć się w terminie 25-26.03. br. przedstawiając dokument potwierdzający ten fakt.

5. Funkcjonowanie w kontrolowanej jednostce Systemu Zarządzania Bezpieczeństwem informacji.

Zgodnie z wyjaśnieniami kierownika kontrolowanej jednostki w Archiwum Państwowym w Katowicach obowiązuje System Zarządzania Bezpieczeństwem Informacji (SZBI), wprowadzony Zarządzeniem nr 24/2023 Dyrektora Archiwum Państwowego w Katowicach

z dnia 17 maja 2023 r. w sprawie wprowadzenia w Archiwum Państwowym w Katowicach systemu zarządzania bezpieczeństwem informacji, który zastąpił poprzednio obowiązującą Politykę Bezpieczeństwa Informacji, zatwierdzoną zarządzeniem nr 32/2019 Dyrektora Archiwum Państwowego w Katowicach z dnia 31 grudnia 2019 r.
Dowód: wyjaśnienia zawarte w piśmie sygn. DAG.0910.1.2023 z dnia 12.01.2024 r. i kopie dokumentów kontrolowanej jednostki – akta kontroli str. 43-52.
Biorąc pod uwagę powyższe zagadnienie oceniono **pozytywnie**.

Biorąc pod uwagę oceny cząstkowe kontrolowanych zagadnień oraz mając na względzie przyjętą skalę ocen, działalność Archiwum Państwowego w Katowicach w zakresie realizacji wybranych aspektów dotyczących bezpieczeństwa teleinformatycznego należy ocenić **pozytywnie pomimo stwierdzonych nieprawidłowości**.

Biorąc pod uwagę powyższe ustalenia i oceny, na podstawie art. 46 ust. 3 pkt 1 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 zalecenia i wniosku pokontrolnego:

1. dostarczenia dokumentu potwierdzającego, że osoba do zadań której należy przeprowadzanie audytów wewnętrznych w zakresie bezpieczeństwa informacji, uzyskała uprawnienia Audytora Wewnętrznego Systemu Zarzadzania Bezpieczeństwem Informacji ISO 27001.

Na podstawie art. 49 ww. ustawy proszę o poinformowanie mnie o sposobie realizacji zaleceń i wniosków pokontrolnych w terminie do dnia 31.05.2024 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.084.10.2023
Identyfikator dokumentu:	1115687
Nazwa dokumentu:	WYSTĄPIENIE POKONTROLNE Z KONTROLI W AP W KATOWICACH.DOCX
Suma kontrolna SHA256 dokumentu:	90b1bc5591f94365506e94ad97406d79d4b7d237797ffb6085b3128a5d4004 1d

Wydrukował(a): [redacted]

Data wydruku: 2024-03-20 12:14:45

.....

Podpisy dokumentu:

Paweł Pietrzyk

Data podpisu: 2024-03-19 19:06:14

Rodzaj podpisu: Kwalifikowany podpis elektroniczny

Numer certyfikatu: 491137481763416838

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