NAJWYŻSZA IZBA KONTROLI

Delegatura w Szczecinie

LSZ.411.3.1.2023

Pani
Marzena Grzywińska
Wójt Gminy Stare Czarnowo

Urząd Gminy w Starym Czarnowie,
ul. Świętego Floriana 10
74-106 Stare Czarnowo

WYSTĄPIENIE POKONTROLNE

I/23/001/LSZ - Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy w Starym Czarnowie, ul. Świętego Floriana 10, 74-106 Stare Czarnowo[1].
Kierownik jednostki kontrolowanej	Marzena Grzywińska, Wójt Gminy Stare Czarnowo od 8.12.2014 r.[2]
Zakres przedmiotowy kontroli	1. Stworzenie, wdrożenie i przestrzeganie polityki z zakresu bezpieczeństwa teleinformatycznego. 2. Przygotowanie organizacyjno – kadrowe do zapewnienia bezpieczeństwa teleinformatycznego.
Okres objęty kontrolą	Lata 2019-2023 do dnia zakończenia kontroli[3], z wykorzystaniem dowodów sporządzonych przed tym okresem, mogących mieć wpływ na ocenę realizacji kontrolowanej działalności.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Szczecinie.
Kontrolerzy	1. Tomasz Cyranka, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/180/2023 z 6 listopada 2023 r. 2. Małgorzata Chabiniak, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/191/2023 z 30 listopada 2023 r. 3. Marta Górska-Jaś, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/195/2023 z 6 grudnia 2023 r. (akta kontroli str. 1-5, 13-16)

[1] Dalej: Urząd lub Jednostka.
[2] Dalej: Wójt.
[3] Tj. do 5 stycznia 2024 r.
[4] Dz.U. z 2022 r. poz. 623; dalej: ustawa o NIK.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli negatywnie ocenia działalność jednostki w badanym zakresie.

W ocenie NIK działania w zakresie zapewnienia bezpieczeństwa przetwarzania informacji nie były wystarczające. W Urzędzie w szczególności nie ustanowiono Systemu Zarządzania Bezpieczeństwem Informacji[6] (zgodnego z normą PN-ISO/IEC 27001[7]), co było niezgodne z § 20 ust. 1 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[8]. W okresie od 28 sierpnia 2018 r. (daty wejścia w życie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa) do dnia 22 lutego 2022 r. w Urzędzie nie wyznaczono osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[9]. Urząd nie posiadał również przygotowanych procedur pozwalających na zachowanie ciągłości działania i odtworzenie utraconych zasobów obejmujących wszystkie aktywa, w szczególności nie sklasyfikowano istniejących w Urzędzie procesów i zasobów informatycznych, w wyniku czego nie opracowano planu odtworzenia wszystkich utraconych zasobów. Urząd nie przeprowadził również analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej, co było działaniem nierzetelnym oraz niezgodnym z § 20 ust. 2 pkt 3 KRI. W Urzędzie nie przeszkolono wszystkich pracowników z zakresu cyberbezpieczeństwa oraz nie zapewniono aktualności inwentaryzacji całego zasobu informatycznego.

Na powyższą ocenę nie wpływają prawidłowe umiejscowienie głównych elementów infrastruktury (serwerowni), tj. w lokalizacji minimalizującej zagrożenia związane z powodzią lub podtopieniami. Jak również zabezpieczenie Urzędu przed zagrożeniami związanymi z elektrycznością w postaci bateryjnych urządzeń podtrzymujących napięcie (UPS-ów), posiadane przez Urząd oprogramowania zabezpieczającego adekwatnego do zidentyfikowanych rodzajów ryzyka, zdefiniowanie fizycznych środków bezpieczeństwa, w tym przebywania w Urzędzie osób nieupoważnionych oraz zasad zarządzania kluczami. Pracownicy stosowali zasady minimalizujące ryzyko nieuprawnionego dostępu do systemów informatycznych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[10] kontrolowanej działalności

OBSZAR

1. Stworzenie, wdrożenie i przestrzeganie polityki z zakresu bezpieczeństwa teleinformatycznego przez Urzędy Gminy

Opis stanu faktycznego

[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Dalej: SZBI.
[7] Norma ISO.
[8] Dz. U. z 2017 r. poz. 2247, dalej: KRI.
[9] Dz. U. z 2023 r. poz. 913, dalej: KSC.
[10] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

1.1. Obowiązująca w Urzędzie, w okresie objętym kontrolą, Polityka Ochrony Danych[11], Polityka Bezpieczeństwa Danych Osobowych[12] wraz z Instrukcją zarządzania systemem informatycznym[13] nie były zgodne z normą PN-ISO/IEC 27001, co stanowiło naruszenie § 20 ust. 3 KRI. Powyższe zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości*. Obowiązujące w Urzędzie POD/PBDO nie zostały poddane certyfikacji PN-ISO/IEC 27001.

(akta kontroli str. 6-12, 47-49)

W Urzędzie w obowiązujących, w okresie objętym kontrolą, zarządzeniach dotyczących ochrony danych osobowych określono zasady, osoby odpowiedzialne za przegląd polityki bezpieczeństwa danych osobowych, częstotliwość przeglądów (co najmniej raz w roku, lub częściej w przypadku np. incydentów). Przeglądy nie były realizowane, co zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 6-12, 35-41, 48-49, 261-278)

W okresie objętym kontrolą nie przeprowadzano corocznych audytów z zakresu bezpieczeństwa informacji (za wyjątkiem przeprowadzonej w 2022 r. Diagnozy Bezpieczeństwa[14]), zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że okresowy audyt w zakresie bezpieczeństwa informacji powinien być prowadzony nie rzadziej niż raz na rok. Powyższe zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 38-41)

W POD i PBDO zadania z zakresu przeprowadzania audytu polityki bezpieczeństwa informacji przypisano Inspektorowi Ochrony Danych[15], co zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 502-503)

1.2. Zasady przeglądu i analizy ryzyka zostały określone w POD z 2019 r. i PBDO z 2022 r., a częstotliwość wykonywania tych prac, została określona na co najmniej raz do roku w PBDO z 2022 r.

(akta kontroli str. 52)

Wójt wyjaśniła: *w PBDO nie określono częstotliwości przeprowadzania analizy ryzyka oraz metodyki tej oceny, ponieważ nie wynika to żadnych obowiązujących przepisów prawa. Zapisy takie planujemy wprowadzić podczas tworzenia SZBI[16], który będzie wykonany w przyszłym roku w ramach środków pochodzących z programu Centrum Projektów Polska Cyfrowa - Cyberbezpieczny Samorząd*.

(akta kontroli str. 38-41, 52-226)

Urząd nie przeprowadzał okresowych analiz ryzyka[17], co było niezgodne z § 20 ust. 2 pkt 3 KRI i zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 6-12, 38-41)

---

[11] Dalej: POD, wprowadzona Zarządzeniami Wójta Gminy nr 59.2018 z 28 września 2018 r., następnie zmieniona zarządzeniem nr 70.2019 z 24 września 2019 r.

[12] Dalej: PBDO, wprowadzona Zarządzeniem Wójta Gminy nr 39.2022 z 13 maja 2022 r.

[13] Wprowadzona Zarządzeniem Wójta Gminy nr 70.2019 z 24 września 2019 r. oraz nr 39.2022 z 13 maja 2022r.

[14] Diagnoza Cyberbezpieczeństwa została przeprowadzona przez Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-ISO/IEC 27001 w ramach kategorii cyberbezpieczeństwo Konkursu Grantowego Cyfrowa Gmina, Oś V, Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, Program Operacyjny Polska Cyfrowa na lata 2014 – 2020

[15] Dalej: IOD.

[16] Systemu zarządzania bezpieczeństwem informacji.

[17] Diagnoza Cyberbezpieczeństwa, pkt. 12: Oceny zgodności z KRI i z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U. z 2018 r. poz. 1560 z późn. zm.

1.3 Jak wyjaśniła Wójt Gminy, dnia 23 lutego 2021 r. wyznaczono dwie osoby[18] odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz tego samego dnia dokonano zgłoszenia do CSIRT NASK[19] ich danych obejmujących: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej. Zarządzeniem nr 70.2021 z dnia 30 września 2021 r. Wójt Gminy wyznaczyła osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu bezpieczeństwa, z datą obowiązywania od 23 lutego 2021 r. Od 28 sierpnia 2018 r. (daty wejścia w życie KSC) do dnia 22 lutego 2022 r. w Urzędzie nie wyznaczono osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z art. 21 ust.1 ustawy KSC. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

Nie zostały wyznaczone osoby wymienione w art. 21 ust 2 i 3 ustawy o KSC, tj. osoby do utrzymywania ww. kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane i przez jej jednostki organizacyjne.

(akta kontroli str. 6-12, 279-283, 481, 500-501)

1.4 W Urzędzie sposób identyfikowania i reagowania na incydenty związane z ochroną danych osobowych zostały zawarte w obowiązujących w okresie kontroli zarządzeniach dotyczących ochrony danych osobowych. Określony także został wzór rejestru takich zdarzeń, jednakże jak wyjaśniła Wójt nie było do tej pory zidentyfikowanych incydentów, przez co nie było konieczności uzupełniania rejestru. Sposób zarządzania incydentami w Urzędzie nie był zgodny z wymaganiami art. 22 KSC, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 6-12, 284-312)

Urząd zapewnił osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami poprzez opublikowanie na swojej stronie stareczarnowo.pl[20] informacji o zagrożeniach związanych z cyberbezpieczeństwem: dwóch komunikatów z 12 września 2019 r. i 22 września 2022 r. Komunikaty te zawierały opis najpopularniejszych zagrożeń i sposobów zabezpieczania się przed nimi, odnośniki do stron internetowych o takiej treści, wykaz podmiotów zajmujących się cyberbezpieczeństwem z adresami ich stron oraz opis sposobu zgłaszania incydentów.

(akta kontroli str. 24-30, 313-319)

1.5 W Urzędzie nie zostały zidentyfikowane krytyczne dane i operacje oraz nie został wprowadzony plan zachowania ciągłości działania. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 6-12, 513-515)

1.6 Kopia zapasowa danych z systemów informatycznych Urzędu była tworzona na serwerze znajdującym się w osobnym, nieoznaczonym pomieszczeniu, innym niż główna serwerownia. Serwer znajdował się w zamykanej szafce, w której zamontowano wentylator. W Urzędzie nie została opracowana szczegółowa procedura odzyskiwania danych, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 320-325, 334-339)

---

[18] Zastępcę Wójta i Kierownika Referatu Organizacyjnego, Spraw Obywatelskich, Promocji i Oświaty - pełniącego też funkcję administratora systemów teleinformatycznych.

[19] Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

[20] https://stareczarnowo.pl/aktualnosci/pokaz/2049 i https://stareczarnowo.pl/aktualnosci/pokaz/2048.

1.7 Urząd nie zlecał tworzenia kopii zapasowej podmiotom zewnętrznym, za wyjątkiem kilku programów, znajdujących się na serwerach firmy zewnętrznej, tj. systemu Rada[21] wraz z dedykowanym kanałem telewizyjnym, BIP[22], e-OBIEG[23], e-BOT[24], CMS do zarządzania stroną www.stareczarnowo.pl oraz poczty e-mail będącej częścią kompleksowego rozwiązaniem Systemu eURZĄD[25]. W umowach zawieranych z firmą zewnętrzną, Wykonawca zobowiązany był do wykonywania backupu różnicowego, jak również pełnego w celu przywrócenia danych. Urząd nie weryfikował procesu tworzenia kopii zapasowych przez podmiot zewnętrzny, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 6-12, 340-379, 461-462, 498-499)

1.8 Testy planów odtwarzania zasobów nie były przeprowadzane. Wójt wyjaśniła: „*Urząd Gminy Stare Czarnowo nie posiada zasobów sprzętowych do odtworzenia zasobów kopii*".

(akta kontroli str. 6-12)

1.9 Urząd Gminy nie posiada ubezpieczenia od zagrożeń fizycznych zasobów informatycznych oraz od utraty ciągłości systemów informatycznych.

(akta kontroli str. 6-12, 41, 500-501)

Wójt wyjaśniła: *Urząd Gminy Stare Czarnowo nie posiada ubezpieczenia od zagrożeń fizycznych zasobów informatycznych oraz od utraty ciągłości systemów informatycznych. Nie było takiej potrzeby i nie wynika to z żadnych przepisów prawa*.

(akta kontroli str. 6-12, 481, 500-501)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Niezgodność obowiązującego w Urzędzie POD/PBDO z normą PN-ISO/IEC 27001, tj. informacji o planowanych działaniach (w POD z 2018 r. i 2019 r.), opisu procesów i zasobów (w POD z 2018 r.), potwierdzenia zakomunikowania polityk wszystkim pracownikom (POD z 2018 r. i 2019 r.), opisu zasad wykonywania telepracy (w POD z 2019 r.), klasyfikacji przetwarzanych informacji (w POD z 2018 r.), co było niezgodne z § 20 ust. 3 KRI.

Ponadto w opinii biegłego aktualnie obowiązująca PBDO określa zasady bezpieczeństwa danych osobowych, a więc ogranicza się tylko do danych osobowych i nie odnosi się do wszystkich innych informacji wymagających ochrony (zgodnie z § 20 ust. 1 KRI).

(akta kontroli str. 47-51, 463-480)

Wójt wyjaśniła: *W Urzędzie Gminy Stare Czarnowo nie opracowano systemu zarządzania bezpieczeństwem informacji (dalej SZBI). Jednakże ustanowiono Politykę Bezpieczeństwa Danych Osobowych (dalej PBDO) wraz z Instrukcją zarządzania systemem informatycznym, będącą załącznikiem do PBDO. Instrukcja ta została wdrożona w dniu 13.09.2019 r., a następnie zaktualizowana 05.05.2022 r.* (…)*SZBI jest dokumentem obszernym, na które opracowanie nie mieliśmy do tej pory środków finansowych. Jednak w związku z naborem w programie Centrum Projektów Polska Cyfrowa - Cyberbezpieczny Samorząd, planujemy opracować i sfinansować*

[21] System wspomagający pracę Rady Miasta, Gminy i Powiatu pozwala na dostarczanie dokumentów na posiedzenia w formie elektronicznej, przeprowadzanie głosowań, tworzenie porządku obrad i dodatkowo - automatycznie prezentuje wybrane informacje (o pracy Radnych) na portalu informacyjnym przeznaczonym dla Obywateli.

[22] System do prowadzenia Biuletynu Informacji Publicznej.

[23] System elektronicznego obiegu dokumentów.

[24] Oprogramowania wraz z mechanizmem umożliwiającym wytwarzanie kart usług i formularzy w Elektronicznym Biurze Obsługi Interesanta.

[25] www.elektronicznysamorzad.pl.

SZBI w 2024 r. w ramach środków pochodzących z zadania Cyberbezpieczny Samorząd. W związku z tym, że w Urzędzie Gminy Stare Czarnowo nie opracowano SZBI, nie poddano go certyfikacji ISO 27001. Zastępca Wójta wyjaśnił: *Nie posiadamy list potwierdzających fakt zapoznania się z zarządzeniami nr 70.2019 z 24.9.2019 r. i 59.2018 z 28.9.2018 r.* W 2021 r. w oświadczeniach składanych przez pracowników Urzędu w związku z upoważnieniem do przetwarzania danych osobowych wprowadzono zapis mówiący o zapoznaniu się z obowiązującymi w tym obszarze regulacjami wewnętrznymi Urzędu.

(akta kontroli str. 6-12,35-37, 48-51)

2. Nieprzeprowadzenie przez Wójta w okresie objętym kontrolą przeglądów POD/PBDO. Zgodnie z § 20 ust. 1 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. W rozumieniu normy PN-ISO/IEC 27001 najwyższe kierownictwo powinno przeprowadzać przegląd systemu zarzadzania bezpieczeństwem informacji w organizacji w zaplanowanych odstępach czasu, w celu zapewnienia jego stałej przydatności, adekwatności i skuteczności. Przegląd zarządzania powinien uwzględniać:
a) stan działań podjętych w następstwie wcześniejszych przeglądów zarzadzania;
b) zmiany czynników zewnętrznych i wewnętrznych, istotnych dla systemu zarządzania bezpieczeństwem informacji;
c) informacje zwrotne o wynikach działań na rzecz bezpieczeństwa informacji, w tym trendach w zakresie:
   1) niezgodności i działań korygujących;
   2) wyników monitorowania i pomiarów;
   3) wyników audytów; oraz
   4) spełniania celów bezpieczeństwa informacji.
d) informacje zwrotne od stron zainteresowanych;
e) wyniki szacowania ryzyka i stan planów postępowania z ryzykiem; oraz
f) możliwości ciągłego doskonalenia.
Dane wyjściowe z przeglądu zarządzania powinny zawierać decyzje związane z możliwościami ciągłego doskonalenia i potrzebami dotyczącymi zmian w systemie zarządzania bezpieczeństwem informacji.

(akta kontroli str. 35-41)

W sprawie niewykonywania przeglądów POD/PBDO Zastępca Wójta wyjaśnił: „*W 2019 r. został wykonany raport z uproszczonej analizy ryzyka w oparciu o PBDO, natomiast w kwietniu 2020 roku przeprowadzono audyt w zakresie analizy przetwarzania danych osobowych oraz podjętych działań, a także przygotowania dalszych rekomendacji do wdrożenia zmian w systemie ochrony danych osobowych, czego efektem były wnioski i rekomendacje dotyczące wprowadzenia zmian w PBDO. Od przeprowadzenia audytu w kwietniu 2020 r. trwały prace nad nową polityką ochrony danych wdrożoną w maju 2022 r. Wszystkie uwagi i problemy które wyniknęły w czasie prac nad polityka zostały w niej ujęte. W tym czasie nie przeprowadzano przeglądów. Raz wzroku wykonywany jest audyt sprzętu i oprogramowania w celu wyeliminowania sprzętu przestarzałego technologicznie i oprogramowania.* Wójt wyjaśniła: „*W ramach audytu firma zewnętrzna sprawdza stacje robocze pracowników urzędu i przekazuje informacje, które komputery należy wymienić lub części np.: dyski lub RAM. Sprzęt w serwerowni sprawdzany jest na bieżąco i wymieniany jest lub modernizowany w zależności od awarii i posiadanych środków finansowych. Dodatkowo na bieżąco sprawdzane jest oprogramowanie na komputerach.*” Jak

wyjaśnił administrator systemów informatycznych[26], od 2019 r. nie wprowadzono w Urzędzie Gminy Stare Czarnowo nowych systemów przetwarzających dane.

(akta kontroli str. 35-41)

3. Nieprzeprowadzanie corocznych audytów z zakresu bezpieczeństwa informacji (za wyjątkiem przeprowadzonej w 2022 r. Diagnozy Bezpieczeństwa), zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że okresowy audyt w zakresie bezpieczeństwa informacji powinien być prowadzony nie rzadziej niż raz na rok.
W dniach od 2 marca 2020 r. do 16 kwietnia 2020 r. w Urzędzie przeprowadzono audyt w zakresie analizy przetwarzania danych osobowych oraz podjętych działań, a także przygotowania dalszych rekomendacji do wdrożenia zmian w systemie ochrony danych osobowych, czego efektem były wnioski i rekomendacje dotyczące wprowadzenia zmian w PBDO. Przeprowadzony audyt dotyczył kwestii formalnych w zakresie ochrony danych osobowych, nie objął swoim zakresem art. 32 RODO[27], który odnosi się do bezpieczeństwa przetwarzania, a więc brak podstaw na potwierdzenie, że niniejsze zadanie odnosiło się do bezpieczeństwa informacji. Wnioski i rekomendacje z audytu nie zostały wdrożone[28].

(akta kontroli str. 6-12, 38-41, 227-278)

Wójt wyjaśniła: „*Wnioski i rekomendacje zawarte w przeprowadzonym w kwietniu 2020 r. audycie, planowaliśmy wdrożyć w 2020 r. Jednak w związku z pandemią COVID-19, było to niemożliwe. Obecnie wszystkie wnioski planujemy wykorzystać podczas tworzenia SZBI, który będzie wykonany w przyszłym roku w ramach środków w programie Centrum Projektów Polska Cyfrowa - Cyberbezpieczny Samorząd*".

(akta kontroli str. 6-12, 38-41, 227-260)

W sprawie nieprzeprowadzania corocznych audytów zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI Wójt wyjaśniła: „*Audyt z zakresu bezpieczeństwa informacji planowaliśmy przeprowadzić w 2020 r., jednak w związku z pandemią COVID-19, było to niemożliwe. Audyt planujemy przeprowadzić w przyszłym roku, w ramach środków pochodzących z programu Centrum Projektów Polska Cyfrowa - Cyberbezpieczny Samorząd*".

(akta kontroli str. 38-41)

NIK zauważa, że w przeprowadzonej w 2022 r. Urzędzie Diagnozie Cyberbezpieczeństwa, obejmującej ocenę wybranych aspektów bezpieczeństwa systemów informatycznych, sformułowano następujące zalecenia, które do dnia zakończenia kontroli nie zostały zrealizowane:

- Instytucje realizujące zadania publiczne muszą działać zgodnie z wytycznymi KRI, w tym wprowadzić politykę bezpieczeństwa informacji, tj. zestaw udokumentowanych, dostosowanych do organizacji zasad i procedur wraz z planem wdrożenia i monitorowania. Polityka bezpieczeństwa danych osobowych powinna stanowić element większej Polityki Bezpieczeństwa Informacji dla podmiotów publicznych (§ 20 ust. 1 KRI). Kierownictwo organizacji (zgodnie z § 20 ust. 2 KRI) powinno mieć warunki umożliwiające egzekwowanie działań takich jak: bieżąca aktualizacja inwentaryzacji sprzętu i oprogramowania, prowadzenie okresowych analiz ryzyka, zapewnienie planu szkoleń dla osób zaangażowanych w przetwarzanie informacji dotyczących zapewnienia bezpieczeństwa informacji, zapewnienie ochrony danych przed kradzieżą, nieuprawnionym dostępem, zapewnienie audytów wewnętrznych w zakresie bezpieczeństwa informacji.

[26] Dalej: ASI
[27] Dz.Urz.UE.L nr 119, str. 1, dalej: RODO
[28] Diagnoza Cyberbezpieczeństwa, pkt. 12.

- Należy przygotować kompletną dokumentację dotyczącą architektury rozwiązań, architektury sieci, zmian w systemach informacyjnych, rejestr dostępu do dokumentacji itp.

(akta kontroli str. 38-41, 261-278)

4. Przypisanie w POD i PBDO zadań z zakresu przeprowadzania audytu polityki bezpieczeństwa informacji Inspektorowi Ochrony Danych, powyższe stanowiło naruszenie art. 38 ust. 6 Rozporządzenia 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/We (RODO).

Art. 38 ust. 6 RODO - *Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.*

(akta kontroli str. 502-503*)*

Wójt wyjaśniła: „*Przepisy prawa nie zabraniają Inspektorowi Danych Osobowych przeprowadzania audytu polityk w dziedzinie ochrony danych osobowych. W Urzędzie Gminy Stare Czarnowo sprawami dotyczącymi RODO zajmuje się jedna osoba. Przeprowadzanie audytów polityk przez podmiot zewnętrzny, prowadziłoby to powstania dodatkowych kosztów, na pokrycie których, nie mieliśmy środków w budżecie gminy*".

(akta kontroli str. 513-515)

W ocenie NIK w niniejszym przypadku przypisanie IOD zadań z zakresu przeprowadzania audytu polityki bezpieczeństwa informacji powoduje powstanie konfliktu interesu. Powyższe wynika z faktu, iż zadaniem audytora jest sprawdzenie przestrzegania zgodności działań urzędu (jego pracowników) z przepisami prawa (w tym RODO), natomiast jednym z zadań IOD jest decydowanie o stosowaniu przepisów RODO w Urzędzie (art. 39 ust. 1 RODO).

(akta kontroli str. 502-503)

5**.** Nieprzeprowadzenie przez Urząd w okresie objętym kontrolą okresowych analiz ryzyka, co było niezgodne z § 20 ust. 2 pkt 3 KRI.

Zgodnie z art. 20 ust. 2 pkt 3 KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy. Ponadto brak identyfikacji występujących w Urzędzie krytycznych danych i operacji uniemożliwił dokonanie ich okresowej oceny przy zastosowaniu powyższych kryteriów.

(akta kontroli str. 261-278)

Wójt wyjaśniła: „*Analizę ryzyka planowaliśmy przeprowadzić w 2020 r., jednak w związku z pandemią COViD"19, było to niemożliwe. W 2022 r. zaktualizowano PBDO wraz z Instrukcją zarządzania systemem informatycznym. Na tej podstawie obecnie przeprowadzana jest analizy ryzyka*".

(akta kontroli str. 6-12, 38-41)

W okresie objętym kontrolą w Urzędzie co prawda przeprowadzono w 2019 r. uproszczoną analizę ryzyka w celu określenia ogólnego poziomu ryzyka dla przetwarzania danych osobowych. W raporcie z 18 września 2019 r. ogólny poziom ryzyka dla przetwarzania danych osobowych określono jako niski i zalecono zastosowanie technicznych i organizacyjnych środków bezpieczeństwa właściwych dla Poziomu I. Przeprowadzona analiza koncentrowała się jedynie na ryzyku praw

i wolności osób, których dane są przetwarzane (i ogranicza się tylko do utraty poufności i dostępności pomijając integralność), a więc odnosiła się tylko do analizy wpływu na osoby fizyczne. Nie objęto analizą ryzyka bezpieczeństwa informacji i analizy wpływu zmaterializowania się zagrożenia na Urząd, przez co Urząd nie miał możliwości weryfikacji jakie zagrożenia i podatności były brane pod uwagę.

(akta kontroli str. 6-12, 217-226)

6. Niewyznaczenie w Urzędzie w okresie od 28 sierpnia 2018 r. (daty wejścia w życie KSC) do dnia 22 lutego 2022 r. osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z art. 21 ust. 1 ustawy KSC – *Podmiot publiczny, (…) realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa*.

(akta kontroli str. 6-12, 279-283)

Wójt wyjaśniła: *Nie mieliśmy świadomości, że jest taki obowiązek. Niezwłocznie po otrzymaniu informacji, że należy wyznaczyć osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, osoby zostały wyznaczone*.

(akta kontroli str. 481, 500-501)

7. Nieokreślenie i niewdrożenie w Urzędzie, w okresie objętym kontrolą, kompleksowego procesu zarządzania incydentami związanymi z bezpieczeństwem informacji. Na podstawie opinii biegłego ustalono[29], iż PBDO określa zasady bezpieczeństwa danych osobowych, a więc ogranicza się tylko do danych osobowych i nie odnosi się do wszystkich innych informacji wymagających ochrony (zgodnie z § 20 ust. 1 rozporządzenia KRI). Ustanowiona procedura postępowania w związku z naruszeniem ochrony danych osobowych (Załącznik nr 10 do PBDO) określa zasady postępowania w przypadku wystąpienia lub podejrzenia wystąpienia naruszenia ochrony danych osobowych u Administratora, a więc procedura ta nie obejmuje swoim zakresem zasad postępowania w przypadkach wystąpienia incydentu związanego z bezpieczeństwem informacji (innych niż dane osobowe). Jednostka nie wprowadziła zasad i odpowiedzialności w związku z wymogiem określonym w § 20 ust .2 pkt 13) rozporządzenia KRI oraz w zakresie zgłaszania i obsługi incydentu w podmiocie publicznym w związku z art. 22 i art. 23 KSC.

(akta kontroli str. 301-312,463-480)

Wójt wyjaśniła: *Zasady i odpowiedzialność w związku z wymogiem określonym w § 20 ust. 2 pkt. 13 rozporządzenia KRI oraz Zgłaszanie i obsługę incydentu w podmiocie publicznym w związku z art. 22 i art. 23 ustawy o krajowym systemie cyberbezpieczeństwa zostaną ujęte w systemie zarządzania bezpieczeństwem informacji, który planujemy opracować w 2024 roku.*

(akta kontroli str. 516-518)

8. Niedokonanie klasyfikacji procesów i zasobów informatycznych, co skutkowało brakiem możliwości określenia adekwatnych mechanizmów zabezpieczeń celem ich ochrony. Powyższe było działaniem nierzetelnym, albowiem zgodnie ze standardem C.12 zawartym w Komunikacie nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych – *Należy zapewnić istnienie mechanizmów służących utrzymaniu ciągłości działalności jednostki sektora finansów publicznych wykorzystując, między innymi, wyniki analizy ryzyka*. Natomiast zgodnie ze standardem C.15 – *Należy określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych*.

[29] W oparciu o sprawozdanie z przeprowadzonych analiz w obszarze bezpieczeństwa teleinformatycznego biegłego powołanego w trakcie kontroli NIK.

(akta kontroli str. 6-12)

Wójt wyjaśniła: „*W Urzędzie Gminy Stare Czarnowo zidentyfikowane mamy krytyczne dane i operacje, tylko nie są one spisane w formie dokumentu. Na chwilę obecną nie widzimy potrzeby posiadania takiego dokumentu, skoro znane są nam krytyczne dane i operacje*".

(akta kontroli str. 513-515)

9. Niezawarcie, w okresie objętym kontrolą, w obowiązujących planach ciągłości działania[30] szczegółowych wykazów aplikacji, usług, systemów operacyjnych, zbiorów danych oraz ram czasowych niezbędnych do ich odtworzenia w przypadku awarii lub ich utraty, które powinny zapewniać możliwość wykonania tych czynności w niekorzystnych warunkach, np. w przypadku niedostępności osoby (firmy), która za ten proces na co dzień odpowiada.
W planie będącym załącznikiem do POD z 2018 r. jako zasoby podlegające archiwizacji wskazano wszystkie dane (pliki, bazy danych, systemy pocztowe). W planach będącym załącznikami do POD z 2018 r. i PBDO z 2022 r. wymieniono: bazy danych zawierające dane osobowe, programy i aplikacje wykorzystywane do przetwarzania danych osobowych, system operacyjny, dane konfiguracyjne systemu informatycznego, logi systemowe, inne zasoby, jeżeli wykonywanie ich kopii zapasowych jest zasadne w świetle ochrony danych osobowych. W planie ciągłości działania nie zostały uwzględnione inne zagrożenia, takie jak np. brak dostępności kluczowych osób, kradzież czy zniszczenie fizycznych dokumentów, brak dostępu do mediów (zasilania, Internetu), masowy atak malware, atak ransomware, niedostępność głównej siedziby z powodu pożaru, zalania itp.

(akta kontroli str. 320-333)

Wójt wyjaśniła: „*W chwili tworzenia zapisów zawartych we wskazanych zarządzeniach założono, że prawdopodobieństwo wystąpienia innych zagrożeń jest niewielkie*".

(akta kontroli str. 514-515)

Urząd nie opracował ponadto szczegółowych procedur i zasad dotyczących zarządzania konfiguracją, które określają, jak konfiguracja systemów jest dokumentowana, aktualizowana i kontrolowana. Nie posiadał także udokumentowanej, aktualnej konfiguracji systemu, tzn. zbioru plików konfiguracyjnych, zrzutów ekranu lub innych sposobów udokumentowania aktualnej konfiguracji (ustawień) używanych w Urzędzie programów. W odpowiedzi na pytanie, czy Urząd posiada ww. procedury i zasady, Wójt wyjaśniła: *Nie. Backupy systemu wykonywane są regularnie. Nigdy nie mieliśmy przypadku utracenia danych*.

(akta kontroli str. 261-278, 461-462, 498-499)

W Urzędzie nie istniała spójna dokumentacja zmian w systemach. Informacje te można było pozyskać z uzupełnianego opisu aktualizacji i zestawienia z „Rejestracji Czasu Pracy" pracownika firmy zewnętrznej, świadczącej usługi wsparcia technicznego[31].

(akta kontroli str. 261-278)

Wójt wyjaśniła: *Zdarzały się pojedyncze przypadki odtworzenia plików z kopii np. po skasowaniu przez użytkownika potrzebnych plików lub po problemach z aktualizacją używanych przez urząd aplikacji księgowych. W 2019 r. został wymieniony jeden z serwerów (aplikacja EZD eObieg) - dane zostały odtworzone z lokalnej kopii bezpieczeństwa. Zadanie to zostało wykonane przez firmę zewnętrzną, która*

[30] Określonych w obowiązujących w okresie objętym kontrolą POD/PODO.
[31] Diagnoza Cyberbezpieczeństwa, pkt. 3.5 Oceny wybranych aspektów bezpieczeństwa systemów informatycznych.

zajmowała się na podstawie zawartej z Urzędem umowy obsługą i utrzymaniem tej aplikacji. W 2021 r. miało miejsce przywrócenie systemu księgowego i plików użytkowników z kopii po awarii serwera udostępniającego aplikacje, co zostało wykonane w ramach umowy o świadczenie usług informatycznych przez firmę zewnętrzną. Nigdy nie mieliśmy przypadku utracenia danych. Obie te umowy zawierały zapisy o poufności. Zgodnie z PBDO kopie zapasowe są przechowywane przez okres 12 miesięcy i niszczone zgodnie z odrębną procedurą, zaś oględziny wykazały, że jest to od 7 do 14 dni.

(akta kontroli str. 6-12, 340-379, 461-462, 498-499)

10. Nieweryfikowanie przez Urząd procesu tworzenia kopii zapasowych przez podmiot zewnętrzny w tym: nie weryfikował czy zapisane pliki/oprogramowanie w procesie tworzenia kopii zapasowych lub odtwarzania utraconych zasobów przeszły jakiekolwiek modyfikacje, nie weryfikował czy usługodawca zapewnia proces testowania kopii zapasowych i odtwarzania utraconych zasobów, nie włączył do umowy z usługodawcą zapewnienia ciągłości działania, nie przeprowadził testów planu odtwarzania utraconych zasobów.

Urząd nie zlecał tworzenia kopii zapasowej podmiotom zewnętrznym, za wyjątkiem kilku programów, znajdujących się na serwerach firmy zewnętrznej tj. systemu Rada[32] wraz z dedykowanym kanałem telewizyjnym, BIP[33], e-OBIEG[34], e-BOT[35], CMS do zarządzania stroną www.stareczarnowo.pl oraz poczty e-mail będącej częścią kompleksowego rozwiązaniem Systemu eURZĄD[36]. W umowach zawieranych z firmą zewnętrzną, Wykonawca zobowiązany był do wykonywania backupu różnicowego jak również pełnego w celu przywrócenia danych.

(akta kontroli str. 6-12, 340-379)

Wójt wyjaśniła: *Nigdy nie mieliśmy przypadku utracenia danych*.

(akta kontroli str. 461-462, 498-499)

W opinii biegłego Jednostka nie przedstawiła udokumentowanych dowodów na systematyczne testowanie i weryfikację kopii zapasowych, co budziło poważne obawy w zakresie możliwości pełnego i efektywnego odtwarzania danych oraz systemów informatycznych w przypadku awarii. Ponadto, dostarczona dokumentacja nie zawierała szczegółowych procedur awaryjnego odtworzenia zbiorów danych i wykorzystywanych systemów informatycznych oraz planu zapewnienia ciągłości działania, dostosowanego do specyficznych potrzeb i procesów operacyjnych Jednostki. Brak takiego planu oraz brak dowodów na zdolność Jednostki do skutecznego odtworzenia procesów w akceptowalnych ramach czasowych wskazywała na istotne luki w przygotowaniach na ewentualne sytuacje awaryjne lub kryzysowe. Zidentyfikowane braki w procesach testowania kopii zapasowych oraz w opracowaniu procedur awaryjnego odtwarzania danych i systemów informatycznych, a także brak kompleksowego planu zapewnienia ciągłości działania, mogły narażać Jednostkę na znaczne ryzyko w przypadku wystąpienia sytuacji awaryjnych, co wymagało niezwłocznego podjęcia działań korygujących.

(akta kontroli str. 463-480)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w badanym zakresie.

---

[32] System wspomagający pracę Rady Miasta, Gminy i Powiatu pozwala na dostarczanie dokumentów na posiedzenia w formie elektronicznej, przeprowadzanie głosowań, tworzenie porządku obrad i dodatkowo - automatycznie prezentuje wybrane informacje (o pracy Radnych) na portalu informacyjnym przeznaczonym dla Obywateli.

[33] System do prowadzenia Biuletynu Informacji Publicznej.

[34] System elektronicznego obiegu dokumentów.

[35] Oprogramowania wraz z mechanizmem umożliwiającym wytwarzanie kart usług i formularzy w Elektronicznym Biurze Obsługi Interesanta

[36] www.elektronicznysamorzad.pl

Negatywną ocenę cząstkową uzasadnia brak podjęcia prawidłowych działań dotyczących stworzenia, wdrożenia i przestrzegania polityki z zakresu cyberbezpieczeństwa. Powyższe potwierdzają stwierdzone nieprawidłowości, w szczególności wskazujące na niezgodność obowiązujących Urzędzie POD/PBDO z normą PN-EN ISO/IEC 27001, jak również przypisanie zadań z zakresu przeprowadzania audytu i polityki bezpieczeństwa informacji IOD powodujące konflikt interesów. W okresie od 28 sierpnia 2018 r. do 22 lutego 2022 r. w Urzędzie nie było wyznaczonej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Urząd nie przeprowadzał okresowych analiz ryzyka (zgodnie z § 20 ust. 2 pkt 3 KRI), corocznych przeglądów (zgodnie z § 20 ust. 1 KRI) i audytów (zgodnie z § 20 ust. 2 pkt 14 KRI) obowiązujących w okresie kontroli POD/PBDO. Urząd nie dokonał klasyfikacji procesów i zasobów informatycznych i w związku z tym nie był w stanie określić adekwatnych mechanizmów zabezpieczeń celem ich ochrony. Proces zarządzania incydentami związanymi z bezpieczeństwem informacji ogranicza się tylko do danych osobowych i nie odnosi się do wszystkich innych informacji wymagających ochrony (zgodnie z §20 ust. 1 rozporządzenia KRI). Urząd nie posiadał również przygotowanych procedur pozwalających na zachowanie ciągłości działania i odtworzenie utraconych zasobów obejmujących wszystkie aktywa, w szczególności nie sklasyfikowano istniejących w Urzędzie procesów i zasobów informatycznych, w wyniku czego nie opracowano planu odtworzenia wszystkich utraconych zasobów oraz nie opracował szczegółowych procedur i zasad dotyczących zarządzania konfiguracją, które określają, jak konfiguracja systemów jest dokumentowana, aktualizowana i kontrolowana oraz nie posiadał udokumentowanej, aktualnej konfiguracji systemu. Urząd nie weryfikował procesu tworzenia kopii zapasowych przez podmiot zewnętrzny tego oprogramowania.

OBSZAR

2. Przygotowanie organizacyjno-kadrowe urzędu do zapewnienia bezpieczeństwa teleinformatycznego

Opis stanu faktycznego

2.1. Oględziny[37] głównych elementów infrastruktury (serwerowni) wykazały m.in., że zostały one umiejscowione na drugim piętrze budynku Urzędu, co minimalizowało zagrożenia związane z powodzią lub podtopieniami, ponadto serwerownia wyposażona była w klimatyzację.

(akta kontroli str. 385-386)

Urząd nie przeprowadził analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej, co było działaniem nierzetelnym oraz niezgodnym z § 20 ust. 2 pkt 3 KRI. Szerzej o tym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 6-12)

2.2. W Urzędzie podjęto działania zabezpieczające przed zagrożeniami związanymi z elektrycznością. Urząd posiadał zabezpieczenie w przypadku przerw w dostawie prądu, tj. według stanu na 30 listopada 2023 r. wszyscy pracownicy (z wyjątkiem jednego) pracujący przy komputerze mieli podłączone komputery i monitory do UPS. W przypadku pracownika nieposiadającego UPS Wójt wyjaśniła m.in., że: *pracownik we wrześniu 2023 r. zmienił lokalizację i został przeniesiony do innego pokoju, w którym znajdował się tylko jeden UPS, do którego były już podłączone maksymalnie cztery urządzenia; zaplanowano zakup dodatkowego UPS, w ramach naboru Cyberbezpieczny Samorząd, w którym Gmina złoży wniosek.*
Przewidywana (planowana) długość podtrzymywania napięcia przez UPS, zgodnie z instrukcją producenta wynosiła od jednej do 30 minut. Akumulatory będące

[37] Przeprowadzone 10 listopada 2023 .

elementami systemu UPS były wymieniane zgodnie z deklarowaną przez producenta żywotnością, która została określona na trzy - cztery lata. W okresie objętym kontrolą wystąpiło 20 (na 24 UPS) takich wymian.

(akta kontroli str. 42-44, 380-381, 382)

W Urzędzie nie prowadzono ewidencji dotyczącej regularnego serwisowania i konserwacji systemów UPS oraz nie przeprowadzano regularnych testów urządzeń UPS. Wójt wyjaśniła m.in., że: *(…) prowadzenie ewidencji nie wynika z żadnych przepisów prawa. W Urzędzie nie wykonujemy zaplanowanych testów urządzeń UPS. Sprawność urządzeń weryfikujemy podczas wyłączeń energii elektrycznej przez firmę energetyczną, które mają miejsce kilkukrotnie w ciągu każdego roku. Po każdym takim przypadku pracownicy zgłaszają telefonicznie (…) każdy zaistniały przypadek niesprawnego działania UPS-ów. Na tej podstawie urządzenia oddawane są do firmy informatycznej do oględzin i do naprawy.*

W Urzędzie nie przeprowadzano w przypadku UPS testów obejmujących sprawdzenie rzeczywistego czasu podtrzymania napięcia w stosunku do czasu deklarowanego przez producenta. Wójt wyjaśniła, że takie testy mogłyby doprowadzić przy podłączonych urządzeniach typu monitory i stacje robocze do ich uszkodzenia.

W sprawie przeszkolenia personelu odpowiedzialnego za obsługę i utrzymanie UPS Wójt wyjaśniła m.in., że: *Pracownicy Urzędu (…) zostali odpowiednio przeszkoleni z obsługi UPS-ów. Podczas podłączenia UPS-ów na danym stanowisku pracy, pracownicy byli informowani (…), że nie mogą żadnego sprzętu podłączać samodzielnie do UPS-ów, a w przypadku awarii, polegającej na wyłączeniu się samodzielnemu stacji roboczej podczas wyłączeń energii elektrycznej, mają każdy taki przypadek niezwłocznie zgłaszać (…).*

(akta kontroli str. 43-44)

Oględziny[38] wyłączników zasilania w budynku Urzędu wykazały, że znajdowały się cztery przeciwpożarowe wyłączniki prądu, w tym jeden na zewnątrz budynku (przy wejściu) oraz trzy przy schodach łączących piętra budynku Urzędu. Wyłączniki znajdowały się w obudowie zabezpieczającej (szybka) przed przypadkowym użyciem oraz zawierały opis informujący do czego służą.

(akta kontroli str. 383-384)

2.3. W Urzędzie nie zatrudniano pracowników ochrony. Zasady fizycznego dostępu do pomieszczeń[39], opisano w załączniku nr 12 do PBDO[40] – Opis technicznych i organizacyjnych środków bezpieczeństwa. Według ww. załącznika do fizycznych środków bezpieczeństwa zaliczało się m.in.: zamykanie pomieszczeń na klucz (fizyczna kontrola dostępu) - zabezpieczenie wejść do pomieszczeń zamkami, elektrozaczepami lub innymi urządzeniami ograniczającymi dostęp; ograniczenie wstępu osób trzecich - uniemożliwienie osobom nieupoważnionym przebywania w pomieszczeniach bez zgody Administratora lub wyłącznie w towarzystwie Użytkowników[41] oraz zarządzanie kluczami – wprowadzenie zasad udostępniania kluczy. Zgodnie z zasadą udostępniania kluczy Administrator wydawał klucze lub inne urządzenia dostępowe (karty, chipy) wyłącznie uprawnionym Użytkownikom oraz stosował środki chroniące klucze przed dostępem osób nieupoważnionych. Klucze zapasowe do pomieszczeń mogły być wydawane w sytuacjach awaryjnych. Użytkownik dysponujący kluczami nie mógł ich przekazywać osobom

[38] Przeprowadzone 10 listopada 2023 r.

[39] Rozumie się przez to budynki, lokale, pokoje, pomieszczenia lub części pomieszczeń określone przez Administratora, w których przetwarzane są dane w formie papierowej (kartotekach) lub systemach informatycznych, tworzące obszar przetwarzania danych.

[40] Z 13 maja 2022 r.

[41] Rozumie się przez to pracownika lub osobę upoważnioną przez Administratora lub osobę przez niego wyznaczoną, uprawnioną do bezpośredniego dostępu do danych papierowych lub danych elektronicznych.

nieupoważnionym oraz był obowiązany przedsięwziąć działania celem wykluczenia ryzyka ich utraty. Przebywanie osób innych aniżeli pracownicy w pomieszczeniach było możliwe wyłącznie w obecności Użytkowników lub za zgodą Administratora. Stały dostęp do pomieszczeń, w których przetwarzane były dane osobowe mieli tylko Użytkownicy.

(akta kontroli str. 8-12, 504-512)

W sprawie opisu pisemnych zasad wstępu i przebywania w serwerowni i pomieszczeniu z serwerem do tworzenia kopii zapasowych (pracowników, serwisu, osób sprzątających) Zastępca Wójta wyjaśnił, że nie opisano pisemnie ww. zasad, ale ustalono, że do serwerowni mają dostęp tylko osoby wskazane przez ASI lub Inspektora bezpieczeństwa teleinformatycznego. Ponadto osoby pobierające klucze do serwerowni, mają obowiązek udokumentowania tego faktu w zeszycie wejść do serwerowni. Klucze do serwerowni znajdują się w pokoju (w skrzynce na klucze), do których dostęp mają tylko ww. osoby. W sprawie prowadzonej listy osób upoważnionych do odbioru kluczy do ww. pomieszczeń Zastępca Wójta wyjaśnił, że taka lista nie jest prowadzona.

(akta kontroli str. 24-30)

Oględziny[42] serwerowni w budynku Urzędu wykazały, że pomieszczenie to, zawierające główne elementy infrastruktury, znajdowało się na drugim piętrze budynku Urzędu oraz nie było oznaczone. Brak było planów zamieszczonych w przestrzeni ogólnodostępnej Urzędu, na których oznaczono znajdujące się ww. pomieszczenie. Serwerownia była wyposażona w klimatyzację. Pomieszczenie to nie było zabezpieczone w sposób minimalizujący nieuprawniony dostęp, w szczególności nie posiadało drzwi przeciwpożarowych / antywłamaniowych oraz zamka o zwiększonej odporności na włamanie. Wejście do serwerowni nie było rejestrowane przez elektroniczny system kontroli dostępu ani monitorowane przez system monitoringu wizyjnego. Prowadzono rejestr osób niebędących pracownikami Urzędu odwiedzających to pomieszczenie.

(akta kontroli str. 385-386, 387-388)

2.4. W okresie objętym kontrolą w Urzędzie przeprowadzono dwa szkolenia z zakresu cyberbezpieczeństwa dla trzech (z 28) pracowników, tj. inspektora bezpieczeństwa teleinformatycznego i administratora systemu teleinformatycznego[43] oraz pracownika Referatu Inwestycji, Nieruchomości, Gospodarki Komunalnej, Rolnictwa i Ochrony Środowiska[44]. Pozostali pracownicy nie zostali przeszkoleni w zakresie cyberbezpieczeństwa. Ponadto dwóch pracowników Urzędu uczestniczyło w łącznie czterech szkoleniach dotyczących programu Rodzina 500+. Szerzej o tym w sekcji *Stwierdzone nieprawidłowości.*

W sprawie określenia w Urzędzie planu szkoleń dla pracowników Zastępca Wójta wyjaśnił, że: *nie został określony plan szkoleń. Pracownicy ustalają udział w szkoleniach na bieżąco ze swoim bezpośrednim przełożonym i wynika on w dużej mierze ze zmiany przepisów, które zmieniają się w ciągu roku, co utrudnia opracowanie planu szkoleń. Pracownicy zajmujący się w urzędzie cyberbezpieczeństwem, są szkoleni w tym zakresie na bieżąco.*

(akta kontroli str. 24-30, 394-402)

---

[42] Przeprowadzone 10 listopada 2023 r.

[43] Specjalistyczne szkolenie dla administratorów systemów i inspektorów bezpieczeństwa teleinformatycznego wymagane przepisami art. 52 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych; przeprowadzone 12 maja 2023 r. przez Agencję Bezpieczeństwa Wewnętrznego.

[44] Przeciwdziałanie cyberzagrożeniom w aspekcie ochrony informacji krytycznej; przeprowadzone w dniach 13-14 września 2022 r. przez Zachodniopomorski Urząd Wojewódzki Wydział Bezpieczeństwa i Zarządzania Kryzysowego.

W sprawie określenia przez Urząd wykazów umiejętności niezbędnych dla poszczególnych stanowisk Zastępca Wójta wyjaśnił, że: *w trakcie naboru na dane stanowiska pracy, określone są w ogłoszeniach wykazy umiejętności niezbędnych, które musi posiadać przyszły pracownik do zajmowania danego stanowiska.*

(akta kontroli str. 24-30)

Z 28 osób pracujących w Urzędzie na stanowisku pracy z komputerem 6 grudnia 2023 r. 25 pracowników zostało poddanych testowi wiedzy z zakresu cyberbezpieczeństwa. Test obejmował zagadnienia dotyczące: zabezpieczania osobistych urządzeń, rozpoznawania i reagowania na cyberzagrożenia, zabezpieczenia sieci, świadomości dotyczącej ochrony prywatności i danych, postępowania w przypadku incydentów cyberbezpieczeństwa. Średnio pracownicy rozwiązali test na 57,5%, z czego najniższy wynik wyniósł 40%, a najwyższy 76,7%. W wyniku szczegółowej analizy udzielonych odpowiedzi ustalono, iż na 11 pytań (36,7% zadanych) mniej niż połowa testowanych udzieliła poprawnych odpowiedzi.
Wśród pytań, na które udzielono najmniej poprawnych odpowiedzi znalazły się m.in. pytania dotyczące:

- identyfikacji, czy konto w serwisie internetowym zostało przejęte przez cyberprzestępcę – pięć osób odpowiedziało poprawnie;
- tworzenia bezpiecznego hasła – sześć osób odpowiedziało poprawnie;
- identyfikacji, czy na komputerze znajduje się wirus – sześć osób odpowiedziało poprawnie;
- poprawnej reakcji na zidentyfikowanego wirusa na komputerze – nikt nie odpowiedział poprawnie.

(akta kontroli str. 389-390, 392-393)

2.5. Oględziny[45] pięciu stanowisk do pracy z komputerem w budynku Urzędu w zakresie stosowania przez pracowników zasad minimalizujących ryzyko nieuprawnionego dostępu do systemów informatycznych Urzędu wykazały, że pracownicy takie zasady stosowali poprzez m.in.: niezamieszczanie danych do logowania w widocznym miejscu w pokoju, w którym znajdowało się stanowisko pracy, stosowanie haseł zgodnie z wewnętrznymi procedurami, tj. o odpowiedniej długości, niepowtarzalności i złożoności oraz ich zmianie po 30 dniach (co było wymuszane przez serwer domenowy). Wszyscy pracownicy potrafili zablokować swój komputer.

(akta kontroli str. 403-404)

2.6. W Urzędzie nie funkcjonował dział informatyczny. Obsługę informatyczną zapewniała firma zewnętrzna, świadcząca usługi na podstawie zawieranej co roku umowy zlecenia. Przedmiotem umowy było wykonywanie usług informatycznych polegających na wsparciu serwisowym w zakresie: serwisu sprzętu komputerowego Urzędu; użytkowników w zakresie instalacji i konfiguracji i obsługi programów znajdujących się w posiadaniu Urzędu; administrowania siecią teleinformatyczną; konfiguracji i obsługi poczty elektronicznej; konsultingu IT dotyczącego zakupów i rozwoju infrastruktury informatycznej i usług IT oraz innych prac informatycznych zlecanych przez Urząd.
Ponadto osobami odpowiedzialnymi za zapewnienie bezpieczeństwa teleinformatycznego w Urzędzie były trzy osoby: inspektor bezpieczeństwa teleinformatycznego, administrator systemu teleinformatycznego i inspektor ochrony danych[46]. Dwie z nich zostały przeszkolone w zakresie cyberbezpieczeństwa.

[45] Przeprowadzone 14 listopada 2023 r.
[46] Powołani Zarządzeniami Wójta Gminy Stare Czarnowo: nr 39.2023 z dnia 30 maja 2023 r., 99.2019 z dnia 31 grudnia 2019 r. i nr 50.2022 z dnia 23 czerwca 2022 r.

W Urzędzie nie istniały wykazy umiejętności, jakie powinny posiadać pracownicy, którym przypisano zadania z zakresu bezpieczeństwa informacji. W sprawie sposobu przeprowadzenia wyboru ww. pracowników w zakresie potrzebnych wymagań oraz posiadanych przez nich niezbędnych kompetencji do objęcia tych funkcji Zastępca Wójta wyjaśnił: *Do pełnienia funkcji z zakresu bezpieczeństwa informacji w Urzędzie wybrano osoby, które ze względu na swoje kwalifikacje i doświadczenie zawodowe wyróżniały się znajomością procedur administracyjnych i funkcjonowania naszej jednostki. Osoby te w sposób szczególny wykazywały rzetelne podejście do wykonywania swoich obowiązków służbowych i wykazywały wysoki poziom etyki zawodowej. Wobec powyższego były one kierowane przez pracodawcę do odbycia różnych szkoleń i kursów celem poszerzenia ich wiedzy i trenowania odpowiednich umiejętności. W ocenie Administratora Danych Osobowych przy przydzielaniu istotnych funkcji poszczególnym pracownikom posiadali oni niezbędne kompetencje, czego potwierdzeniem są wystawione odpowiednie dokumenty załączone do akt osobowych każdego z pracowników.*
W Urzędzie nie określono planu szkoleń dla ww. pracowników. Zastępca Wójta wyjaśnił, że poszczególni pracownicy pogłębiają swoją wiedzę w formie samokształcenia kierowanego z wykorzystaniem technologii internetowych, w zależności od potrzeb i zmieniających się przepisów. Ponadto wskazał, że Urząd nie planował zatrudnienia pracownika na stanowisko informatyka.

(akta kontroli str. 24-30, 355-379, 405-407, 408-423)

2.7. W sprawie dokonywanych przez Urząd analiz potrzeb z zakresu cyberbezpieczeństwa Wójt wyjaśniła, że: *w Urzędzie dokonywano analizy (…), jednak nie posiadamy w tym zakresie dokumentacji, ponieważ potrzeby z zakresu cyberbezpieczeństwa konsultowano na koniec każdego roku z firmą zewnętrzną, świadczącą usługę informatyczną na rzecz Urzędu (…).*

(akta kontroli str. 6-12)

W poszczególnych latach objętych kontrolą wydatki na zadania z zakresu cyberbezpieczeństwa łącznie wyniosły 85 877,38 zł, tj.:
- w 2019 r.: 17 373,17 zł (w tym: wymiana sprzętu informatycznego 12 384,29 zł oraz oprogramowanie 4 988,88 zł),
- w 2020 r.: 22 306,54 zł (w tym: wymiana sprzętu informatycznego 15 985,94 zł, oprogramowanie 4 709,3 zł oraz zapewnienie bezpieczeństwa fizycznego 1 611,3 zł),
- w 2021 r.: 25 449,36 zł (w tym: wymiana sprzętu informatycznego 15 398,29 zł, oprogramowanie 6 730,07 zł oraz zapewnienie bezpieczeństwa fizycznego 3 321 zł),
- w 2022 r.: 4 008,91 zł wymiana sprzętu informatycznego,
- w 2023 r. (do 22 listopada): 16 739,4 zł (w tym: wymiana sprzętu informatycznego 13 530 zł, oprogramowanie 2 435,4 zł oraz szkolenia pracowników 774 zł).

W 2022 r. Urząd skorzystał z zewnętrznych źródeł finansowania cyberbezpieczeństwa w kwocie 100 tys. zł na realizację projektu dofinansowanego w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020, z którego zakupiono m.in. UTM do serwerowni.

(akta kontroli str. 29-30)

2.8. Oględziny[47] pięciu stanowisk pracy z komputerem w zakresie używanego oprogramowania antywirusowego oraz innego zainstalowanego oprogramowania (w tym poprawek systemu Windows) wykazały, że w Urzędzie wykorzystywano aplikację antywirusową z ważną asystą do grudnia 2024 r. oraz urządzenie odseparowujące sieć wewnętrzną Urzędu od sieci zewnętrznej Internet, posiadające asystę ważną do maja 2025 r.

[47] Przeprowadzone 23 listopada 2023 r.

Adekwatność posiadanego przez Urząd oprogramowania zabezpieczającego do zidentyfikowanych rodzajów ryzyka potwierdził biegły[48] oraz pozytywnie ocenił stosowane przez Urząd wielowarstwowe zabezpieczenia / rozwiązania w zakresie różnego rodzaju zagrożeń. Biegły nie wnosił zastrzeżeń do stosowanego przez Urząd oprogramowania zabezpieczającego. W ocenie biegłego warto uzupełnić stosowane przez Urząd zabezpieczenia w zakresie systemu DLP, którego celem byłoby zapobieganie niekontrolowanemu wyciekowi informacji z Urzędu, np. poprzez zablokowanie możliwości podłączenia pamięci przenośnych lub zgrywania na nie danych, monitorowania przesyłu danych np. na skrzynki prywatne.

(akta kontroli str. 424-443, 463-480)

2.9. Urząd posiadał wykaz sprzętu i oprogramowania oraz zestawienie „wartości niematerialne i prawne - programy komputerowe i licencje Urzędu Gminy Stare Czarnowo". Ponadto okresowo (raz w roku) był przeprowadzany wewnętrzny audyt sprzętu i oprogramowania, mający na celu wyeliminowania sprzętu przestarzałego technologicznie i oprogramowania. W odniesieniu do oprogramowania audyt ograniczał się głównie do zainstalowanego systemu operacyjnego i Office. Wykaz oprogramowania prowadzony przez Urząd nie był kompletny, nie zawierał wszystkich aplikacji zainstalowanych na stacjach końcowych. W zestawieniu dotyczącym posiadanych licencji nie było pozycji dotyczącej oprogramowania ochrony antywirusowej ESET.

W ocenie biegłego w kontekście zarządzania środowiskiem informatycznym Urzędu, istotne jest podkreślenie znaczenia zarządzania podatnościami i aktualizacjami na wszystkich urządzeniach. Chociaż roczne audyty sprzętu i oprogramowania są - zdaniem biegłego - działaniem pozytywnym, niezbędne jest rozszerzenie zakresu tych przeglądów o dokładną analizę używanych wersji aplikacji. Weryfikacja legalności licencji oraz aktualności wersji aplikacji jest kluczowa do identyfikacji i eliminacji oprogramowania z przestarzałymi lub nieaktualnymi wersjami, które mogą posiadać znane podatności. Dodatkowo w ocenie biegłego, brak dedykowanych narzędzi i szczegółowych procedur do zarządzania podatnościami i poprawkami (PBDO ograniczała się tylko do określenia w tym zakresie obowiązku ASI przeprowadzania regularnych aktualizacji oprogramowania na wszystkich stacjach roboczych - laptopach, zgodnie z zaleceniami producentów oprogramowania) stanowi istotne ryzyko, które wymaga uwagi w celu wzmocnienia bezpieczeństwa informatycznego Urzędu. Szerzej o tym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 17, 450-456, 463-480)

W sprawie posiadanej przez Urząd wiedzy na temat funkcjonujących w Urzędzie urządzeń informatycznych podłączonych do sieci komputerowej oraz przypadków funkcjonowania w sieci Urzędu niezidentyfikowanych urządzeń Zastępca Wójta wyjaśnił: *Urządzenie UTM jest tak skonfigurowane, że nie „wpuszcza / dopuszcza" urządzeń z poza białej listy do sieci komputerowej urzędu – tylko znane urządzenia będą miały dostęp do Internetu i zasobów. Nie występowały przypadki funkcjonowania w sieci Urzędu niezidentyfikowanych urządzeń.*

(akta kontroli str. 24-30)

W Urzędzie nie były przeprowadzane testy penetracyjne, które mogły wskazywać na wykorzystywane oprogramowanie zabezpieczające, jego skuteczność oraz wszelkie identyfikowane luki.

(akta kontroli str. 35-37)

2.10. W okresie objętym kontrolą Urząd nie korzystał z usług chmurowych. W sprawie korzystania przez Urząd z prowadzonego przez Ministerstwo Cyfryzacji Systemu

[48] W oparciu o sprawozdanie z przeprowadzonych analiz w obszarze bezpieczeństwa teleinformatycznego biegłego powołanego w trakcie kontroli NIK.

Zapewniania Usług Chmurowych Wójt wyjaśniła, że Urząd nie korzystał z takich systemów.

(akta kontroli str. 6-12, 463-480)

2.11. Oględziny[49] pięciu stanowisk do pracy z komputerem w budynku Urzędu w zakresie korzystania przez pracowników Urzędu na komputerach służbowych z prywatnych skrzynek mailowych, w tym do celów służbowych wykazały, że każdorazowo w pismach kierowanych do petentów pracownicy wskazywali przypisane im służbowe skrzynki pocztowe; ponadto istniała możliwość wejścia z komputera służbowego na stronę operatora webmail np. Gmail.com.pl., poczta.wp.pl. Kierownik Referatu Organizacyjnego, Spraw Obywatelskich, Promocji i Oświaty[50] wyjaśnił, że: *strony te nie są blokowane, gdyż nieraz pracownicy Urzędu zakładają skrzynki pocztowe interesantom (np. w programie Czyste Powietrze), co jest niezbędne do przystąpienia do programu.* Wójt wyjaśniła: *Pracownicy urzędu zakładali 6-krotnie skrzynki pocztowe interesantom, składającym wnioski w ramach programu Czyste Powietrze. Wszystkie przypadki miały miejsce na jednym komputerze i nie zastosowano w tym przypadku dodatkowych mechanizmów zabezpieczeń, bo nie było to konieczne.*

(akta kontroli str. 457-458, 481, 500-501)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Urząd nie przeprowadził analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej, co było działaniem nierzetelnym. Ponadto było to niezgodne z § 20 ust. 2 pkt 3 KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. działań przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

(akta kontroli str. 8-12)

Wójt wyjaśniła: *Analizę ryzyka planowaliśmy przeprowadzić w 2020 r., jednak w związku z pandemią COVID-19 było to niemożliwe. W 2022 r. zaktualizowano PBDO wraz z Instrukcją zarządzania systemem informatycznym. Na tej podstawie obecnie przeprowadzana jest analiza ryzyka.*

(akta kontroli str. 45-46)

2. W Urzędzie nie przeszkolono wszystkich pracowników z zakresu cyberbezpieczeństwa, z 28 pracowników pracujących przy komputerze tylko trzech odbyło takie szkolenia. Było to niezgodne z § 20 ust. 2 pkt 6 KRI, który stanowi, że: zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. działań: zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna oraz stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

(akta kontroli str. 24-30, 394-402)

Wójt wyjaśniła: *W Urzędzie (…) zaplanowaliśmy szkolenie pracowników w dwóch etapach. W pierwszym etapie, przeszkolone zostały osoby zajmujące się na co dzień*

[49] Przeprowadzone 14 listopada 2023 r.
[50] Pełniący też funkcję administratora systemów teleinformatycznych.

zagadnieniami z zakresu bezpieczeństwa teleinformatycznego i przeciwdziałania cyberzagrożeniom w aspekcie ochrony infrastruktury krytycznej. W drugim etapie przeszkoleni zostaną pozostali pracownicy Urzędu (...) z zakresu zarządzania bezpieczeństwem informacji. Szkolenie takie planowaliśmy w 2023 r. jednak w związku z naborem w programie Centrum Projektów Polska Cyfrowa-Cyberbezpieczny Samorząd, w ramach którego można przeprowadzić szkolenia z zakresu zarządzania bezpieczeństwem informacji, szkolenie przesunęliśmy na 2024r.

(akta kontroli str. 45-46)

3. W Urzędzie nie zapewniono aktualności inwentaryzacji całego zasobu informatycznego, tj. w zakresie wszystkich zainstalowanych aplikacji, co było niezgodnie z § 20 ust. 2 pkt 2 KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Także zgodnie z normą PN-ISO/IEC 27002:2014-12, pkt 8.1.1, wszystkie aktywa powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany spis wszystkich aktywów informatycznych.
W ocenie NIK brak inwentaryzacji wszystkich zainstalowanych aplikacji może prowadzić do braku ich aktualizacji, możliwości wychwycenia incydentów oraz reakcji w przypadku ich wystąpienia (np. nielegalne lub podatne na atak oprogramowanie). Brak skutecznie wdrożonego procesu zarządzania podatnościami i poprawkami naraża Urząd na konsekwencje związane z wykorzystaniem przez atakujących i złośliwe oprogramowanie istniejących w systemach podatności, co może w dalszej konsekwencji prowadzić do incydentów bezpieczeństwa.
Ponadto posiadane przez Urząd zestawienie „wartości niematerialne i prawne - programy komputerowe i licencje urzędu gminy Stare Czarnowo" należy uznać za element ewidencji księgowej. Inwentaryzacja prowadzona na podstawie przepisów ustawy z dnia 29 września 1994 r. o rachunkowości[51] nie jest tożsama z inwentaryzacją wskazaną w KRI, która rozumiana jest jako stałe posiadanie aktualnych informacji w zakresie nie tylko posiadanego sprzętu informatycznego i oprogramowania, ale również jego konfiguracji.

(akta kontroli str. 17, 450-456, 459-460, 463-480)

Wójt wyjaśniła: *Jesteśmy małym Urzędem, z małym budżetem. Staramy się na bieżąco aktualizować posiadany zasób informatyczny. Nie posiadamy jednego dokumentu, w którym zapisane jest, jakie aplikacje zainstalowane są na poszczególnych komputerach. Jednak mamy wiedzę, jakie programy są zainstalowane na komputerach, w tym kto ma uprawnienia do danego programu. W przekazanym zestawieniu dotyczącym środków trwałych, są umieszczone wyłącznie programy, do których mamy licencje wyłącznie dożywotnie. Program typu ESET, są programami, na które wykupujemy licencje na dany okres, np. roku. Dlatego nie pojawił się w zestawieniu. ESET zainstalowany jest na wszystkich jednostkach roboczych. Informatycy z firmy zewnętrznej regularnie monitorują całą sieć urzędu, w tym sprawdzają czy aplikacje są aktualne lub czy występują incydenty.*

(akta kontroli str. 496-497)

OCENA CZĄSTKOWA

Urząd nie przeprowadził analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej, co było działaniem nierzetelnym oraz niezgodnym z § 20 ust. 2 pkt 3 KRI. Jednocześnie za pozytywne należy uznać umiejscowienie głównych elementów infrastruktury (serwerowni) w lokalizacji

[51] Dz.U. z 2023 r. poz. 120.

minimalizującej zagrożenia związane z powodzią lub podtopieniami. W Urzędzie zabezpieczono się przed zagrożeniami związanymi z elektrycznością w postaci bateryjnych urządzeń podtrzymujących napięcie (UPS). Posiadane przez Urząd oprogramowanie zabezpieczające było adekwatne do zidentyfikowanych rodzajów ryzyka. W Urzędzie nie przeszkolono wszystkich pracowników z zakresu cyberbezpieczeństwa oraz nie zapewniono aktualności inwentaryzacji całego zasobu informatycznego.

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Zapewnienie zgodności obowiązującego SZBI z normą PN-ISO/IEC 27001 i KRI.
2. Zapewnienie przeprowadzania okresowych przeglądów SZBI.
3. Zapewnienie przeprowadzania audytów z zakresu bezpieczeństwa informacji.
4. Zapewnienie braku konfliktu interesów audytora przeprowadzającego audyt systemu zarządzania bezpieczeństwem informacji.
5. Zapewnienie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
6. Zapewnienie każdorazowego wyznaczania osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
7. Opracowanie i wdrożenie procedury zarządzania incydentami związanymi z bezpieczeństwem informacji.
8. Przeprowadzenie klasyfikacji krytyczności procesów i zasobów informatycznych Urzędu.
9. Opracowanie, wdrożenie i przestrzeganie planu odtworzenia utraconych zasobów zapewniającego ciągłość działania.
10. Zapewnienie weryfikacji kopii zapasowych Urzędu wykonywanych przez podmioty zewnętrzne.
11. Przeprowadzenie analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej Urzędu.
12. Przeszkolenie wszystkich pracowników Urzędu z zakresu cyberbezpieczeństwa.
13. Zapewnienie aktualności inwentaryzacji całego zasobu informatycznego Urzędu.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Szczecinie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 30 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Szczecin, 11 stycznia 2024 r.

Delegatura w Szczecinie
Dyrektor
Marcin Stefaniak

Kontroler

Najwyższa Izba Kontroli

Tomasz Cyranka
Główny specjalista
kontroli państwowej

.....
podpis

.....
Podpis

Marta Górska-Jaś
Główny specjalista
kontroli państwowej

.....
Podpis

Wystąpienie pokontrolne podpisane elektronicznie