NAJWYŻSZA IZBA KONTROLI

Delegatura w Szczecinie

LSZ.411.3.4.2023

Danuta Ankutowicz
Wójt Gminy Marianowo

Urząd Gminy Marianowo
ul. Mieszka I 1
73-121 Marianowo

WYSTĄPIENIE POKONTROLNE

Zmienione zgodnie z treścią uchwały nr KPK-KPO.441.35.2024 Komisji Rozstrzygającej z dnia 8 marca 2024 r.

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 Marianowo[1], ul. Mieszka I 1, 73-121 Marianowo.
Kierownik jednostki kontrolowanej	Danuta Ankutowicz, Wójt Gminy Marianowo[2], od 23 listopada 2018 r.
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.
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[5] Delegatura w Szczecinie
Kontroler	Izabela Kirysiuk, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/165/2023 z 18 października 2023 r. (akta kontroli str.1-2)

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

II. Ocena ogólna[6] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli negatywnie ocenia działalność jednostki w badanym zakresie.

Uzasadnienie oceny ogólnej

Negatywną ocenę uzasadniają nieprawidłowości w obszarze dotyczącym wdrożenia i przestrzegania polityki z zakresu bezpieczeństwa teleinformatycznego.

W szczególności Urząd nie dokonywał okresowych analiz ryzyka w latach 2019-2021 i 2023 (do dnia przeprowadzenia czynności kontrolnych) i corocznych audytów bezpieczeństwa informacji w latach 2019-2020 i 2023 (do dnia przeprowadzenia czynności kontrolnych). Urząd zlecał zadania z zakresu przeprowadzania audytu i polityki bezpieczeństwa informacji Inspektorowi Ochrony Danych Osobowych, co powodowało konflikt interesów. W okresie od 28 sierpnia 2018 r. do 10 lipca 2022 r. w Urzędzie nie było wyznaczonej 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[7]. Urząd nie zgłaszał incydentów do CSIRT NASK[8] lub nie ujmował zgłoszonych incydentów w Rejestrze incydentów bezpieczeństwa informacji. Urząd nie posiadał również przygotowanych procedur pozwalających na zachowanie ciągłości działania i odtworzenie utraconych zasobów, w szczególności nie sklasyfikowano istniejących w Urzędzie procesów i zasobów informatycznych, w wyniku czego nie opracowano planu odtworzenia utraconych zasobów.

Powyższą ocenę uzasadnia również negatywne ocenienie obszaru dotyczącego przygotowania organizacyjno – kadrowego Urzędu do zapewnienia bezpieczeństwa teleinformatycznego.

W szczególności nie zapewniono pracownikom Urzędu szkoleń z zakresu bezpieczeństwa teleinformatycznego, nie zapewniono długości haseł do systemu stosowanych przez pracowników zgodnej z obowiązującym w Urzędzie systemem zarządzania bezpieczeństwem informacji, nie wpisano do umów o świadczenie usług informatycznych obowiązków wynikających z systemu zarządzania bezpieczeństwem informacji, wykorzystywano aplikacje w nieaktualnych wersjach, nie opracowano procedur i nie monitorowano wykorzystywania usług chmurowych, nie wyłączono możliwości korzystania przez pracowników Urzędu z prywatnych skrzynek pocztowych na komputerach służbowych.

[6] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[7] Dz. U. z 2023 r. poz. 913, dalej: KSC.

[8] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (art. 2 pkt 3 KSC).

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1. W Urzędzie został opracowany i wdrożony[10] system zarządzania bezpieczeństwem informacji[11] na podstawie Zarządzenia Wójta nr 14/2019 z dnia 29 stycznia 2019 r.

W wyniku analizy zapisów SZBI (wersje 1.0 i 2.0) ustalono, że w badanym zakresie[12] Polityka Bezpieczeństwa Informacji[13] była zgodna z wymogami normy PN-EN ISO/IEC 27001[14].

(akta kontroli str. 136-137, 250-415)

Urząd przeprowadził przegląd i zaktualizował SZBI do wersji 2.0 26 października 2023 r., ale do dnia zakończenia czynności kontrolnych nie zostało zmienione Zarządzenie Wójta nr 14/2019 z dnia 29 stycznia 2019 r. wprowadzające SZBI w wersji 1.0.

(akta kontroli str. 136-137, 250-251, 324-414)

Procedura zarządzania incydentami nie zawierała obowiązku każdorazowego wyciągania wniosków z obsłużonego incydentu w celu zaplanowania działań zapobiegawczych (Rozdział 14 Załącznika nr 6 do Polityki Bezpieczeństwa Informacji wersji 2.0). Ponadto tytuł tego rozdziału brzmiał *Obowiązek zachowania poufności i ochrony danych osobowych*. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 403-406)

2. W kontrolowanym okresie w Urzędzie została przeprowadzona jedna analiza ryzyka utraty integralności, dostępności informacji, poufności informacji, czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy[15]. W wyniku przeprowadzonej analizy, Zespół do spraw SZBI zarekomendował podjęcie zabezpieczeń obniżających ryzyko: zaplanowanie przeprowadzenia testów penetracyjnych, zakup i wdrożenie firewall z UTM, wdrożenie bezpłatnego rozwiązania systemu IDS, blokowanie kont po pięciu próbach błędnego wpisania hasła, szyfrowanie nośników danych komputerów przenośnych

[9] 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.

[10] Zarządzenie nr 14/2019 Wójta Gminy Marianowo z dnia 29 stycznia 2019 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Marianowo ustanawiające Politykę Bezpieczeństwa Informacji w Urzędzie Gminy Marianowo wersja 1.0; 26 października 2023 r. została zatwierdzona przez Zastępcę Wójta Gminy Marianowo wersja 2.0.

[11] Dalej: SZBI, Polityka Bezpieczeństwa Informacji.

[12] Tj. badanie ustanowienia w SZBI uregulowań dotyczących: zarządzania i nadzoru nad SZBI, zakresu SZBI, opublikowania i zakomunikowania SZBI, szacowania ryzyka, środków zapewnienia bezpieczeństwa informacji, wyznaczenia osób odpowiedzialnych za przegląd polityki bezpieczeństwa informacji, uprawnień i odpowiedzialności użytkowników, kontroli dostępu do systemu i aplikacji, zasad kształcenia i szkolenia z bezpieczeństwa informacji, zasad klasyfikacji przetwarzanych informacji, zasad przeglądu i analizy ryzyka SZBI, zasad zgłaszania lub podejrzenia wystąpienia i obsługi incydentów bezpieczeństwa informacji.

[13] Badanie przeprowadzono za pomocą kwestionariusza zawierającego 16 pytań dotyczących obszarów i zagadnień uregulowanych w SZBI obowiązującym w Urzędzie.

[14] Dalej: PN-ISO/IEC 27001.

[15] Raport z przeprowadzonej analizy ryzyka w Urzędzie Gminy w Marianowie w okresie od października do listopada 2022 r., opracowany przez Zespół do spraw SZBI, powołany na podstawie § 2 ust. 2 Zarządzenia nr 14/2019 Wójta Gminy Marianowo z dnia 29 stycznia 2019 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Marianowo. W skład Zespołu do spraw SZBI wchodzili: Sekretarz, Informatyk/Administrator Systemu Informatycznego, Podinspektor ds. obronnych, obrony cywilnej i zarządzania kryzysowego oraz zarządzania bezpieczeństwem, Inspektor ochrony danych.

oraz stacjonarnych ulokowanych na parterze budynku, wyłączenie portów USB, uruchomienie procesu separacji sieci oraz wyłączenie nieużywanych gniazd LAN, regularne aktualizacje oprogramowania i firmware. Do raportu z przeprowadzonej analizy ryzyka załączono arkusz analizy ryzyka, zawierający charakterystykę aktywów, rodzajów zagrożenia, podatności na zagrożenia, prawdopodobieństwa, następstw i ryzyk, rodzajów ryzyka, postępowania z ryzykiem, zabezpieczenia obniżającego ryzyko oraz statusu[16].

(akta kontroli str. 416-432)

W toku kontroli Zastępca Wójta przedstawił zestawienie kolejnych ryzyk zredukowanych do 15 listopada 2023 r.: błąd/awaria oprogramowania, błędy projektowe/konfiguracyjne, keylogger i ransomware (złośliwe oprogramowanie), wirusy, trojany, phishing, podrzucanie nośników danych, zagubienie nośnika lub dokumentów, włamania z wykorzystaniem podatności sprzętu, poprzez wykonanie następujących działań: wdrożono nowy system do tworzenia kopii zapasowych oraz oprogramowanie AV, UTM w ramach projektu „Cyfrowa Gmina", zastosowano minimalizację uprawnień, przeprowadzono szkolenie pracowników, wdrożono nową wersję SZBI, zapoznano pracowników z nową wersją SZBI.

(akta kontroli str. 445-446)

Zastępca Wójta wyjaśnił, że *Po przeprowadzeniu analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie Gminy Marianowo nie zostały wprowadzone nowe systemy informatyczne, w których byłyby przetwarzane dane, z uwagi na ograniczone środki finansowe. Urząd Gminy Marianowo rozważa możliwość pozyskania nowych systemów informatycznych w ramach konkursu grantowego „Cyberbezpieczny Samorząd", którego nabór został wyznaczony do dnia 14 grudnia 2023 r.*

(akta kontroli str. 615)

W kontrolowanym okresie w Urzędzie przeprowadzono dwa audyty bezpieczeństwa informacji (w grudniu 2021 r. i w lipcu 2022 r.)[17]. Audytor ustalił, że Urząd: nie przedstawił rejestru zasobów teleinformatycznych i aktualnej dokumentacji odtworzeniowej środowiska, nie dokonywał okresowej analizy ryzyka, nie przeprowadzał szkoleń dla pracowników z bezpieczeństwa informacji, nie wdrożył usługi monitorowania sieci (brak urządzenia UTM), nie posiadał protokołów potwierdzających próbę odtworzenia danych z kopii zapasowych, nie posiadał wpisów w rejestrze incydentów bezpieczeństwa informacji, nie przeprowadzał audytów bezpieczeństwa informacji w okresach rocznych. Audytor stwierdził, że *W audytowanym podmiocie brak podejścia systemowego do zarządzania bezpieczeństwa informacji, wszelkie zmiany w dokumentacji wynikają ze zmian w przepisach prawa, wprowadzane zmiany nie są konsekwencją wyników analizy ryzyka, wniosków z przeglądów SZBI, zaleceń z audytu lub wniosków z analizy incydentów naruszenia bezpieczeństwa informacji*. Przeprowadzone audyty

[16] Arkusz analizy ryzyka zawierał 451 pozycji, spośród których dokonano identyfikacji 344 nieakceptowalnych ryzyk, 80 warunkowych ryzyk, 19 akceptowalnych ryzyk i 8 krytycznych ryzyk. Ryzyka krytyczne dotyczyły: zagrożenia złośliwym oprogramowaniem ransomware w odniesieniu do komputerów przenośnych, stacjonarnych, serwera, dysków sieciowych, dysków przenośnych, dysków pendrive i kart SD, zagrożenia zagubieniem nośników lub dokumentów na dyskach przenośnych, dyskach pendrive i na kartach SD, zagrożenia wygaśnięciem licencji dla oprogramowania antywirusowego, zagrożenia nieprzestrzeganiem procedur przez pracowników. Status zastosowanych zabezpieczeń w celu redukcji ryzyka kształtował się następująco: 292 zabezpieczeń wdrożono, 134 zabezpieczeń opisano jako „do zaplanowania", 6 zabezpieczeń było w trakcie wdrożenia.

[17] Raporty z audytu bezpieczeństwa informacji w Urzędzie Gminy Marianowo z 20 grudnia 2021 r. i z 25 lipca 2022 r.

nie wykazały niezgodności zapisów SZBI z normą PN-ISO/IEC 27001, wnioski audytora dotyczyły nieprawidłowości w funkcjonowaniu SZBI w Urzędzie.

W lipcu 2022 r. w Urzędzie została przeprowadzona również diagnoza cyberbezpieczeństwa w ramach realizacji projektu grantowego „Cyfrowa Gmina”[18], której wyniki były zbieżne z ustaleniami przeprowadzonych audytów bezpieczeństwa informacji.

Przeprowadzenie w kontrolowanym okresie tylko jednej analizy ryzyka i dwóch audytów bezpieczeństwa informacji było niezgodne z § 20 ust. 2 pkt 3 i pkt 14 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[19], co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 416-432, 448-477, 530-556)

Powyższe audyty i diagnoza zostały przeprowadzone przez osobę, która pełniła jednocześnie funkcję Inspektora Ochrony Danych Osobowych w Urzędzie[20]. Osoba ta wykonała ww. audyty i diagnozę jako Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001. Szczegółowo zostało to opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 138-169, 448-491, 520-557)

3. Od 28 sierpnia 2018 r. do 10 lipca 2022 r. w Urzędzie nie wyznaczono osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Osoba ta została wyznaczona przez Wójta 11 lipca 2022 r. [21]. Funkcję tę pełnił Sekretarz Gminy Marianowo[22]. Dane wyznaczonej osoby zostały przekazane do CSIRT NASK 14 lipca 2022 r.[23] z zachowaniem terminu 14 dni[24]. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 433-436)

4. W Urzędzie prowadzono *Rejestr incydentów bezpieczeństwa informacji (prowadzony na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa)*. Rejestr ten nie zawierał żadnych wpisów.

(akta kontroli str. 589-593)

Zastępca Wójta wyjaśnił, że *W latach 2019 – 2023 Urząd Gminy Marianowo nie dokonywał zgłoszeń incydentów krytycznych do CSIRT NASK, ponieważ nie wystąpiła taka konieczność. Na okoliczność ewentualnej potrzeby dokonania takiego zgłoszenia przygotowany jest formularz „Rejestru incydentów”, który z uwagi na brak incydentów nie zawiera w chwili obecnej wpisów.*

(akta kontroli str. 447)

W toku kontroli ujawniono, że Zastępca Wójta dokonywał zgłoszeń przypadków phisingu do CSIRT NASK. Zgłoszenia były dokonywane przez dedykowaną stronę

---

[18] Raport z przeprowadzonej diagnozy cyberbezpieczeństwa w Urzędzie Gminy Marianowo w ramach realizacji projektu grantowego „Cyfrowa Gmina” z 25 lipca 2022 r.

[19] Dz. U. z 2017 r. poz. 2247 t.j., dalej: KRI.

[20] Pięć umów o świadczenie usług związanych z realizacją zadań ochrony danych osobowych oraz zadań przypisanych inspektorowi ochrony danych zawarte z D.S.: nr OC/13/2019 z 03.01.2019 r., nr OC/9/2020 z 02.01.2020 r., nr OC/4/2021 z 04.01.2021 r., nr OC/1/2022 z 04.01.2022 r., nr OC/1/2023 z 02.01.2023 r. wraz z pięcioma umowami powierzenia przetwarzania danych osobowych stanowiącymi uzupełnienie powyższych umów: nr OC/14/2019 z 03.01.2019 r., nr OC/10/2020 z 02.01.2020 r., nr OC/5/2021 z 04.01.2021 r., nr OC/2/2022 z 04.01.2022 r., nr OC/2/2023 z 02.01.2023 r.

[21] Zarządzenie nr 97/2022 Wójta Gminy Marianowo z dnia 11 lipca 2022 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

[22] Dalej: Sekretarz.

[23] Zgłoszenie zarejestrowane pod nr 1741386.

[24] Art. 22 ust. 1 pkt 5 KSC.

https://incydent.cert.pl, po czym potwierdzenie takiego zgłoszenia Sekretarz otrzymywał na skrzynkę mailową. W toku kontroli Urząd przedłożył potwierdzenie przyjęcia jednego zgłoszenia z 17 sierpnia 2023 r. podejrzanej wiadomości e-mail, zawierającej odnośnik do rzekomej aktualizacji serwera poczty elektronicznej. Potwierdzenia innych zgłoszeń nie zostały przedłożone. Powyższy stan został opisany w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 904-908, 988-992, 1054-1057)

Na stronie Urzędu[25] nie było udostępnionej informacji o cyberbezpieczeństwie[26]. Informacja taka pojawiła się na stronie Urzędu pod zakładką „Dla mieszkańca – Cyberbezpieczeństwo"[27] po zadaniu pytania w tej kwestii w trakcie czynności kontrolnych NIK[28]. Umieszczono tam podstawowe informacje z zakresu cyberbezpieczeństwa wraz z odnośnikami do serwisów m.in.: *CSIRT, CERT Polska, Baza wiedzy w serwisie gov.pl, Przeglądy wybranych oszustw internetowych, OUCH!* Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 1055-1056, 1064-1076)

5. W Urzędzie nie opracowano planu zachowania ciągłości działania, zawierającego klasyfikację krytycznych danych i operacji wraz z określeniem dodatkowych zabezpieczeń oraz zbioru usług, systemów operacyjnych i danych wraz z określeniem ram czasowych niezbędnych do ich odtworzenia w przypadku awarii lub ich utraty. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 615)

6. W Urzędzie funkcjonował plan tworzenia kopii zapasowych. Wykonywano codziennie kopię zapasową automatyczną. Ponadto w każdy poniedziałek była tworzona kopia zapasowa ręczna z utworzonym skryptem na dysk zewnętrzny przenośny, odłączany od serwera po wykonaniu kopii. Podczas tworzenia kopii zapasowej na dysk zewnętrzny przenośny weryfikowane były zapisane pliki i oprogramowanie.

(akta kontroli str. 615-617)

7. Urząd nie przedłożył dokumentacji potwierdzającej weryfikację liczby, stanów plików i oprogramowania w ramach tworzenia kopii zapasowych. Umowy z dostawcą usług informatycznych nie zawierały regulacji dotyczących obowiązku zapewnienia przez usługodawcę ciągłości działania Urzędu, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 170-199, 617, 1034-1041)

8. Urząd nie przedłożył dokumentacji potwierdzającej przeprowadzanie testów planu odtwarzania zasobów, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 617, 1034-1041)

9. W kontrolowanym okresie Urząd posiadał ubezpieczenie mienia i odpowiedzialności cywilnej, w tym sprzętu elektronicznego stacjonarnego i przenośnego, oprogramowania, kosztów odtworzenia danych, nośników danych oraz zwiększonych kosztów działalności[29]. Sprzęt elektroniczny stacjonarny i przenośny był ubezpieczony na kwoty: 45 214,74 zł w 2019 r., 43 505,80 zł w 2020 r., 44 321,29 zł w 2021 r., 38 665,93 zł w 2022 r., 42 036,48 zł w 2023 r. (była to wartość odtworzeniowa sprzętu z ewidencji środków trwałych załączonej do polis

[25] https://marianowo.pl/.
[26] Sprawdzono kilkukrotnie w trakcie kontroli.
[27] https://marianowo.pl/cyberbezpieczenstwo.html.
[28] Tj. 19.12.2023 r.
[29] Poniesionych w celu uniknięcia lub skrócenia przerw w działalności, powstałych na skutek szkody w sprzęcie elektronicznym.

ubezpieczeniowych); nośniki danych były ubezpieczone na kwotę 2000,00 zł w latach 2019-2021 oraz na kwotę 3000,00 zł w latach 2022-2023; oprogramowanie oraz odtworzenie danych były ubezpieczone na kwotę 10 000,00 zł w 2019 r. i na kwotę 20 000,00 zł w latach 2020-2023; zwiększone koszty działalności zostały ubezpieczone do kwoty 10 000,00 zł w latach 2019-2021 i do kwoty 5000,00 zł w latach 2022-2023[30].

(akta kontroli str. 200-246, 248-249)

Stwierdzone nieprawidłowości

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

1. Brak ujęcia w Procedurze zarządzania incydentami w § 20 Załącznika nr 6 do Polityki Bezpieczeństwa Informacji wersji 2.0 obowiązku każdorazowego wyciągania wniosków z obsłużonego incydentu w celu zaplanowania działań zapobiegawczych, uwzględniającego analizę przyczyn i okoliczności incydentów oraz identyfikację słabych punktów w systemach i procedurach, co mogło spowodować ryzyko, że podobne incydenty będą się powtarzać. Ponadto błędnie zatytułowana ww. procedura stwarzała ryzyko, że pracownicy mogli nie być świadomi rzeczywistego zakresu procedur, co mogło prowadzić do nieporozumień i błędnej interpretacji regulacji, i w konsekwencji do niewłaściwego postępowania w sytuacjach incydentów bezpieczeństwa. Było to niezgodne z art. 22 ust. 1 pkt 1 KSC, który stanowi, że podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego zapewnia zarządzanie incydentem w podmiocie publicznym.

   (akta kontroli str. 403-406, 1080, 1086-1088)

   Zastępca Wójta wyjaśnił, że *Wyżej wymieniona procedura nie zawierała „obowiązku każdorazowego wyciągania wniosków z obsłużonego incydentu w celu zaplanowania działań zapobiegawczych", ponieważ taki obowiązek jest wpisany w § 2 ust. 1 pkt 2 Zarządzenia Nr 14/2019 Wójta Gminy Marianowo z dnia 29 stycznia 2019 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Marianowo, zgodnie z którym Zespół ds. SZBI w Urzędzie Gminy Marianowo dokonuje analizy incydentów naruszenia bezpieczeństwa informacji i określa działania korygujące. Niemniej jednak wyżej wymieniona procedura zostanie rozszerzona o sugestię Biegłego podczas następnej aktualizacji dokumentacji związanej z SZBI, która planowana jest na pierwszą połowę 2024 r. w związku z tym, że uległa zmianie norma PN-EN ISO/IEC 27001:2023-08.* Dodatkowo Zastępca Wójta wyjaśnił, że *W rozdziale 14 omyłkowo wpisano tytuł rozdziału „Obowiązek zachowania poufności i ochrony danych osobowych". Błąd jakiś czas temu został zauważony i skorygowany poprzez przekreślenie tytułu rozdziału i wpisanie prawidłowego o treści „Procedura Zarządzania Incydentami".*

   (akta kontroli str. 1056, 1061-1062, 1099-1106)

2. Niedokonywanie okresowych analiz ryzyka w latach 2019-2021 i 2023 (do dnia przeprowadzenia czynności kontrolnych) i corocznych audytów bezpieczeństwa informacji w latach 2019-2020 i 2023 (do dnia przeprowadzenia czynności kontrolnych), co było niezgodne z § 20 ust. 2 pkt 3 i pkt 14 KRI. Zgodnie

[30] Umowy ubezpieczenia zawarte z Towarzystwem Ubezpieczeń Wzajemnych na podstawie ogólnych warunków ubezpieczenia dla jednostek samorządu terytorialnego „Bezpieczna Gmina" przez Gminę Marianowo (ubezpieczenie obejmujące jednostki: Urząd Gminy Marianowo, Bibliotekę Publiczną w Marianowie, Gminny Ośrodek Pomocy Społecznej w Marianowie, Szkołę Podstawową w Marianowie): nr OG 32493291 zawarta na okres od 01.01.2019 do 31.12.2019 r., nr GB 32763588 zawarta na okres od 01.01.2020 do 31.12.2020 r., nr GB 32850131 zawarta na okres od 01.01.2021 do 31.12.2021 r., nr GB 32926105 zawarta na okres od 01.01.2022 do 31.12.2022 r., nr GB 32968177 zawarta na okres od 01.01.2023 do 31.12.2023 r.

z § 20 ust. 2 pkt 3 KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, oraz zgodnie z § 20 ust. 2 pkt 14 KRI, do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W badanym okresie została przeprowadzona tylko jedna analiza ryzyka (w 2022 r.) oraz dwa audyty (w 2021 i 2022 r.).

(akta kontroli str. 416-432, 448-477)

Zastępca Wójta wyjaśnił, że *Przeprowadzenie wyżej wymienionej liczby audytów i analiz ryzyka wynikała z faktu, iż od 20 marca 2020 r. do 15 maja 2022 r. obowiązywał w Polsce stan epidemii, ograniczający bardzo mocno funkcjonowanie urzędów w całym kraju. Ponadto we wspomnianym powyżej okresie miała miejsce długoterminowa nieobecność członka Zespołu ds. SZBI w Urzędzie Gminy Marianowo - podinspektora ds. obronnych, obrony cywilnej i zarządzania kryzysowego oraz zarządzania bezpieczeństwem. Zespół do spraw Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Marianowo w drugiej dekadzie grudnia 2023 r. przeprowadził analizę ryzyka w Urzędzie Gminy Marianowo, obecnie trwają prace nad ostateczną wersją raportu z przeprowadzonej analizy ryzyka, którego zakończenie planowane jest na drugą dekadę stycznia 2024 r.*

(akta kontroli str. 1099-1106)

3. Zlecenie wykonania audytów bezpieczeństwa informacji i diagnozy cyberbezpieczeństwa osobie, która pełniła w Urzędzie funkcję Inspektora Ochrony Danych Osobowych[31] w Urzędzie. 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 (Ogólne Rozporządzenie o Ochronie Danych)[32]. Zgodnie z tym przepisem, inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów. Osoba, która pełniła funkcję IODO, wykonała ww. audyty i diagnozę jako Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001.

   (akta kontroli str. 138-169, 448-491, 520-557)

   Zastępca Wójta wyjaśnił, że *W ocenie Wójta Gminy Marianowo nie ma przeszkód do sporządzania audytów wewnętrznych SZBI przez osobę pełniącą w Urzędzie Gminy Marianowo obowiązków IOD na podstawie umowy. Nadmienić należy, że posiada stosowne uprawnienia audytora wg normy ISO 27001, co uprawnia go do przeprowadzania takich audytów zgodnie z etyką zawodową. SZBI w Urzędzie Gminy Marianowo jest obszernym dokumentem nie skupiającym się wyłącznie na zagadnieniach związanych z samą ochroną danych osobowych.*

   W uzupełnieniu powyższych wyjaśnień, pełniący obowiązki IODO D. S. złożył pismo, w którym oświadczył, że w jego ocenie *nie ma przeciwskazań na łączenie*

[31] Dalej: IODO.
[32] Dz.Urz.UE.L nr 119, str. 1, dalej: RODO.

dwóch funkcji, tj. inspektora ochrony danych oraz audytora SZBI, ponieważ obie funkcje realizowane są w oparciu o inne przepisy, tj.:

- ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (…) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (…),

- rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (…).

Zależność (…) istniałaby wówczas, jakby audytor SZBI pełnił (realizował) obowiązki informatyka/administratora systemów informatycznych, ponieważ jak się szczegółowo przeanalizuje zakres audytu SZBI w dużej mierze dotyczy systemów informatycznych i podczas audytu doszłoby do sprawdzania „samego siebie", co mogłoby powodować, że audyt nie byłby obiektywny.

(akta kontroli str. 906, 1011)

Ponadto Urząd przedłożył dokument pn. Polityka zarządzania konfliktem interesów Inspektora Ochrony Danych w Urzędzie Gminy Marianowo wersja 1.0, zatwierdzona przez Wójta 18 grudnia 2023 r. (tj. po dniu zakończenia czynności kontrolnych), której celem zgodnie z § 1 ww. Polityki jest zapewnienie zarządzania konfliktem interesów Inspektora Ochrony Danych.

(akta kontroli str. 1058-1060)

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

(akta kontroli str. 138-169, 448-491, 520-557)

4. Niewyznaczenie od 28 sierpnia 2018 r. do 10 lipca 2022 r. w Urzędzie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z art. 21 ust. 1 KSC.

(akta kontroli str. 433-436)

Zastępca Wójta na pytanie, czy wcześniej niż w lipcu 2022 r. była wyznaczona i zgłoszona osoba kontaktowa do CSIRT NASK, wyjaśnił, że *Prawdopodobnie tak, po wejściu w życie ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, aczkolwiek nie posiadamy na tę okoliczność żadnego potwierdzenia w formie dokumentu, ponieważ zgłoszenia dokonywane są w formie elektronicznej i prawdopodobnie potwierdzenie nie zostało wydrukowane. Dlatego dla pewności dokonano ponownego zgłoszenia w dniu 14 lipca 2022 r. wraz z formalnym wyznaczeniem osoby kontaktowej w formie Zarządzenia Nr 97/2022 Wójta Gminy Marianowo z dnia 11 lipca 2022 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.*

(akta kontroli str. 1054)

5. Niezgłaszanie incydentów do CSIRT NASK i nieujmowanie zgłoszonych incydentów w prowadzonym przez Urząd Rejestrze incydentów bezpieczeństwa informacji, co stanowiło naruszenie art. 22 ust. 1 pkt 1-3 KSC i § 20 ust. 2 pkt 13 KRI. Rejestr ten nie zawierał żadnych zgłoszonych incydentów, natomiast w toku kontroli ujawniono, że Urząd zgłaszał incydenty do CSIRT NASK. Również wnioski zawarte w przeprowadzonych dwóch audytach bezpieczeństwa informacji wskazywały na nieprawidłowe funkcjonowanie procesu identyfikacji

i zgłaszania incydentów: *Rejestr nie zawiera wpisów dotyczących incydentów bezpieczeństwa, co świadczy, że proces raczej nie funkcjonuje w sposób prawidłowy.*

(akta kontroli str. 589-593, 447,461, 476, 904-908, 988-992, 1054-1057)

Ponadto, zgodnie z opinią biegłego, powtarzalność obserwacji w raportach z audytów bezpieczeństwa informacji może wskazywać na brak rozliczalności w zakresie wdrożenia niezbędnych działań naprawczych, co zwiększa ryzyko, że incydenty pozostają niewykryte i niezaraportowane, co może uniemożliwiać odpowiednią reakcję i zarządzanie nimi.

(akta kontroli str. 1079-1080, 1086-1088)

Zastępca Wójta wyjaśnił, że *(…) zgłoszenia incydentów do CSIRT NASK w okresie 2019-2023 dokonywane były w zakresie zgłoszeń podejrzanych wiadomości e-mail i dotyczyły kilku przypadków. Zgłoszenia dokonywane były w trybie natychmiastowym po otrzymaniu takich wiadomości na skrzynkę pocztową w formie elektronicznej poprzez dedykowany kanał do zgłaszania incydentów i innych incydentów na stronie https://incydent.cert.pl. Nie dysponujemy potwierdzeniami zgłoszeń, ponieważ po otrzymaniu wiadomości zwrotnej z CSIRT NASK o podjętych działaniach i informacji o zagrożeniach wynikających z treści wiadomości, takie wiadomości po jakimś czasie były usuwane w celu utrzymania higieny programu pocztowego. W poprzednich wyjaśnieniach dołączono jedno z takich potwierdzeń. Zgłoszenia dokonywane były ustnie przez pracowników do Sekretarza Gminy / Zastępcy Wójta.*

(akta kontroli str. 1054-1055)

6. Nieumieszczenie na stronie internetowej Urzędu informacji o cyberbezpieczeństwie dla mieszkańców Gminy Marianowo, co stanowiło naruszenie art. 22 ust. 1 pkt 4 KSC. Informacja taka pojawiła się dopiero po zadaniu pytania w tej kwestii przez NIK, tj. 19 grudnia 2023 r. W raporcie z przeprowadzonej diagnozy cyberbezpieczeństwa (z dnia 25 lipca 2022 r.) wskazano na istnienie takiej zakładki, jednak do 15 grudnia 2023 r. nie znaleziono na stronie Gminy Marianowo wskazanej zakładki ani innych informacji dotyczących cyberbezpieczeństwa.

   (akta kontroli str. 538, 1055, 1064-1076)

   Zastępca Wójta wyjaśnił, że *Od października 2020 r. Urząd Gminy Marianowo posiada nową stronę internetową www.marianowo.pl, ponieważ poprzednia strona nie spełniała standardów Web Content Accessibility Guidelines. Menu strony było budowane od podstaw. Zgodnie z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, w zakładce menu głównego „Dla Mieszkańca" zamieszczona została zakładka „Cyberbezpieczeństwo" zawierająca informacje dla mieszkańców dot. cyberbezpieczeństwa. Niemniej jednak, aby treść informacji mogła być widoczna na stronie, w panelu administracyjnym strony należy zaznaczyć check-box czy dane menu ma być „widoczne" na stronie. Prawdopodobnie podczas redakcji (edycji któregoś z elementów menu) i zarządzania strukturą menu strony omyłkowo odznaczono check-box zakładki „Cyberbezpieczeństwo", przez co była ona niewidoczna na stronie m.in. w dniu 15 grudnia 2023 r. Niezwłocznie po otrzymaniu w trakcie kontroli informacji w powyższej sprawie, przywrócono wyświetlanie treści menu „Cyberbezpieczeństwo" na stronie urzędu.*

   (akta kontroli str. 1055, 1099-1106)

7. Nieopracowanie planu zachowania ciągłości działania, zawierającego klasyfikację krytycznych danych i operacji wraz z określeniem dodatkowych

zabezpieczeń oraz zbioru usług, systemów operacyjnych i danych wraz z określeniem ram czasowych niezbędnych do ich odtworzenia w przypadku awarii lub ich utraty. 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[33], 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. Wobec braku dokonania klasyfikacji procesów i zasobów informatycznych Urząd nie był w stanie zapewnić adekwatnych mechanizmów zabezpieczeń celem ich ochrony. Ponadto umowy z dostawcą usług informatycznych nie zawierały regulacji dotyczących obowiązku zapewnienia przez usługodawcę ciągłości działania Urzędu.

(akta kontroli str. 615, 1034-1041, 1080, 1088-1090)

Zastępca Wójta wyjaśnił, że *w najbliższym czasie zostaną podjęte działania w celu opracowania i wdrożenia takiego planu w Urzędzie Gminy Marianowo.* Dodatkowo Zastępca Wójta wyjaśnił, że zatrudniony zewnętrzny specjalista do świadczenia usług informatycznych *nie posiada opracowanych procedur eksploatacyjnych niezbędne do zachowania ciągłości działania.*

(akta kontroli str. 615, 1034-1041)

8. Brak weryfikacji liczby, stanów plików i oprogramowania w ramach tworzenia kopii zapasowych. Zgodnie ze standardem C.12 Standardów kontroli zarządczej, 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. Wobec braku weryfikacji liczby, stanów plików i oprogramowania w ramach tworzenia kopii zapasowych, Urząd nie był w stanie zapewnić adekwatnych mechanizmów zabezpieczeń celem ich ochrony.

(akta kontroli str. 615-617, 1035-1041, 1080, 1088-1090)

Zastępca Wójta wyjaśnił, że podczas tworzenia kopii (…) *weryfikowane są pliki i oprogramowanie zapisane w ramach stworzonej kopii zapasowej,* jednak nie przedłożył dokumentacji potwierdzającej weryfikację. Dodatkowo Zastępca Wójta wyjaśnił, że *Zapasowe kopie danych przechowywane na dwóch urządzeniach (…) wykonywane są z wykorzystaniem aplikacji (…). Dodatkowo wykonywane są kopie na dysk zewnętrzny, który po wykonaniu kopii odłączany jest od serwera i przechowywany w metalowej szafie. Niektóre kopie wykonywane są w sposób przyrostowy więc nie ma możliwości przedstawienia zrzutów ekranowych z kilku miesięcy.*

(akta kontroli str. 615-617, 1035-1041)

9. Brak dokumentacji potwierdzającej przeprowadzanie testów planu odtwarzania zasobów. Zgodnie ze standardem C.12 Standardów kontroli zarządczej, 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. Wobec braku dokumentacji potwierdzającej przeprowadzanie

[33] Dz. Urz. MF nr 15, poz. 84, dalej: Standardy kontroli zarządczej.

testów planu odtwarzania zasobów, Urząd nie był w stanie udowodnić, że zapewnia adekwatne mechanizmy zabezpieczeń celem ich ochrony.

(akta kontroli str. 617, 1088-1090)

Zastępca Wójta wyjaśnił, że *Urząd Gminy Marianowo przeprowadzał testy planu odtwarzania utraconych zasobów, jednak nie posiada na tę okoliczność dokumentacji dowodowej.*

(akta kontroli str. 617)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w badanym zakresie.

Negatywną ocenę cząstkową uzasadnia niedokonywanie okresowych analiz ryzyka w latach 2019-2021 i 2023 (do dnia przeprowadzenia czynności kontrolnych) i corocznych audytów bezpieczeństwa informacji w latach 2019-2020 i 2023 (do dnia przeprowadzenia czynności kontrolnych). Zlecanie zadań z zakresu przeprowadzania audytu i polityki bezpieczeństwa informacji IODO powodujące konflikt interesów. W okresie od 28 sierpnia 2018 r. do 10 lipca 2022 r. w Urzędzie nie było wyznaczonej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Urząd nie zgłaszał incydentów do CSIRT NASK lub nie ujmował zgłoszonych incydentów w Rejestrze incydentów bezpieczeństwa informacji. Urząd nie posiadał również przygotowanych procedur pozwalających na zachowanie ciągłości działania i odtworzenie utraconych zasobów, w szczególności nie sklasyfikowano istniejących w Urzędzie procesów i zasobów informatycznych, w wyniku czego nie opracowano planu odtworzenia utraconych zasobów.

OBSZAR

2. Przygotowanie organizacyjno – kadrowe do zapewnienia bezpieczeństwa teleinformatycznego.

Opis stanu faktycznego

1. W Urzędzie nie została przeprowadzona odrębna analiza ryzyka obejmująca wyłącznie czynniki środowiskowe. W kontrolowanym okresie Urząd przeprowadził jedną analizę ryzyka utraty integralności, dostępności informacji, poufności informacji, czynników środowiskowych, co zostało szczegółowo opisane w obszarze 1 wystąpienia pokontrolnego. W zakresie czynników środowiskowych, zidentyfikowano zagrożenia wynikające z wystąpienia klęski żywiołowej (pożar, zalanie), wypadku, zdarzenia, w wyniku których utracono poufność danych osobowych. Ryzyko te oceniono jako akceptowalne i nie wymagające działań obniżających ryzyko[34].

(akta kontroli str. 416-432)

W Gminie Marianowo obowiązywał Gminny Plan Zarządzania Kryzysowego[35]. W Planie ryzyko wystąpienia czynników środowiskowych pożaru i powodzi oceniono jako średnie[36] (prawdopodobne w przypadku pożaru, możliwe w przypadku powodzi[37]).

(akta kontroli str. 748-876)

Na podstawie przeprowadzonych 28 listopada 2023 r. w Urzędzie oględzin[38] ustalono, że serwer był umieszczony na drugim piętrze budynku Urzędu, co eliminowało potencjalne zagrożenie powodzią.

(akta kontroli str. 595, 602-605)

[34] Raport z przeprowadzonej analizy ryzyka w Urzędzie Gminy w Marianowie w okresie od października do listopada 2022 r.

[35] Opracowany przez Wójta w lutym 2016 r. (znak OC.553.1.2016.WR), zatwierdzony przez Starostę Stargardzkiego 23 marca 2016 r.; dalej: Plan.

[36] Skala poziomu ryzyka to: minimalne, małe, średnie, duże, ekstremalne.

[37] Skala prawdopodobieństwa zaistnienia zagrożenia: minimalne, małe, średnie, duże, ekstremalne.

[38] Protokół oględzin z 28.11.2023 r.

2. Urząd posiadał zabezpieczenie w przypadku przerw w dostawie energii elektrycznej. Urząd posiadał agregat prądotwórczy Evolution NPEGG7500 trójfazowy[39]. W przypadku długotrwałej przerwy w dostawie energii elektrycznej agregat mógł być wykorzystany do zasilania urządzeń (jednak do momentu przeprowadzenia kontroli nie zaistniała taka sytuacja). Agregat był poddawany konserwacji okresowej co trzy miesiące[40]. Ponadto komputery stacjonarne w Urzędzie podłączone były do urządzeń UPS, które w przypadku przerw w dostawie prądu służyły do bezpiecznego zamknięcia systemów operacyjnych i wyłączenia komputerów. W serwerowni Urzędu zainstalowany został zasilacz awaryjny CyberPower PR2200ERTXL2U wraz z kartą zarządzającą SNMP o mocy 2200 VA/2200 W, służący do zasilania urządzenia w serwerowni i bezpiecznego wyłączenia w przypadku dłuższej przerwy w zasilaniu.

(akta kontroli str. 595, 934-987)

Na podstawie przeprowadzonych 28 listopada 2023 r. w Urzędzie oględzin ustalono, że główny wyłącznik energii elektrycznej znajdował się na parterze budynku w rozdzielnicy elektrycznej podtynkowej zamkniętej na klucz.

(akta kontroli str. 594, 608)

3. W Urzędzie nie była prowadzona kontrola ruchu osób wchodzących i wychodzących z budynku Urzędu przez pracowników ochrony. W wyniku oględzin ustalono, że w budynku Urzędu funkcjonował monitoring wizyjny i system alarmowy, przy wejściu do głównego holu była umieszczona kamera skierowana na wejście oraz dwa czujniki ruchu (w przedsionku i holu). Osobami uprawnionymi do otwierania i zamykania budynku byli: Wójt, Zastępca Wójta, pracownicy obsługi: konserwator – palacz CO oraz sprzątaczka. Każda z tych osób miała nadany indywidualny kod zabezpieczający w systemie alarmowym, który wprowadzała przy otwieraniu i zamykaniu budynku. Każdy z pracowników pobierał i oddawał klucze do zajmowanych pomieszczeń ze skrzynki znajdującej się w sekretariacie Urzędu. Pobieranie i oddawanie kluczy odbywało się za pomocą wprowadzenia odpowiedniego kodu zabezpieczającego w celu otwarcia szafki. Procedura ta była uregulowana w obowiązującym Regulaminie pracy w Urzędzie Gminy Marianowo, wprowadzonym Zarządzeniem nr 52/2009 Wójta Gminy Marianowo z dnia 29 czerwca 2009 r., zmienionym Zarządzeniem nr 66/2013 z dnia 18 września 2013 r. Serwerownia znajdowała się na drugim piętrze w osobnym pomieszczeniu bez okien, zamkniętym na klucz (brak oznaczeń na drzwiach). Klucz przechowywany był u Zastępcy Wójta. Oprócz serwera w pomieszczeniu znajdowały się: zasilacz awaryjny CyberPower, router, urządzenia UPS oraz rejestrator systemu monitoringu. W serwerowni znajdowało się również urządzenie do klimatyzacji. Na parterze budynku znajdowało się pomieszczenie Urzędu Stanu Cywilnego, ewidencji ludności, dowodów osobistych oraz archiwum zakładowe. Wejście do tego pomieszczenia było zabezpieczone dodatkowo elektronicznym kodem dostępu. Według oświadczenia Zastępcy Wójta i Zastępcy Kierownika Urzędu Stanu Cywilnego, w pomieszczeniu tym wstawione były trzyszybowe okna wraz z folią antywłamaniową oraz czujnikiem reagującym na zbicie szyb i na ruch. Na drugim piętrze znajdowało się pomieszczenie Kancelarii Informacji Niejawnych, zabezpieczonej dodatkowo elektronicznym kodem dostępu. W pomieszczeniu tym znajdowało się urządzenie, na którym sporządzana była dodatkowa kopia bezpieczeństwa danych. Na planie ewakuacji na drugim piętrze było oznaczone pomieszczenie serwerowni, co w ocenie NIK zwiększało ryzyko

[39] O mocy maksymalnej 7,5 KV chłodzony powietrzem, czterosuwowy z silnikiem spalinowym górnozaworowym.

[40] Wpisy w karcie przeglądów potwierdzające konserwację urządzenia co trzy miesiące w okresie od 7 stycznia 2019 r. do 1 września 2023 r.

związane z nieuprawnionym dostępem osób z zewnątrz poprzez możliwość identyfikacji i lokalizacji pomieszczenia serwerowni.

(akta kontroli str. 594-610)

4. W Urzędzie nie sporządzono wykazów umiejętności dla stanowisk ustanowionych w Urzędzie zgodnie z Regulaminem organizacyjnym. Zastępca Wójta przedłożył zakresy czynności, obowiązków i uprawnień dla wybranych stanowisk.

(akta kontroli str. 613-614, 719-739)

Zastępca Wójta wyjaśnił, że *warunki zatrudnienia, obowiązki pracowników samorządowych, podnoszenie kompetencji zawodowych, uprawnienia pracowników samorządowych itp. uregulowane zostały w ustawie z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz. U. z 2022 r. poz. 530). Dodatkowo, wymagania kwalifikacyjne niezbędne do wykonywania pracy na poszczególnych stanowiskach w Urzędzie uregulowane zostały również w rozporządzeniu Rady Ministrów z dnia 25 października 2021 r. w sprawie wynagradzania pracowników samorządowych (Dz. U. z 2021 r. poz. 1960). Ponadto w Regulaminie pracy w Urzędzie (…) określone zostały „obowiązki pracowników" (…) Zgodnie z Regulaminem naboru na wolne stanowiska urzędnicze w Urzędzie indywidualnie stawiane są wymagania na poszczególnych stanowiskach pracy i komunikowane w ogłoszeniu o naborze.*

(akta kontroli str. 613-614)

Urząd nie przedłożył planu szkoleń pracowników obowiązującego w latach 2019-2023. Zgodnie z oświadczeniem Zastępcy Wójta, pracownicy brali udział w bezpłatnych szkoleniach online z zakresu cyberbezpieczeństwa, jednak w toku kontroli nie zostały przedłożone zaświadczenia ani listy obecności na tych szkoleniach (przedłożone zostało jedno zaświadczenie o uczestnictwie jednego pracownika w szkoleniu online „Cyberbezpieczeństwo w samorządach" z 22 stycznia 2021 r.), co zostało opisane w sekcji *Stwierdzone nieprawidłowości*. W złożonym wniosku o grant w ramach projektu „Cyfrowa Gmina" założono przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa (na kwotę 4 000,00 zł). Zgodnie z dokumentem rozliczającym projekt, Urząd zrezygnował z organizacji szkolenia, co uzasadniono korzystaniem z darmowych szkoleń organizowanych przez różne podmioty (w efekcie dokonano zwrotu kwoty grantu w wysokości 3 821,00 zł).

(akta kontroli str. 492-498, 578-586, 613-614, 618-718)

6 grudnia 2023 r. 16 pracowników Urzędu zostało poddanych testowi wiedzy z zakresu cyberbezpieczeństwa (z 19 osób pracujących w Urzędzie na stanowisku pracy z komputerem). 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 58,3%, z czego najniższy wynik wyniósł 33,3%[41], a najwyższy 76,7%[42]. W wyniku szczegółowej analizy udzielonych odpowiedzi ustalono, że na 10 pytań (33% zadanych) mniej niż połowa testowanych udzieliła poprawnych odpowiedzi. Wśród pytań, na które udzielono najmniej poprawnych odpowiedzi znalazły się m.in. pytania dotyczące:

- konsekwencji nieostrożnego korzystania z serwisów społecznościowych – dwie osoby odpowiedziały poprawnie;
- tworzenia bezpiecznego hasła – trzy osoby odpowiedziały poprawnie;
- postępowania w przypadku identyfikacji wirusa komputerowego – cztery osoby odpowiedziały poprawnie;

[41] W jednym przypadku.
[42] W jednym przypadku.

- korzystania z sieci Wi-Fi; identyfikacji, czy na komputerze znajduje się wirus; identyfikacji ataku typu phishing; środków ostrożności na wypadek kradzieży smartfona lub tabletu – pięć osób odpowiedziało poprawnie.

(akta kontroli str. 1042-1053, 1107-1110)

5. Na podstawie oględzin sześciu stanowisk pracy z komputerem ustalono, że na stanowiskach pracy nie było zamieszczonych w widocznych miejscach danych do logowania. Pracownicy stosowali hasła o długości znaków:

- jeden pracownik – cztery znaki (w trakcie oględzin pracownik zmienił hasło z czterech znaków na 12 znaków);
- dwóch pracowników – 10 znaków;
- dwóch pracowników – 11 znaków;
- jeden pracownik – 14 znaków.

Długość haseł była niezgodna z obowiązującym w Urzędzie na dzień oględzin[43] SZBI 2.0, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

Pracownicy potrafili zablokować komputer (za pomocą paska poleceń – wyloguj, blokuj lub uśpij), co było zgodne z § 66 pkt 3 SZBI 2.0, który stanowił, że *Wymaga się, aby użytkownicy sieci teleinformatycznej (…) zabezpieczali nieużywane w danym momencie komputery osobiste lub terminale przed nieupoważnionym dostępem poprzez blokadę klawiatury lub w inny równoważny sposób, np. dostęp do komputera po podaniu hasła.*

(akta kontroli str. 595-596, 609-610)

6. Urząd w kontrolowanym okresie zatrudniał zewnętrznego specjalistę do świadczenia usług informatycznych, prowadzącego działalność gospodarczą, w ramach zawartych pięciu umów cywilnoprawnych[44]. Zgodnie z treścią tych umów, do obowiązków usługodawcy należało m.in.:

- świadczenie nadzoru informatycznego oraz usuwanie usterek i awarii sieci informatycznej oraz systemów serwerowych Urzędu,
- konserwacja sprzętu komputerowego oraz oprogramowania wykorzystywanego w Urzędzie,
- nadzór i administracja sieci komputerowej, serwerów, usług internetowych, baz danych Urzędu,
- nadzór i administracja systemów backupu danych,
- kontrola bezpieczeństwa sieci komputerowej,
- nadzór nad prawidłową eksploatacją i administrowaniem serwerów oraz funkcjonowaniem mechanizmów uwierzytelniania użytkowników,
- instalacja oprogramowania systemowego oraz aplikacyjnego na stacjach roboczych,
- świadczenie usług doradczych m.in. poprzez udział w pracach związanych z zakupami sprzętu komputerowego oraz oprogramowania,
- wsparcie użytkowników w zakresie użytkowania oprogramowania systemowego, aplikacyjnego oraz sprzętu komputerowego i peryferyjnego,
- analiza wymagań użytkowników dotyczących wprowadzenia zmian w użytkowanych systemach informatycznych,
- usuwanie awarii w oprogramowaniu oraz sprzęcie informatycznym,
- przestrzeganie wdrożonych u Zleceniodawcy Polityk Bezpieczeństwa Informacji (SZBI).

[43] Tj. 28.11.2023 r.

[44] Umowy zawarte pomiędzy Gminą Marianowo a M. K., prowadzącym działalność gospodarczą, na świadczenie usług informatycznych: nr SG/32/2019 z 3 stycznia 2019 r. na okres od 03.01.2019 do 31.12.2019 r.; nr SG/40/2020 z 2 stycznia 2020 r. na okres od 02.01.2020 do 31.12.2020 r.; nr SG/16/2021 z 4 stycznia 2021 r. na okres od 04.01.2021 do 31.12.2021 r.; SG/18/2022 z 4 stycznia 2022 r. na okres od 03.01.2022 do 31.12.2022 r.; SG/18/2023 z 2 stycznia 2023 r. na okres od 01.01.2023 do 31.12.2023 r.

Do ww. umów nie zostały wpisane obowiązki wynikające z SZBI, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 170-199, 250-414)

Zastępca Wójta wyjaśnił, że *korzystanie z usług zewnętrznego podmiotu ds. obsługi informatycznej w Urzędzie nie było spowodowane problemami z pozyskaniem pracownika w ramach rekrutacji na to stanowisko, ani też innymi trudnościami. W latach 2019-2023 w Urzędzie nie przeprowadzano naboru na stanowisko związane z obsługą informatyczną Urzędu.* Ponadto, zgodnie z wyjaśnieniami Zastępcy Wójta, *Urząd nie weryfikował kwalifikacji podmiotu do świadczenia tych usług, ponieważ współpracuje z tym podmiotem od około 20 lat w zakresie obsługi informatycznej Urzędu i bazuje na własnej ocenie kompetencji i kwalifikacji tego podmiotu, znajomości przed podmiot zastosowanych w Urzędzie rozwiązań informatycznych, przy wdrożeniu których brał czynny udział w formie doradczej.*

(akta kontroli str. 446, 615)

7. Gmina Marianowo 16 listopada 2021 r. złożyła wniosek o grant w ramach projektu „Cyfrowa Gmina" na kwotę 100 000,00 zł, 31 stycznia 2022 r. została podpisana umowa. W ramach otrzymanych środków Urząd w pierwszym etapie przeprowadził diagnozę cyberbezpieczeństwa[45]. Na podstawie wyników przeprowadzonej diagnozy, w drugim etapie zakupiono nowy serwer wraz z oprogramowaniem, serwer do przechowywania danych (kopii bezpieczeństwa), urządzenie sieciowe typu UTM, zasilacz awaryjny UPS, oprogramowanie do centralnego zarządzania kopiami bezpieczeństwa, siedem zestawów komputerowych (stacja robocza, monitor, mysz, klawiatura, oprogramowanie biurowe), trzy monitory, dwa zestawy kamer internetowych i słuchawek z mikrofonem. We wniosku założono przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, jednak na etapie realizacji umowy zrezygnowano z organizacji szkolenia, co uzasadniono korzystaniem z dostępnych darmowych szkoleń. W toku kontroli nie przedłożono innych analiz potrzeb Urzędu z zakresu cyberbezpieczeństwa. Urząd wydatkował środki zaplanowane w budżecie na zadania związane z informatyzacją (na sprzęt, licencje, usługi) w wysokości: w roku 2019 – 35 803,12 zł, w roku 2020 – 37 190,86 zł, w roku 2021 – 25 046,00 zł, w roku 2022 – 27 559,88 zł, w roku 2023 – 155 964,21 zł (w tym środki z projektu grantowego „Cyfrowa Gmina"). Urząd planował złożenie wniosku w ramach konkursu grantowego „Cyberbezpieczny Samorząd" (termin na złożenie wniosku upływał 14 grudnia 2023 r.) w celu m.in. pozyskania środków na nowe systemy informatyczne.

(akta kontroli str. 492-588, 614-615)

Zastępca Wójta wyjaśnił, że *w latach 2019-2023 budżet Gminy Marianowo nie był i nie jest prowadzony w formie budżetu zadaniowego, a jego szczegółowość opierała się na klasyfikacji budżetowej do poziomu paragrafu, co oznacza, że środki w nim zaplanowane nie wskazują przeznaczenia na konkretne wydatki. Stąd też wykazanie środków przeznaczonych w budżecie wyłącznie na działania z zakresu cyberbezpieczeństwa jest utrudnione. (…) Środki na działania związane z informatyzacją Urzędu planowane są w budżecie Gminy Marianowo na poziomie pozwalającym zapewnić wystarczający poziom cyberbezpieczeństwa w Urzędzie, niemniej potrzeby w tym zakresie są wciąż wysokie, a środki finansowe Gminy są ograniczone.*

(akta kontroli str. 614-615)

8. Oprogramowanie zabezpieczające wykorzystywane przez Urząd było aktualne i adekwatne do zidentyfikowanych rodzajów ryzyka oraz do możliwości i skali

[45] Szczegółowo opisano w obszarze 1.

działania Urzędu. Na podstawie opinii biegłego i przedłożonej dokumentacji ustalono, że Urząd stosował wielowarstwowe zabezpieczenia w zakresie różnego rodzaju zagrożeń. W ramach rozwiązań dedykowanych do ochrony brzegu sieci Urząd wykorzystywał urządzenie UTM. Rozwiązanie to dedykowane było do średnich sieci, w związku z tym było w pełni adekwatne do potrzeb Urzędu. Urządzenie konsolidowało i kontrolowało wszystkie składniki zabezpieczeń za pomocą jednej konsoli zarządzania. W Urzędzie były zainstalowane moduły, które obejmowały:

- Antywirus – pozwalający m.in. na analizę sygnaturową czy behawioralną zagrożeń,
- Moduły antyspyware i antymalware, antyspam – zapewniające ochronę sieci przed szpiegującym i szkodliwym oprogramowaniem,
- Firewall,
- VPN,
- IPS (Intrusion Prevention System) – wykrywający i blokujący tego rodzaju działania w czasie rzeczywistym,
- Kontrolę aplikacji – umożliwiając analizę aplikacji używanych na poszczególnych urządzeniach końcowych, w razie potrzeby blokując instalację/użycie niebezpiecznego oprogramowania,
- Web filtering – narzędzia ograniczające korzystanie z Internetu, mające na celu m.in. utrzymanie przepustowości łącza.

Na poziomie hostów Urząd wykorzystywał oprogramowanie antywirusowe/antymalware, które zapewniało ochronę przed szerokim spektrum zagrożeń, takich jak wirusy, trojany, spyware, a także inne rodzaje złośliwego oprogramowania.

(akta kontroli str. 1015-1041, 1081, 1090-1091)

9. Urząd posiadał zinwentaryzowane środowisko informatyczne. Na podstawie opinii biegłego i przedłożonej dokumentacji ustalono, że Urząd wykorzystywał niektóre aplikacje w nieaktualnych wersjach, w tym ze znanymi podatnościami, które to podatności oznaczone zostały jako krytyczne i umożliwiały np. zdalne wykonanie kodu lub przejęcie kontroli nad systemem. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości*. Zgodnie z oświadczeniem Zastępcy Wójta, nie wystąpiły przypadki funkcjonowania niezidentyfikowanych urządzeń w sieci Urzędu.

(akta kontroli str. 1015-1041, 1081, 1090-1093)

10. Na podstawie opinii biegłego i przedłożonej dokumentacji (analiza inwentaryzacji oprogramowania na stacjach roboczych) ustalono, że pracownicy Urzędu mieli możliwość korzystania z rozwiązań chmurowych. Zgodnie z oświadczeniem Zastępcy Wójta, Urząd nie korzystał z rozwiązań chmurowych. Powyższa sytuacja została opisana w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 617, 1015-1041, 1081, 1090-1093)

11. Na podstawie przeprowadzonych oględzin stanowisk komputerowych ustalono, że pracownicy mieli możliwość zalogowania się na prywatną skrzynkę pocztową z komputerów służbowych. Jeden pracownik oświadczył, że czasami logował się na prywatną skrzynkę pocztową, pozostali pracownicy[46] oświadczyli, że nie korzystali z prywatnej skrzynki pocztowej na komputerach służbowych. Powyższa sytuacja została opisana w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 595-596)

Podczas oględzin ustalono, że pracownicy Urzędu podawali w korespondencji służbowe adresy e-mail, tj. ug@marianowo.pl, sekretarz@marianowo.pl, rada@marianowo.pl, usc@marianowo.pl, komunalny@marianowo.pl, transport@marianowo.pl.

[46] Pięć osób.

(akta kontroli str. 595-596, 933)

Stwierdzone nieprawidłowości

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

1. Nieprzeprowadzanie szkoleń dla pracowników Urzędu z zakresu cyberbezpieczeństwa, co stanowiło naruszenie § 20 ust. 2 pkt 6 KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.
   Pracownicy Urzędu, zgodnie z oświadczeniem Zastępcy Wójta, odbywali bezpłatne szkolenia online z zakresu cyberbezpieczeństwa. Jednocześnie nie przedłożono list obecności, zaświadczeń ani certyfikatów potwierdzających odbycie takich szkoleń. Urząd pozyskał środki na odbycie szkolenia z zakresu cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina", jednak środki te nie zostały wykorzystane i zostały zwrócone grantodawcy. W celu udowodnienia zgodności z powyższymi wymogami prawnymi, Urząd powinien zapewnić dokumentowanie odbywania szkoleń przez pracowników z podaniem tematyki szkolenia, udziału pracowników, terminów przeprowadzenia szkoleń i efektów szkoleń. Przeprowadzony test wiedzy z zakresu cyberbezpieczeństwa wykazał, że pracownicy nie mieli wystarczającej wiedzy z tego zakresu.
   (akta kontroli str. 492-498, 578-587, 613, 618-718, 1042-1053, 1055-1057)

   Zastępca Wójta wyjaśnił, że *pracownicy Urzędu korzystali z możliwości bezpłatnych szkoleń prowadzonych poprzez różnego rodzaju platformy szkoleniowe w formule online, prowadzonych przez takie podmioty, jak CERT NASK, Sekurak, Narodowy Instytut Samorządu Terytorialnego, czy Związek Powiatów Polskich itp. Szkolenia te obejmowały np. tematy: 1) przegląd ostatnich głośnych cyberataków na firmy/internautów w Polsce, 2) jak ransomware dostaje się do firm, 3) czym grozi otwarcie załącznika z maila, 4) cyberbezpieczeństwo w samorządach. Proces wyglądał następująco: po otrzymaniu lub pozyskaniu informacji o szkoleniu, Sekretarz wysyłał informację o szkoleniu pracownikom Urzędu z informacją o możliwości udziału w takim szkoleniu lub osobiście dokonywał zgłoszenia na szkolenie, które następnie oglądane było przez pracowników w czasie rzeczywistym na Sali konferencyjnej Urzędu, wyposażonej do tego typu rozwiązań szkoleniowych w formule online. Z uwagi na fakt, że zgłaszana przez Urząd była jedna osoba, a pozostali pracownicy uczestniczyli w szkoleniu, nie było możliwości otrzymania certyfikatu udziału w szkoleniu przez wszystkich uczestników, tylko przez osobę zgłoszoną. Na bieżąco przekazywane są pracownikom Urzędu ważne informacje dotyczące zasady cyberbezpieczeństwa, różnego rodzaju poradniki, ostrzeżenia czy komunikaty*[47].

[47] Na potwierdzenie tego stanu rzeczy przedłożono: Poradnik ransomware NASK, informację od NASK Zespół CERT o potencjalnym zagrożeniu, prezentację NASK dotycząca zapisów ustawy o Krajowym Systemie Cyberbezpieczeństwa, wskazówek, standardów, Podręcznik NASK ABC bezpieczeństwa, Poradnik PRCyber-02 Zgłaszanie incydentów przez jednostki samorządu terytorialnego, podziękowanie za udział w sondażu NASK z 21.07.2023 r., informacje w formie wiadomości e-mail od Sekretarza do pracowników Urzędu dotyczące szkoleń z zakresu cyberbezpieczeństwa i ostrzeżeń o przypadkach phisingu i ataków hakerskich (z 09.12.2019,

(akta kontroli str. 613, 618-718)

2. Niezapewnienie długości haseł do systemu, stosowanych przez pracowników, zgodnej z obowiązującym w Urzędzie na dzień oględzin[48] SZBI 2.0. Zgodnie z § 62 ust. 6 pkt 1 SZBI, hasło dobrej jakości dla standardowego użytkownika miało długość co najmniej 12 znaków (tj. 14 znaków). W wyniku oględzin ustalono, że tylko jeden pracownik stosował hasło zgodnie z zapisami SZBI, pozostali pracownicy (pięć osób) mieli hasła składające się z mniejszej liczby znaków, w tym jedna osoba zmieniła w trakcie oględzin długość hasła z czterech na 12 znaków. Ponadto, zgodnie z zaleceniami Zespołu CERT Polska, działającego w strukturach Naukowej i Akademickiej Sieci Komputerowej[49], należy stosować długie hasła powyżej 14 znaków.

   (akta kontroli str. 354, 595-596, 1063)

   Zastępca Wójta wyjaśnił, że *Z informacji uzyskanych od pracowników stosujących niewłaściwą strukturę haseł wynika, że stosowanie haseł o długości co najmniej 12 znaków, w połączeniu z częstym włączaniem się wygaszacza ekranu monitora zabezpieczonego takim hasłem, mocno utrudnia pracę i jest irytujące. Ponadto, pracownicy myśleli, że kwestie dotyczące liczby znaków w haśle są wyłącznie zaleceniem, a nie obowiązkiem, więc ustalali hasła krótsze ale zawierające trzy grupy znaków spośród czterech w postaci: małe litery, duże litery, cyfry, znaki specjalne. Poinstruowano pracowników o konieczności stosowania się do zaleceń zawartych w SZBI.*

   (akta kontroli str. 1099-1106)

3. Niewpisanie do umów o świadczenie usług informatycznych obowiązków wynikających z SZBI, co było działaniem nierzetelnym. NIK zauważa, że brak precyzyjnych postanowień w umowie oraz brak ciągłości działania mogły negatywnie wpłynąć na skuteczność zarządzania ryzykiem i ciągłością operacyjną w przypadku wystąpienia awarii lub innych nieprzewidzianych zdarzeń u dostawcy usług IT. Brak szczegółowych wymagań w zakresie planowania i demonstracji zdolności dostawcy usług IT do kontynuacji świadczenia tych usług mogło spowodować, że w przypadku wystąpienia sytuacji kryzysowej (tzw. katastrofy) u usługodawcy Urząd mógł doświadczyć nieplanowanych przerw w dostępie do kluczowych usług IT, co mogło wpłynąć na ciągłość działania Urzędu i jego zdolność do wykonywania zadań.

   (akta kontroli str. 170-199, 250-414, 1088-1090)

   Zastępca Wójta wyjaśnił, że *przez niedopatrzenie osoby sporządzającej projekt umowy z firmą informatyczną obowiązki te nie zostały uwzględnione w projekcie. W umowach zawieranych w przyszłości obowiązki te będą uwzględniane. Pomimo braku odpowiednich zapisów w umowie większość obowiązków, o których mowa powyżej była przez informatyka realizowana, aczkolwiek nie zawsze udokumentowana.*

   (akta kontroli str. 1055-1057)

4. Wykorzystywanie aplikacji w nieaktualnych wersjach, np.: 7-Zip, WinRar, Firefox, PdfCreator, w tym ze znanymi podatnościami, które to podatności oznaczone zostały jako krytyczne i umożliwiały np. zdalne wykonanie kodu lub przejęcie kontroli nad systemem. Wymagało to podjęcia natychmiastowych działań

20.06.2022, 20.10.2022, 28.04.2023, 30.05.2023, 10.08.2023, 16.11.2023 r.), zaświadczenie z NASK o uczestnictwie S. S. w szkoleniu online „Cyberbezpieczeństwo w samorządach" z 22.01.2021 r.

[48] Tj. 28.11.2023 r.

[49] Wynikające ze zbioru zasad dotyczących bezpiecznego korzystania z poczty elektronicznej i mediów społecznościowych przygotowanych przez CSIRT NASK https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf

korygujących, aby poprawić poziom bezpieczeństwa informatycznego. NIK zauważa, że używanie nieaktualnego oprogramowania, w tym aplikacji ze znanymi podatnościami, niesie ze sobą znaczące ryzyka utraty poufności, integralności i dostępności wrażliwych danych, a także może prowadzić do zakłóceń w działalności Urzędu, co może mieć negatywne skutki dla świadczenia usług publicznych. Powyższe było niezgodne z § 20 ust. 2 pkt 7 KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami przez: monitorowanie dostępu do informacji, czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

(akta kontroli str. 1015-1034, 1081, 1092)

Zastępca Wójta wyjaśnił, że *Z ustaleń poczynionych z podmiotem zewnętrznym obsługującym Urząd Gminy Marianowo w zakresie IT wynika, że część z wyżej wymienionych aplikacji np. WinRar czy PdfCreator zostało zainstalowanych przy okazji instalacji innych aplikacji na zasadzie oprogramowania osadzonego w formie promocji (reklamy) do określonej aplikacji i nie było fizycznie wykorzystywane. Oprogramowanie to nie było aktualizowane lub usuwane przez przeoczenie informatyka, o czym został poinformowany. Nie dysponujemy w urzędzie dedykowanym oprogramowaniem, które umożliwiałoby automatyzację procesu aktualizacji wszystkich aplikacji na wszystkich komputerach w urzędzie. Indywidualne aktualizacje na każdej jednostce sprzętu są wydłużone w czasie, odrywają pracowników od pracy i są mozolne. Dlatego w ramach projektu grantowego „Cyberbezpieczny Samorząd" zaplanowaliśmy dedykowane do tego celu oprogramowanie, ale w chwili obecnej urząd oczekuje na ocenę wniosku grantowego. Na przyszłość podjęte zostaną działania związane z doprecyzowaniem umów w zakresie świadczenia usług IT przez podmiot zewnętrzny na rzecz Urzędu Gminy Marianowo.*

(akta kontroli str. 1099-1106)

5. Nieopracowanie procedur i niemonitorowanie przez Urząd wykorzystywania usług chmurowych. Zgodnie z oświadczeniem Zastępcy Wójta, Urząd nie korzystał z rozwiązań chmurowych. Na podstawie opinii biegłego i przedłożonej dokumentacji (analiza inwentaryzacji oprogramowania na stacjach roboczych) ustalono, że pracownicy Urzędu mieli możliwość korzystania z rozwiązań chmurowych, takich jak: Dysk Google, Microsoft OneDrive. W ocenie NIK wskazywało to na niespójność i nieskuteczność w zarządzaniu i kontrolowaniu stosowania oprogramowania w środowisku Urzędu. Dostęp do ww. usług chmurowych na stacjach roboczych bez odpowiednich procedur zarządzania i kontroli mógł prowadzić do nieuprawnionego przechowywania, udostępniania lub przetwarzania danych w chmurze, co stwarzało znaczące ryzyko dla bezpieczeństwa danych Urzędu. Powyższe było niezgodne z § 20 ust. 2 pkt 1 KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

(akta kontroli str. 1015-1034, 1081, 1093-1094)

Zastępca Wójta wyjaśnił, że *W Urzędzie Gminy Marianowo nie są wykorzystywane do celów służbowych rozwiązania chmurowe. Wskazane w pytaniu oprogramowania chmurowe z reguły są zainstalowane w systemie domyślnie, jak np. Microsoft OneDrive, Microsoft OneNote, Microsoft SkyDrive, lub są instalowane przy okazji instalacji niektórych aplikacji, jak np. Google Chrome. W celu korzystania z nich użytkownik musi posiadać konto i być zalogowany. Natomiast pracownicy urzędu nie korzystają z tych rozwiązań podczas wykonywania czynności służbowych. Podjęte zostaną działania w celu usunięcia bądź dezaktywacji ww. aplikacji.*

(akta kontroli str. 1094)

6. Niewyłączenie możliwości korzystania przez pracowników Urzędu z prywatnych skrzynek pocztowych na komputerach służbowych. Powyższe było działaniem nierzetelnym i zwiększało podatność Urzędu na naruszenia cyberbezpieczeństwa. NIK zauważa, że zgodnie z zasadami bezpiecznego użytkowania poczty elektronicznej[50], komputerów służbowych nie powinno się używać do spraw prywatnych (w szczególności do czytania prywatnej poczty elektronicznej). Powyższe może narażać Urząd na możliwość otworzenia przez pracowników fałszywych wiadomości e-mail czy zawierających wirusy (np. typu ransomware). Dodatkowo prywatne skrzynki pocztowe nie są objęte zabezpieczeniami stosowanymi przez Urząd.

(akta kontroli str. 595-596, 1063)

Zastępca Wójta wyjaśnił, że *Zgodnie z SZBI pracownicy nie powinni korzystać z Internetu w tym z prywatnej poczty elektronicznej. Uznano, że skoro są to uregulowania wewnętrzne, do których powinni się stosować wszyscy pracownicy, uznano, że nie ma potrzeby blokowania konkretnych stron czy portali internetowych. Zostało to zakomunikowane wszystkim pracownikom wraz z ewentualnymi konsekwencjami służbowymi. Niemniej jednak po dokonaniu analizy, czy pracownicy łamią ten zakaz, zostaną skonfigurowane mechanizmy blokujące możliwość korzystania z poczty elektronicznej w trakcie świadczenia pracy. Mamy taką możliwość przy wykorzystania urządzenia UTM Fortigate.*

(akta kontroli str. 1012-1014)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w badanym zakresie. Negatywną ocenę cząstkową uzasadnia brak przygotowania organizacyjnego i kadrowego do zapewnienia bezpieczeństwa teleinformatycznego. Powyższe potwierdzają stwierdzone nieprawidłowości, w szczególności: niezapewnienie pracownikom szkoleń z zakresu bezpieczeństwa teleinformatycznego, niezapewnienie długości haseł do systemu stosowanych przez pracowników zgodnej z obowiązującym w Urzędzie SZBI, niewpisanie do umów o świadczenie usług informatycznych obowiązków wynikających z SZBI, wykorzystywanie aplikacji w nieaktualnych wersjach, nieopracowanie procedur i niemonitorowanie przez Urząd wykorzystywania usług chmurowych, niewyłączenie możliwości korzystania przez pracowników Urzędu z prywatnych skrzynek pocztowych na komputerach służbowych.

IV. Uwagi i wnioski

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

[50] Tamże.

Wnioski

1. Zapewnienie procedury obowiązku każdorazowego wyciągania wniosków z obsłużonego incydentu bezpieczeństwa informacji w celu zaplanowania działań zapobiegawczych, uwzględniającej analizę przyczyn i okoliczności incydentów oraz identyfikację słabych punktów w systemach i procedurach.
2. Zapewnienie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy i zapewnienia corocznych audytów bezpieczeństwa informacji.
3. Zapewnienie braku konfliktu interesów audytora przeprowadzającego audyt systemu zarządzania bezpieczeństwem informacji.
4. Zapewnienie aktualności danych osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
5. Opracowanie i wdrożenie skutecznego mechanizmu zarządzania incydentami bezpieczeństwa informacji, w tym schematu zgłaszania incydentów do właściwego CSIRT.
6. Przeprowadzenie klasyfikacji krytyczności procesów i zasobów informatycznych Urzędu.
7. Opracowanie, wdrożenie i przestrzeganie planu odtworzenia utraconych zasobów zapewniającego ciągłość działania.
8. Zapewnienie prowadzenia dokumentacji z przeprowadzonych testów planu odtwarzania zasobów.
9. Zapewnienie pracownikom szkoleń z zakresu cyberbezpieczeństwa.
10. Zapewnienie stosowania haseł do systemu zgodnie z obowiązującym w Urzędzie SZBI.
11. Wpisanie do umów o świadczenie usług informatycznych obowiązków wynikających z SZBI.
12. Zapewnienie aktualnych wersji wykorzystywanych w Urzędzie aplikacji.
13. Zapewnienie monitorowania użycia zasobów dostępnych w modelu chmurowym wraz z przygotowaniem alertów w przypadku wykorzystywania chmury obliczeniowej oraz aplikacji lub platform przetwarzających w nich dane bez zgody Wójta.
14. Wyłączenie możliwości korzystania przez pracowników z prywatnych skrzynek pocztowych na komputerach służbowych.

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 ust. 1 i 2 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 wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 30 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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, 9 stycznia 2024 r.

Kontroler
Izabela Kirysiuk
Główny specjalista kontroli państwowej

/-/

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Szczecinie
p.o. Dyrektor
dr Marcin Stefaniak

/-/

.....
podpis

Zmian w wystąpieniu pokontrolnym dokonał: Marcin Stefaniak p.o. Dyrektora Delegatury NIK w Szczecinie.