NAJWYŻSZA IZBA KONTROLI

Delegatura w Szczecinie

LSZ.411.3.2.2023

Jarosław Burba
Burmistrz Nowego Warpna
Urząd Gminy Nowe Warpno
pl. Zwycięstwa 1
72-022 Nowe Warpno

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 Nowe Warpno[1] Plac Zwycięstwa 1, 72-022 Nowe Warpno
Kierownik jednostki kontrolowanej	Jarosław Burba, Burmistrz Nowego Warpna[2], od 21 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 zakończenia czynności kontrolnych[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 Delegatura w Szczecinie
Kontroler	1. Adam Milczarek, Starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LSZ/178/2023 z 6 listopada 2023 r. 2. Ewelina Kamińska-Nowicka, Specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/179/2023 z 6 listopada 2023 r. (akta kontroli str.1-3)

[1] Dalej: Urząd.

[2] Dalej: Burmistrz.

[3] 15 grudnia 2023 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.

Uzasadnienie oceny ogólnej

Negatywną ocenę uzasadniają nieprawidłowości w obszarze dotyczącym stworzenia, wdrożenia i przestrzegania polityki z zakresu bezpieczeństwa teleinformatycznego. W szczególności obowiązujący w Urzędzie System Zarządzania Bezpieczeństwem Informacji nie był zgodny z normą PN-EN ISO/IEC 27001[6]. W Urzędzie przypisano też zadania z zakresu przeprowadzania audytu i polityki bezpieczeństwa informacji Inspektorowi Ochrony Danych, co powodowało konflikt interesów. W okresie od 28 sierpnia 2018 r. do 12 czerwca 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 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.

Negatywnie oceniono również obszar dotyczący przygotowania organizacyjno-kadrowego Urzędu do zapewnienia bezpieczeństwa teleinformatycznego. W Urzędzie nie zabezpieczono głównych elementów infrastruktury informatycznej przed nieuprawnionym dostępem, umieszczając serwer w jednym z pokoi przechodnich znajdujących się w Urzędzie. Ponadto serwer znajdował się w otwartej szafie meblowej. Natomiast główny wyłącznik prądu znajdował się w przestrzeni ogólnodostępnej, w szafce w której na dzień przeprowadzania oględzin znajdowały się klucze. Urząd nie przeprowadzał analizy potrzeb z zakresu cyberbezpieczeństwa, jak i nie planowano środków na ww. wydatki w budżecie Gminy. Zakupów dokonywano doraźnie, w przypadku konieczności wymiany sprzętu. Pracownicy mieli również możliwość korzystania z prywatnej poczty elektronicznej na komputerach służbowych, co zwiększało ryzyko naruszenia cyberbezpieczeństwa. W Urzędzie nie przestrzegano również obowiązującej polityki kluczy, w tym nie prowadzono ewidencji dostępu do pomieszczeń, jak i ewidencji pobrań kluczy. Pracownikom nie zapewniono szkoleń z zakresu cyberbezpieczeństwa, co skutkowało niskim poziomem wiedzy w zakresie identyfikacji i zachowania w przypadku cyberataku.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1. W Urzędzie Zarządzeniem Burmistrza nr 032/2018 z 24 maja 2018 r. wprowadzono *Politykę Ochrony Danych Osobowych*[9], w skład której wchodziła *Instrukcja zarządzania systemami informatycznymi wraz z wykazem zabezpieczeń*

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

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

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

[8] 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.

[9] Dalej: PODN.

regulacji ochrony danych osobowych oraz *Regulamin ochrony danych osobowych w jednostce.* Powyższa dokumentacja stanowiła obowiązujący w Urzędzie System Zarządzania Bezpieczeństwem Informacji[10].

(akta kontroli str. 4, 10,17-132)

Obowiązujący w Urzędzie SZBI nie zostało poddane certyfikacji PN-ISO/IEC 27001.

(akta kontroli str. 4, 10)

Na potrzeby realizacji programu pn. *Cyfrowa Gmina* Urząd zlecił przeprowadzenie 22 czerwca 2022 r. przez Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-ISO/IEC 27001 oceny zgodności SZBI z rozporządzeniem 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[11] oraz zgodności z ustawą KSC. W wyniku audytu stwierdzono, iż obowiązujące w Urzędzie SZBI nie jest zgodne z ww. aktami prawnymi.

(akta kontroli str. 216-227, 242, 262)

W wyniku szczegółowej analizy SZBI ustalono, iż nie był on zgodny z normą PN-ISO/IEC 27001, co stanowiło naruszenie § 20 ust. 3 KRI. Powyższe zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 236-237)

Burmistrz 6 września 2022 r. wprowadził aktualizację ww. dokumentacji pn. *Polityka bezpieczeństwa informacji,* a 1 kwietnia 2023 r. *Instrukcję zarządzania systemem informatycznym[12].* Powyższa dokumentacja została opracowana, a następnie podpisana (zatwierdzona) przez Burmistrza, natomiast nie została wprowadzona w formie zarządzenia burmistrza. Nie zostało uchylone też obowiązujące zarządzenie nr 032/2018, co zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 17-132, 240, 261)

W wyniku szczegółowej analizy Aktualizacji SZBI ustalono, iż nie była ona zgodna z normą PN-ISO/IEC 27001, co stanowiło naruszenie § 20 ust. 3 KRI. Powyższe zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 238)

W SZBI i w Aktualizacji SZBI zadania z zakresu przeprowadzania audytu polityki bezpieczeństwa informacji przypisane Inspektorowi Ochrony Danych[13], co zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 17-132, 240-241, 261-262)

2. W okresie objętym kontrolą Urząd przeprowadzał analizę ryzyka zawierającą informację na temat zidentyfikowanych zagrożeń: ataków zewnętrznych, zagrożeń dla ciągłości działania zagrożeń danych, błędów ludzkich oraz inwentarz aktywów. Dokument ten został utworzony 28 maja 2019 r., a następnie został zaktualizowany 9 września 2019 r., 7 czerwca 2021 r. i 14 lipca 2022 r.

(akta kontroli str. 141-149, 239, 260, 357, 362)

3. Od 28 sierpnia 2018 r. (daty wejścia w życie KSC) do dnia 12 czerwca 2022 r. w Urzędzie nie wyznaczono osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Osoba ta została wyznaczona 13 czerwca 2022 r. na podstawie zarządzenia Burmistrza nr 050/2022.

---

[10] Dalej: SZBI.

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

[12] Dalej: Aktualizacja SZBI.

[13] Dalej: IOD.

Funkcję tę pełnił zatrudniony w Urzędzie informatyk. Od 31 marca 2023 r. po rozwiązaniu z ww. pracownikiem umowy o pracę do 20 listopada 2023 r., nie przypisano żadnej osobie ww. obowiązków. Powyższe zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. . 4, 10, 133-137, 239, 260, 265)

Wyznaczenie osoby do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa obejmowało swoim zakresem zadania publiczne zależne od systemów informacyjnych realizowanych przez Gminę Nowe Warpno oraz gminne jednostki organizacyjne, tj. Ośrodek Pomocy Społecznej w Nowym Warpnie, Zakład Gospodarki Komunalnej w Nowym Warpnie, Gminna Biblioteka Publiczna w Nowym Warpnie i Zespół Szkolno-Przedszkolny w Nowym Warpnie.

(akta kontroli str.10)

4. Od 24 maja 2018 r. w Urzędzie prowadzono rejestr zdarzeń, w których doszło do naruszenia ochrony danych osobowych.

(akta kontroli str. 4, 10, 17-132,138)

Na podstawie przeprowadzonych przez powołanego w trakcie kontroli Biegłego badań ustalono, iż Urząd nie monitorował zdarzeń w ramach systemów IT, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 4, 10, 17-132,138, 366-389)

W obowiązującym w Urzędzie w okresie objętym kontrolą SZBI zawarto ogólne regulacje związane z obowiązkiem zgłaszania przez pracowników naruszenia bezpieczeństwa danych osobowych. W Aktualizacji SZBI określono sposób postępowania w przypadku wystąpienia incydentów zagrażających bezpieczeństwu danych i informacji. Procedura wymagała jedynie poinformowania przez pracownika przełożonego lub Inspektora Ochrony Danych, którzy powinni przeprowadzić postępowanie wyjaśniające, które ustali przyczyny i zakres niepożądanego zdarzenia oraz określi jego ewentualne skutki.

(akta kontroli str. 4, 10, 17-132)

Na podstawie opinii Biegłego ustalono, iż proces zgłaszania incydentów bezpieczeństwa informacji nie został przez Urząd ustanowiony w sposób odpowiedni, ponieważ koncentrował się głównie na danych osobowych, co mogło prowadzić do sytuacji, w której pracownicy Urzędu mogli zinterpretować te zasady jako dotyczące wyłącznie danych osobowych, pomijając inne rodzaje chronionych informacji, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 366-389*)*

W okresie objęty kontrolą w Urzędzie nie zidentyfikowano incydentów związanych z cyberbezpieczeństwem[14].

(akta kontroli str. 359, 364)

Na stronie BIP Urzędu[15] udostępniono informację dotyczące cyberbezpieczeństwa, wraz z odnośnikami do innych serwisów o tej tematyce, w tym www.cert.pl czy gov.pl. Ostatnią aktualizację strony przeprowadzono 28 listopada 2022 r.

(akta kontroli str. 391)

5. W okresie objętym kontrolą nie dokonano klasyfikacji procesów i zasobów informatycznych Urzędu. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 4, 139, 347, 356, 359, 360-361, 364)

[14] Rozumianym jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

[15] https://bip.nowewarpno.pl/artykul/cyberbezpieczenstwo.

6. Urząd nie posiadał procedury otworzenia danych z kopii zapasowych, a stosowane metody tworzenia i przechowywania kopii zapasowych znacząco zwiększały ryzyko ataku typu ransomware i potencjalnej utraty danych co zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 4, 10, 17-132, 242, 263, 357-389)

7. W okresie objętym kontrolą Urząd nie zlecał tworzenia kopii zapasowych i odtwarzania utraconych zasobów podmiotom zewnętrznym.

(akta kontroli str. 5, 139-140, 242, 263, 360-361, 366-- 389)

8. W Urzędzie w latach 2019-2023 (do zakończenia czynności kontrolnych) nie przeprowadzano testów odtwarzania utraconych zasobów. Natomiast podmiot obsługujący Urząd w zakresie informatyki nie wykonywał okresowego testowego odtwarzania z kopii zapasowych.

(akta kontroli str. 5, 139-140, 242, 263, 360-361, 366-389)

Burmistrz wyjaśnił: *Nie przeprowadzano testów odtwarzania utraconych zasobów ze względu na brak zakupu środowiska testowego, a co za tym idzie nie możemy odtworzyć całego systemu od zera. Natomiast możemy odtworzyć poszczególne bazy danych z kopii zapasowych.*

(akta kontroli str. 5, 139-140).

9. W okresie objętym kontrolą Urząd zawarł pięć umów ubezpieczeniowych, w ramach których przedmiotem ubezpieczenia był:

- stacjonarny i przenośny sprzęt elektroniczny,
- zewnętrzne nośniki danych,
- dane i oprogramowanie,

w zakresie nagłej, nieprzewidzianej i niezależnej od woli ubezpieczającego utraty, zniszczenia lub uszkodzenia wskutek ubezpieczonych zdarzeń oraz zwiększone koszty działalności[16] pod warunkiem, że powstały one w następstwie zdarzeń powodujących szkodę w ubezpieczonym sprzęcie.
Kwota ubezpieczenia obejmowała wartość odtworzeniową ubezpieczonego sprzętu elektronicznego na podstawie wykazu sprzętu przygotowanego przez Urząd, koszty zewnętrznych nośników danych oraz danych i oprogramowania do 30 000 zł oraz zwiększone koszty działalności do 30 000 zł.

(akta kontroli str.5, 140, 150-171)

Stwierdzone nieprawidłowości

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

1. Niezgodność obowiązującego od 24 maja 2018 SZBI z normą PN-ISO/IEC 27001 w zakresie:

- niezaplanowania szczegółowych działań mających na celu zapewnienie bezpieczeństwa informacji;
- nieprzypisania odpowiedzialności administratora do wykonywania przeglądów i konserwacji;
- braku określenia administratora;
- braku zdefiniowania występujących w urzędzie procesów;
- braku określenie kryteriów akceptacji ryzyka;
- braku określenia zasad i osób odpowiedzialnych za przegląd polityki bezpieczeństwa informacji;
- braku separacji obowiązków (zadań) krytycznych;
- braku regulacji dotyczących obecności koniecznej;

[16] Koszty mające na celu uniknięcie lub zmniejszenie zakłóceń w prowadzeniu działalności.

- braku regulacji w zakresie uświadamiania, kształcenia i szkolenia z zakresu bezpieczeństwa informacji;
- nieokreślenia zasad przeglądu i analiz ryzyka SZBI;
- braku szczegółowej procedury zgłaszania wystąpienia lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji oraz obsługi incydentu.

Powyższe stanowiło naruszenie § 20 ust. 3 KRI, zgodnie z którym *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą.*

(akta kontroli str. 4-5,10, 17-132, 139-149, 216-227, 236-242, 260-264, 344-347, 351-352, 356-390)

Burmistrz wyjaśnił: *W Polityce Ochrony Danych Osobowych z 2018 r. zbyt ogólnie opisano część zagadnień, a część poprzez przeoczenie pominięto. W wyniku dalszej analizy tych zapisów wprowadzono szereg zmian w zaktualizowanej dokumentacji z września 2022 roku.*

(akta kontroli str. 358-359, 363)

2. Niewprowadzenie aktualizacji obowiązującego w Urzędzie SZBI w formie zarządzenia burmistrza, co było niezgodne z § 129 ust. 1 w zw. z § 141 Rozporządzenia Prezesa Rady Ministrów w sprawie „Zasad Techniki Prawodawczej" z dnia 20 czerwca 2002 r.[17]. Zgodnie z ww. przepisami, zarządzenie można zmieniać zarządzeniem późniejszym, wydanym na podstawie tego samego, nadal obowiązującego przepisu upoważniającego, przez organ, który wydał zarządzenie zmieniane (…).

Opracowana w Urzędzie Polityka bezpieczeństwa informacji oraz Instrukcja zarządzania systemem informatycznym zostały zatwierdzone przez Burmistrza kolejno 6 września 2022 r. i 3 kwietnia 2023 r. poprzez ich podpisanie. Nie zostały one natomiast wprowadzone w formie zarządzenia burmistrza. Jednocześnie wskazać należy, iż nadal obowiązuje Zarządzenie Burmistrza z nr 032/2018 z 24 maja 2018 r.

(akta kontroli str. 17-132, 240, 261)

Burmistrz wyjaśnił: (…) *uaktualnienia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym zostały wprowadzone poprzez zapoznanie pracowników z nową dokumentacją. Faktycznie błędnie oceniono, że ta forma będzie wystarczająca. Po kontroli zostanie przeprowadzona aktualizacja dokumentacji zgodnie z zaleceniami i zostanie wprowadzona Zarządzeniem, jednocześnie zostaną określone w tym zarządzeniu dokumenty które przestaną obowiązywać.*

(akta kontroli str. 240, 261)

3. Niezgodność Aktualizacji SZBI z normą PN-ISO/IEC 27001 w zakresie:
   - braku zdefiniowania występujących w urzędzie procesów;
   - braku określenia zasad i osób odpowiedzialnych za przegląd polityki bezpieczeństwa informacji;
   - nieokreślenia zasad przeglądu analiz ryzyka SZBI.

Powyższe było niezgodne z § 20 ust. 3 KRI, zgodnie z którym *wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą*.

[17] Dz.U. z 2016 r., poz. 283 t.j.

(akta kontroli str. 4-5,10, 17-132, 139-149, 216-227, 236-242, 260-264, 344-347, ,351-352, 356-390)

Burmistrzy wyjaśnił: *Procesy służące ochronie informacji, a także zasoby podlegające tej ochronie zostały szczegółowo opisane w Polityce Bezpieczeństwa Informacji. Obejmują one:*

- *Zarządzanie ryzykiem: Identyfikacja, ocena i leczenie ryzyka związanego z bezpieczeństwem informacji.*
- *Kontrola dostępu: Zarządzanie dostępem do informacji i systemów informacyjnych.*
- *Ocena skuteczności kontroli: Regularna ocena i przegląd wdrażanych środków bezpieczeństwa.*
- *Zarządzanie incydentami bezpieczeństwa: Procedury odpowiedzi na naruszenia bezpieczeństwa informacji.*
- *Ciągłość działania: Planowanie i implementacja procedur zapewniających ciągłość działania i odzyskiwanie informacji.*
- *Szkolenia i świadomość pracowników: Edukowanie pracowników w zakresie bezpieczeństwa informacji.*

Chronione zasoby określono w załączniku nr 5 do PBI, na które składają się:

- *Personel: Pracownicy odpowiedzialni za wdrażanie i utrzymanie SZBI.*
- *Technologie: Oprogramowanie, sprzęt i infrastruktura IT wspierająca bezpieczeństwo informacji.*
- *Informacji: Zasoby danych, które są chronione.*
- *Finansowanie: Budżet potrzebny do utrzymania i poprawy SZBI.*
- *Środowisko fizyczne: Bezpieczne obiekty i sprzęt do przechowywania i przetwarzania informacji.*
- *Zewnętrzni dostawcy i partnerzy: Usługi i wsparcie od zewnętrznych dostawców.*

Za prowadzenie dokumentacji urzędu oraz jego sprawne działanie wyznaczono Sekretarza, co zostało określone w Regulaminie Organizacyjnym Urzędu. Za skuteczne funkcjonowanie systemu zarządzania bezpieczeństwem informacji w tym danych osobowych odpowiada Kierownik Jednostki. Wszelkie zmiany/aktualizacje procedur wykonywane są na podstawie sprawozdań z wykonanych audytów wykonywanych przez Inspektora Ochrony Danych (…).

(akta kontroli str.359, 364)

Zdaniem NIK przedstawione przez Burmistrza wyjaśnienia nie pozwalają na uznanie, że Aktualizacja SZBI spełnia wymagania określone w normą PN-ISO/IEC 27001. W zakresie braku zdefiniowania występujących w organizacji procesów wskazać należy, iż zgodnie z postanowieniami ogólnymi ww. normy wpływ na treść funkcjonującego w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji mają m.in. procesy funkcjonujące w organizacji, a sam system powinien być częścią tych procesów[18]. Ponadto Burmistrz powinien zapewnić zintegrowanie wymagań ww. systemu z procesami występującymi w organizacji[19]. W Urzędzie nie zidentyfikowano wszystkich procesów w nim występujących, a jedynie jak wskazał Burmistrz procesy służące ochronie informacji.

W zakresie wyjaśnień Burmistrza dot. braku określenia zasad i osób odpowiedzialnych za przegląd polityki bezpieczeństwa informacji wskazać należy, iż zgodnie z normą PN-ISO/IEC 27001 Audyt wewnętrzny[20] i przegląd zarządzania[21] nie są tożsamymi pojęciami. Audyt wewnętrzny powinien być bowiem

[18] Punkt 0.1 normy PN-ISO/IEC 27001.

[19] Punkt 5.1.b. normy PN-ISO/IEC 27001.

[20] Punkt 9.2. normy PN-ISO/IEC 27001.

[21] Punkt. 9.3 normy PN-ISO/IEC 27001.

przeprowadzany w zaplanowanych odstępach czasu, w celu dostarczenia informacji, czy System Zarządzania Bezpieczeństwem Informacji jest zgodny z własnymi wymaganiami organizacji, oraz ww. normą ISO. Ponadto audyt powinien dostarczać informację, czy system został skutecznie wdrożony i jest utrzymywany, a przeglądy powinny być przeprowadzane przez najwyższe kierownictwo (np. Burmistrza), w zaplanowanych odstępach czasu, w celu zapewnienia jego (Aktualizacji SZBI) stałej przydatności, adekwatności i skuteczności. W Aktualizacji SZBI wskazano, iż *Do zadań Administratora należy regularne mierzenie, testowanie i ocena skuteczności środków technicznych o organizacyjnych, które mają zapewnić ochronę przetwarzania danych osobowych. W tym celu należy przeprowadzać regularne audyty w zakresie bezpieczeństwa informacji i ochrony danych osobowych.* Mając na uwadze powyższe zauważyć należy, że w Aktualizacji SZBI przegląd jest równoznacznych z przeprowadzeniem audytu, co stoi w sprzeczności z normą PN-ISO/IEC 27001.

Natomiast w zakresie analizy ryzyka wskazać należy, iż na etapie czynności kontrolnych przedłożono jedynie wyniki analizy ryzyka, natomiast w Aktualizacji SZBI nie zawarto regulacji wymaganych normą PN-ISO/IEC 27001[22], w tym m.in. kryteriów ryzyka (akceptacji i szacowania); zapewniających spójne, poprawne i porównywalne wyniki kolejnych szacowań ryzyka; identyfikację ryzyka w bezpieczeństwie informacji; pozwala na analizę i ocenę ryzyka w bezpieczeństwie informacji.

(akta kontroli str. 17-132, 141-149, 236-242, 260-263, 267-336, 347, 356-365)

4. Przypisanie w SZBI i Aktualizacji SZBI 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 (Ogólne Rozporządzenie o Ochronie Danych)[23] .

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. 17-132, 141-149, 236-242, 260-263, 267-336, 347, 356-365)

Burmistrz wyjaśnił: *Audyt polityk Ochrony Danych Osobowych oraz Bezpieczeństwa Informacji był realizowany we wspólnym zespole z Inspektorem Danych Osobowych ze względu na jego merytoryczną wiedzę z tego zakresu, którą wykorzystywano. Oceniono, że Inspektor ochrony danych może prowadzić także audyty wewnętrzne w zakresie bezpieczeństwa informacji, jeżeli posiada w tym zakresie odpowiednią wiedzę oraz kompetencję, a przeprowadzanie audytów nie będzie negatywnie wpływać na realizowanie jego obowiązków wynikających z przepisów o ochronie danych osobowych. (…). Audyt wymagany przepisami KRI jest przeprowadzany w szerszym zakresie, niż audyt zgodności z RODO, więc IOD będzie mógł podjąć się tego zadania, jedynie jeżeli posiada w tym zakresie odpowiednią wiedzę i kompetencję, a samo zadanie nie będzie powodowało konfliktu interesów, np. weryfikowania procesów, w które zaangażowany jest IOD.*

Faktycznie działania te nie powinny powodować aby zakres zadań podlegający audytowi był realizowany przez podmiot, który niejako sam odpowiada za ich realizację. Zostanie to uwzględnione w przyszłej działalności.

(akta kontroli str. 240-241, 261-262)

[22] Określonych w pkt 6.1.2.

[23] Dz.Urz.UE.L nr 119, str. 1, dalej: RODO.

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. 17-132, 141-149, 236-242, 260-263, 267-336, 347, 356-365)

5. Niewyznaczenie w Urzędzie w okresach od 28 sierpnia 2018 r. (daty wejścia w życie KSC) do dnia 12 czerwca 2022 r. osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Ponadto 30 kwietnia 2023 r. rozwiązano umowę o pracę z osobą pełniącą ww. funkcję i zawarto z nią umowę zlecenia, która nie obejmowała swoim zakresem utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, powyższy brak został usunięty w wyniku czynności kontrolnych NIK 21 listopada 2023 r. Powyższe 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. 4, 10, 133-137, 239, 260, 265)

Burmistrz wyjaśnił: *Obowiązki Burmistrza przejąłem z dniem 21.11.2018r. Nie miałem świadomości, że nie została w gminie wyznaczona osoba do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Po ujawnieniu tego faktu w czerwcu 2022r. taką osobę Zarządzeniem nr 050/2022 z dnia 13.06.2022r. wyznaczono. Uznano, że (…) będzie nadal wyznaczony do utrzymywania kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Natomiast przeoczono fakt, że Zarządzenie wewnętrzne nie jest obowiązujące dla osoby zatrudnionej na umowę zlecenie. Aneksem umowy z dnia 21.11.2023r. uzupełniono ten brak.*

(akta kontroli str. 239, 260)

6. Niezapewnienie skutecznego systemu monitorowania zdarzeń w ramach systemów IT. W trakcie czynności kontrolnych NIK Urząd przedstawił informację, że w okresie podlegającym kontroli nie zidentyfikowano żadnych incydentów bezpieczeństwa informacji wymagających zgłoszenia, zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.

Na podstawie opinii Biegłego z przeprowadzonych badań ustalono, że osoby odpowiedzialne za obsługę informatyczną Urzędu nie analizowały zdarzeń w ramach modułu IPS (Intrusion Prevention System). Tym samym brak stwierdzonych w ww. rejestrze incydentów mógł wynikać z braku monitorowania tego typu zdarzeń w ramach systemów IT.

Powyższe było niezgodne z § 20 ust. 2 pkt 4 KRI, który stanowi, iż *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.*

(akta kontroli str. 4, 10, 17-132,138, 366-386, 389)

Burmistrz wyjaśnił: *Nie przypisano odpowiedzialności w zakresie weryfikacji systemów służących do weryfikacji incydentów w związku ze zbyt ogólnymi sformułowaniami umowy i przyjęciem, że wszystkie zadania związane*

z zabezpieczeniem i funkcjonowaniem sieci będą wykonywane przez podmiot z którym podpisano umowę.

(akta kontroli str. 386, 389)

7. Niezapewnienie skutecznego systemu zarządzania incydentami z zakresu bezpieczeństwa informacji. Na podstawie opinii Biegłego z przeprowadzonych badań ustalono, iż o ile zasady opisane w dokumencie Polityka bezpieczeństwa informacji, w rozdziale V. "Incydenty" odnosiły się do bezpieczeństwa informacji, to ich treść koncentrowała się na danych osobowych, co mogło prowadzić do sytuacji, w której pracownicy Urzędu interpretowali te zasady jako dotyczące wyłącznie danych osobowych, pomijając inne rodzaje chronionych informacji, zgodnie z wymaganiami KRI oraz KSC. Koncentracja wyłącznie na danych osobowych w ramach PBI i nieuwzględnienie pełnego spektrum chronionych informacji w procesach identyfikacji i reagowania na incydenty bezpieczeństwa informacji mogła ograniczać skuteczność Urzędu w zapobieganiu i reagowaniu na różnorodne zagrożenia cybernetyczne i naruszenia bezpieczeństwa.

Ponadto w ww. regulacjach nie zawarto informacji o niezbędności komunikacji z właściwym CSIRT, celem zgłaszania incydentów określonych KSC, co mogło prowadzić do opóźnionego reagowania na incydenty bezpieczeństwa informacji oraz pogłębienie skutków ich wystąpienia.

(akta kontroli str. 4, 10, 17-132, 138, 366-389)

Burmistrz wyjaśnił: *Dokument "Polityka Bezpieczeństwa Informacji" obejmuje zasady ochrony danych osobowych i bezpieczeństwa informacji, w tym procedury postępowania w przypadku naruszeń bezpieczeństwa, zarządzanie dostępem do informacji oraz audyty bezpieczeństwa. Ponadto określa wymogi dotyczące poufności, integralności, dostępności, autentyczności i odpowiedzialności w procesie przetwarzania danych i wymiany informacji. W rozdziale V opisano procedurę na wypadek wystąpienia incydentów zagrażających bezpieczeństwu danych i informacji.*

Dodatkowe procedury w powyższym zakresie opisano w rozdziale VI „Regulamin ochrony Danych". Procedury te mają na celu zapewnienie niezbędnej wiedzy w zakresie bezpieczeństwa danych osobom przetwarzającym dane. Dotyczy to przede wszystkim pracowników, którzy mają dostęp do danych w formie papierowej i w systemach informatycznych. Sekcja dotycząca incydentów związanych z naruszeniem bezpieczeństwa informacji wskazuje na obowiązek niezwłocznego powiadamiania pracodawcy o każdym zdarzeniu, które może wskazywać na naruszenie bezpieczeństwa informacji. Wymienione są różne typy incydentów, w tym zdarzenia losowe (takie jak pożary, kradzieże, awarie sprzętu IT), a także umyślne działania (kradzież danych, wycieki informacji, działania wirusów). Podkreślona jest konieczność reagowania w sytuacjach, które mogą wskazywać na naruszenie bezpieczeństwa, takich jak ślady włamania, podejrzane zachowanie osób w jednostce, czy próby wyłudzenia danych.

(akta kontroli str. 385, 389)

8. Niesklasyfikowanie przez Urząd w okresie objętym kontrolą krytyczności procesów i zasobów informatycznych, szczególności nie dokonano zidentyfikowania krytycznych danych i operacji. 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[24] – *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*

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

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.

(akta kontroli str. 4, 139, 347, 356, 359-361, 364)

Burmistrz wyjaśnił: *Urząd nie posiada w formie dokumentu klasyfikacji krytyczności procesów i zasobów. Ze względu na bardzo mały urząd, pojedyncze stanowiska merytoryczne (zaledwie 14 w całym urzędzie), małą ilość wykorzystywanych programów, przy bieżącej obsłudze informatycznej oceniono, że określenie hierarchii procesów nie wpływa bezpośrednio na szczególne formy zabezpieczeń. Wszystkie dane są chronione.*

(akta kontroli str. 359, 364)

9. Nieopracowanie w okresie objętym kontrolą przez Urząd planu odtworzenia utraconych 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.* Ponadto zgodnie pkt A.12.2.1 zawartego w załączniku A do normy PN-ISO/IEC 27001 – *Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przez szkodliwym oprogramowaniem (…).*

Urząd w okresie objętym kontrolą nie posiadał procedury ani dokumentacji pozwalającej na odtworzenie utraconych zasobów, tj. obejmującą: resetowanie parametrów systemu; instalację łatek; ustalenie ustawień konfiguracji; dostępności dokumentacji systemu i procedur operacyjnych; ponowną instalację oprogramowania i systemu; dostępność najnowszych kopii zapasowych; testy systemu.

Dodatkowo kopie były wykonywane na macierzach dyskowych, przechowywanych w tej samej szafie co serwer Urzędu. Przedstawiony sposób zarządzania kopiami zapasowymi, chroni kopie zapasowe tylko przed ewentualnymi awariami mechanicznymi dysków. Brak kopii zapasowej, przechowywanej w trybie off-line (np. na nośnikach danych), prowadzić może do ryzyka utraty dostępu do wszystkich danych w przypadku infekcji ransomware, która może doprowadzić do zaszyfrowania macierzy dyskowej oraz serwerów.

(akta kontroli str. 5, 139-140, 242, 244-256, 263, 360-361, 366-389)

Na podstawie opinii Biegłego z przeprowadzonych badań ustalono, że kopie zapasowe wykonywane są zgodnie z ustalonym harmonogramem na urządzenia klasy NAS (Network-Attached Storage). Kopia danych z serwerów trafia jako przyrostowa kopia na Synology, natomiast pliki i programy trafiają na macierz QNAP. Zarówno urządzenie Synology jak i QNAP znajdują się w tym samym pomieszczeniu, a nawet w szafie serwerowej co same serwery. Pozostają też one spięte ze sobą, tak by zapewnić funkcjonalność automatycznej kopii. Tym samym Urząd nie posiada kopii w tzw. off-line, co stwarza ryzyko skutecznego ataku typu ransomware.

Powyższe było niezgodne 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.

Ponadto zgodnie z pkt 5.5 Instrukcji zarządzania systemem informatycznym obowiązującej w Urzędzie (“Nośniki zawierające kopie zapasowe, których celem jest zapewnienie możliwości przywrócenia działania i odtworzenia danych po awarii lub innym zdarzeniu o charakterze katastroficznym, winny być przechowywane w innych lokalizacjach niż lokalizacja jednostki, przy jednoczesnym spełnieniu wszystkich

zasad bezpiecznego przechowywania, dających gwarancję ich zabezpieczenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem oraz gwarancję pełnej dostępności na wypadek konieczności ich wykorzystania w celu przywrócenia lub odtworzenia działań jednostki"),

(akta kontroli str. 139-140, 244-256, 286, 360-361, 366-384, 389)

Burmistrz wyjaśnił: *Podejście do odtworzenia utraconych zasobów było oparte o ocenę wewnętrzną możliwości odtwarzania zasobów w razie potrzeby w oparciu o backup. Nie stworzono w tym zakresie pisemnej procedury ze względu na brak złożoności czynności w takim przypadku*.

Dotychczasowe kopie zapasowe są zapisywane na urządzeniach Synology i QNAP jako kopie przyrostowe, co minimalizuje ryzyko utraty danych w atakach typu ransomware. Kopie off-line kluczowych danych (np. baza danych oprogramowania księgowego) zostaną wdrożone w najbliższym czasie.

(akta kontroli str. 357, 362, 386, 389)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w badanym zakresie.

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 obowiązującego w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji 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 12 czerwca 2022 r. w Urzędzie nie było wyznaczonej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. 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 urzędu do zapewnienia bezpieczeństwa teleinformatycznego.

Opis stanu faktycznego

1. W okresie objętym kontrolą nierzetelnie przeprowadzono w Urzędzie analizę rodzajów ryzyka mogących mieć wpływ na elementy infrastruktury informatycznej, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 5, 140, 17-132, 141-149, 228-235, 239-242, 260-262, 359, 364-365)

W opisie podjętych działań minimalizujących zagrożenie w przypadku zalania, powodzi i pożaru na zewnątrz budynku wskazano, że podejmowanie działań nie jest konieczne, zaś w przypadku pożaru wewnątrz budynku, że redukcja ryzyka nastąpi poprzez regularny przegląd systemów przeciwpożarowych.

(akta kontroli str. 17-132, 359, 364-365)

W przypadku zagrożenia powodzią lub podtopieniami główne elementy infrastruktury (serwer) zostały zabezpieczone poprzez umieszczenie ich na środkowej kondygnacji budynku.

(akta kontroli str. 244-256)

2. Urząd posiadał zabezpieczenie w przypadku przerw w dostawie prądu w postaci bateryjnych urządzeń podtrzymujących napięcie (UPS), które były podłączone przy każdym stanowisku komputerowym oraz przy serwerze. Urząd nie

posiadał innego awaryjnego zasilania w przypadku przerw w dostawie prądu. Urząd nie posiadał procedury działania w przypadku awarii zasilania.

(akta kontroli str. 5,140, 242, 263, 337)

W okresie objętym kontrolą jednostka nie prowadziła rejestru działalności konserwacyjnej i serwisowej dla urządzeń UPS. Nie przeprowadzano testów urządzeń UPS. Zgodnie z wyjaśnieniami Burmistrza baterie w urządzeniach UPS były systematycznie wymieniane w latach 2019-2022, w tym również w ramach programu „Cyfrowa Gmina" w listopadzie 2022 r. Urząd nie był jednak w stanie przedstawić informacji o dacie wymiany baterii w konkretnym urządzeniu. Burmistrz oświadczył, że w przypadku pojawienia się zakłóceń w działaniu urządzenia pracownik zgłasza ten fakt informatykowi.

(akta kontroli str. 242, 263, 337)

3. W okresie objętym kontrolą w Urzędzie nie prowadzono kontroli ruchu osób wchodzących i wychodzących z budynku. Burmistrz wyjaśnił: *W urzędzie nie wprowadzono kontroli ruchu poprzez służby ochrony. Podyktowane to jest tym, że ze względu na bardzo małą gminę (ok. 1500 mieszkańców), również ilość interesantów w ramach bezpośredniego kontaktu jest stosunkowo mała. Ze względu na niski budżet występują redukcje w zatrudnieniu pracowników merytorycznych, a taka ochrona rodziłaby dodatkowe koszty.*

(akta kontroli str. 5, 17-132, 140, 257-258, 344-345, 352)

W Urzędzie wprowadzono Zarządzeniem Burmistrza nr 032/2018[25] politykę kluczy, ale nie była ona przestrzegana, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5, 17-132, 140, 257-259, 344-345, 352)

W okresie objętym kontrolą w Urzędzie nie uregulowano kwestii dostępu do pomieszczeń zawierających główne elementy infrastruktury (serwer) przez podmioty obce, jak również nie określono zasad ich wizytowania, ponadto pomieszczenia te nie były zabezpieczone w sposób minimalizujący nieuprawniony dostęp, a jedyny wyłącznik zasilania znajdował się w miejscu ogólnodostępnym, o czym szerzej w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 244-256, 345, 352-353, 355, 358, 363)

Na podstawie przeprowadzonych 20 listopada 2023 r. oględzin ustalono, iż pomieszczenia zawierające główne elementy infrastruktury nie były widocznie oznaczone, w szczególności nie zamieszczono oznaczeń na drzwiach pomieszczenia gdzie znajduje się serwer, ani nie umieszczono takiej informacji na planach ewakuacji znajdujących się w ciągach komunikacyjnych.

(akta kontroli str. 244-256)

4. W okresie objętym kontrolą w Urzędzie nie zostały określone wykazy umiejętności dla poszczególnych stanowisk. Wymagane umiejętności były każdorazowo określane przy ogłoszeniu o naborze na wolne stanowisko i w zakresie umiejętności informatycznych dla stanowisk pracy z komputerem wskazano je jako wymagania dodatkowe związane ze stanowiskiem i określono jako: *znajomość obsługi komputera (w tym pakietu Microsoft Office)* lub *znajomość obsługi komputera (w tym pakietu Microsoft Office, poczta elektroniczna)*.

(akta kontroli str. 172, 242-243, 263, 338)

[25] Załącznik nr 2 do rozdziału V Regulaminu Ochrony Danych Osobowych w Urzędzie Gminy Nowe Warpno.

W Urzędzie w latach 2019-2023[26] nie został określony plan szkoleń pracowników.

(akta kontroli str. 243, 263-264)

W okresie objętym kontrolą pracownicy uczestniczyli w trzech szkoleniach zawierających elementy tematyki cyberbezpieczeństwa, a udział w nich wzięło 75% obecnie zatrudnionych osób na stanowiskach pracy z komputerem. Nie były to jednak szkolenia odnoszące się bezpośrednio do zagrożeń i procedur związanych z cyberbezpieczeństwem, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 5, 140, 172-197, 243, 263-264)

Z 16 osób pracujących w Urzędzie na stanowisku pracy z komputerem w dniach 1 grudnia 2023 r. i 4 grudnia 2023 r. 12 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 48,3%, z czego najniższy wynik wyniósł 33,3%[27], a najwyższy 60%[28]. W wyniku szczegółowej analizy udzielonych odpowiedzi ustalono, iż na 22 pytania (73% zadanych) mniej niż połowa testowanych udzieliła poprawnych odpowiedzi, tj. w przypadku:

- jednego pytania poprawnej odpowiedzi udzieliła jedna osoba;
- pięciu pytań poprawnej odpowiedzi udzieliły dwie osoby;
- sześciu pytań poprawnej odpowiedzi udzieliły trzy osoby;
- dwóch pytań poprawnej odpowiedzi udzieliły cztery osoby;
- sześciu pytań poprawnej odpowiedzi udzieliło pięć osób.

Wśród pytań, na które udzielono najmniej poprawnych odpowiedzi znalazły się m.in. pytania dotyczące:

- identyfikacji, czy konto w serwisie internetowym zostało przejęte przez cyberprzestępcę – cztery osoby odpowiedziały poprawnie;
- reakcji na podejrzanie wyglądającą wiadomość e-mail z załącznikiem – trzy osoby odpowiedziały poprawnie;
- tworzenia bezpiecznego hasła – dwie osoby odpowiedziały poprawnie;
- identyfikacji, czy na komputerze znajduje się wirus – dwie osoby odpowiedziały poprawnie;
- identyfikacji ataku typu phishing – trzy osoby odpowiedziały poprawnie.

(akta kontroli str. 172, 337, 392-394)

5. Na podstawie oględzin pięciu stanowisk pracy ustalono, że na stanowiskach pracy w widocznych miejscach nie było zamieszczonych danych do logowania. Pracownicy logujący się do systemu stosowali hasło o długości zgodnej z procedurami oraz potrafili zablokować komputer. Czterech pracowników dokonywało tego przez kliknięcie start → zasilanie → uśpij, a jeden przez określoną w SZBI kombinację przycisków Windows + L.

(akta kontroli str.244-256)

6. W okresie od 1 października 2011 r. do 31 marca 2023 r. Urząd zatrudniał pracownika na stanowisku informatyka. Po ustaniu stosunku pracy z ww. pracownikiem zawarto z nim umowę o świadczenie usług w zakresie obsługi informatycznej, która miała obowiązywać od 1 kwietnia 2023 r. do 31 grudnia 2023 r.

[26] Do dnia zakończenia czynności kontrolnych.
[27] W dwóch przypadkach.
[28] W jednym przypadku.

Równolegle do ww. umowy Urząd zawarł umowę na obsługę informatyczną z innym podmiotem na okres od 1 kwietnia 2023 r. do 30 czerwca 2024 r.

Zadania zatrudnionego do 31 marca 2023 r. w Urzędzie informatyka z zakresu bezpieczeństwa informacji były określone w Regulaminie Organizacyjnym Urzędu Gminy w Nowym Warpnie oraz w zakresie obowiązków i obejmowały m.in.:

1) nadzór nad ochroną systemów i sieci teleinformatycznych przetwarzających informacje niejawne w gminie,
2) nadzór nad wprowadzeniem zaleceń Służb Ochrony Państwa dotyczących bezpieczeństwa teleinformatycznego,
3) prowadzenie dokumentacji dotyczącej bezpieczeństwa teleinformatycznego,
4) opracowanie szczegółowych zaleceń dotyczących ochrony fizycznej systemów i sieci teleinformatycznych,
5) opracowywanie indywidualnych haseł dostępu, comiesięczna ich zmiana oraz przechowywanie kopii haseł,
6) kontrolę poprawności wprowadzonych przez użytkowników systemu indywidualnych haseł dostępów.
7) instalację nowego sprzętu komputerowego i oprogramowania.

(akta kontroli str. 5, 11, 140, 198-203, 239, 260, 265, 345, 352)

Od 1 kwietnia 2023 r. zadania podmiotów, z którymi zawarto umowy na świadczenie usług informatycznych, zostały określone w treści tych umów. W przypadku umowy o świadczenie usług z osobą, która wcześniej pracowała na stanowisku informatyka, zadania z zakresu bezpieczeństwa informacji były tożsame z określonymi w Regulaminie Organizacyjnym i zakresie obowiązków. Natomiast w przypadku umowy z drugim podmiotem obejmowały one m.in.:

1) administrację siecią LAN w Nowym Warpnie, składającą się: z 15 końcówek klienckich Windows 10, iOS, i do 25 urządzeń sieciowych w tym switchy, drukarek, telefonów voip itp.,
2) administrację serwerem (MS Windows 2019 Server),
3) administrację macierzą dyskową iSCSI wraz nadzorem nad systemem kopii zapasowej,
4) tworzenie na potrzeby urzędu baz danych oraz administrowanie istniejącymi bazami danych,
5) administrację serwerem Windows,
6) administrowanie sieciami wewnętrznymi LAN, zgodnie z zaleceniami,
7) administrowanie kontrolerem domeny, usługami (Active Directory, GPO, DNS, VLAN),
8) administrowanie bazami danych MySql,
9) administrowanie bazami danych MSSql,
10) administrowanie bazami danych Firebird,
11) administrowanie siecią wewnętrzną zgodnie z polityką bezpieczeństwa, dyrektywami Unii Europejskiej i pozostałymi przepisami na potrzeby Urzędu w Nowym Warpnie,
12) obsługę oprogramowania, aktualizacja, archiwizacja na potrzeby Urzędu,
13) aktualizowanie i prowadzenie polityki prywatności na serwerze Urzędu w oparciu o przepisy dotyczące polityki prywatności instytucji państwowych - Krajowe Ramy Interoperacyjności,
14) administrowanie kontami pocztowymi.

(akta kontroli str. 5, 140, 198, 204, 213, 266, 345, 352, 354)

W okresie objętym kontrolą w Urzędzie nie zostały określone wykazy umiejętności dla pracowników działu informatycznego. Wymagane umiejętności zostały określone przy ogłoszeniu o naborze na wolne stanowisko pracy informatyka. Umiejętności

informatyczne określono jako *znajomość obsługi komputera oraz sieci komputerowej urządzeń preferencyjnych, znajomość problematyki bezpieczeństwa teleinformatycznej* i wskazano je w punkcie *wymagania dodatkowe związane ze stanowiskiem*. Na przedmiotowe ogłoszenie o naborze nie została złożona żadna oferta.

(akta kontroli str. 5, 140, 198, 263, 338-343, 345, 352)

W Urzędzie nie został określony plan szkoleń dla pracowników odpowiedzialnych za cyberbezpieczeństwo.

(akta kontroli str. 243, 263)

Burmistrz wyjaśnił, że *w związku ze znalezieniem podmiotu zewnętrznego nie napotkano trudności w zakresie zabezpieczenia obsługi urzędu pod względem informatycznym.*

(akta kontroli str. 345, 352)

7. W Urzędzie w latach 2019-2021 nie przeprowadzano analiz i nie planowano środków na podnoszenie poziomu cyberbezpieczeństwa, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 5, 140, 240, 261, 344, 351-352, 358, 363)

W okresie objętym kontrolą faktycznie wydatkowano w:

- 2019 r. kwotę 3 038 zł na wymianę sprzętu komputerowego,
- 2020 r. kwotę 479,50 zł na wymianę sprzętu komputerowego,
- 2021 r. kwotę 110,70 na wymianę sprzęty komputerowego,
- 2023 r. kwotę 13 065,30 zł na wymianę sprzętu komputerowego.

(akta kontroli str. 344, 351-352, 358, 363)

W ramach projektu „Cyfrowa Gmina" realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 w ramach pierwszego naboru[29] Gmina otrzymała i wykorzystała 100 tys. zł.

(akta kontroli str.344, 351-352)

W zakresie wykorzystywania zewnętrznych źródeł finansowania Burmistrz wyjaśnił: *Aktualnie trwa analiza potrzeb z zakresu cyberbezpieczeństwa pod kątem ewentualnego skorzystania z programu Rządowego „Cyberbezpieczny Samorząd". Jednak ze względu na określone zasady przy składaniu wniosków i określenie progu minimalnego na dofinansowanie w wysokości 200 000,00 zł , przy braku potrzeb aż na taką kwotę w sytuacji bardzo małego samorządu, występuje okoliczność że może wniosek nie zostać złożony. Jednak mimo to analiza potrzeb zostanie przeprowadzona aby uwzględnić to w przyszłych działaniach.*

(akta kontroli str. 5, 140)

8. Na podstawie opinii Biegłego ustalono, iż pomimo dysponowania odpowiednimi możliwościami i środkami technicznymi Urząd nie zapewnił odpowiedniego stanu zabezpieczeń przed cyberzagrożeniami, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 366-390)

9. Na podstawie opinii Biegłego ustalano, iż Urząd nie posiadał pełnej inwentaryzacji aktywów IT, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 366-390)

10.Na podstawie opinii Biegłego stwierdzono, że w Urzędzie nie stosowano mechanizmów kontrolnych w zakresie identyfikacji wykorzystywania rozwiązań

[29] Ogłoszenie wyników naborów 22 listopada 2022 r. - https://www.gov.pl/web/cppc/cyfrowa-gmina4.

chmurowych przez pracowników Urzędu, co zostało opisane w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 366-390)

11. Na podstawie przeprowadzonych oględzin jednego stanowiska komputerowego ustalono, iż na komputerach służbowych była możliwość zalogowania się na prywatną skrzynkę pocztową[30]. Powyższe zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 349)

Na podstawie pięciu wybranych pism kierowanych z Urzędu do petentów ustalono, iż w każdym przypadku były wskazywane maile służbowe Urzędu, tj. urzad@nowewarpno.pl albo podatki@nowewarpno.pl.

(akta kontroli str. 350)

Stwierdzone nieprawidłowości

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

1. Obowiązywanie w Urzędzie w okresie objętym kontrolą nierzetelnej analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej sporządzonej w ramach załącznika nr 7 do Polityki Ochrony Danych Osobowych z dnia 24 maja 2018 roku.

W przedmiotowej analizie ryzyka zidentyfikowano czynniki środowiskowe, tj.

- zalanie, w przypadku którego prawdopodobieństwo wystąpienia oceniono jako średnie, skutek wystąpienia jako mały (do 10 000 zł), a poziom ryzyka jako akceptowalny.
- powódź, w przypadku której prawdopodobieństwo wystąpienia oceniono jako niskie, skutek wystąpienia jako mały (do 10 000 zł), a poziom ryzyka jako akceptowalny.
- pożar wewnątrz budynku, w przypadku którego prawdopodobieństwo wystąpienia oceniono jako średnie, skutek wystąpienia jako średni (od 1 000 zł do 100 000 zł), a poziom ryzyka jako opcjonalny.
- pożar na zewnątrz budynku, w przypadku którego prawdopodobieństwo wystąpienia oceniono jako średnie, skutek wystąpienia jako mały (do 10 000 zł), a poziom ryzyka jako akceptowalny.

(akta kontroli str. 5, 17-132, 140)

Zauważyć należy, iż w analizie ryzyka przygotowanej na potrzeby obowiązującego w latach 2019-2023 Planu Zarządzania Kryzysowego dla Gminy Nowe Warpno określono, że występuje duże ryzyko wystąpienia powodzi (prawdopodobieństwo wystąpienia: bardzo prawdopodobne, skutki wystąpienia: średnie). Zidentyfikowano ponadto, że powódź miałaby wpływ na zakłócenia funkcjonowania systemów łączności i systemów teleinformatycznych; ograniczenie bądź całkowitą utratę łączności radiowej i telefonicznej; zniszczenia w infrastrukturze wytwarzania, przesyłu lub dystrybucji energii elektrycznej oraz zniszczenia obiektów użyteczności publicznej/lokali mieszkalnych/miejsc pracy. Również ryzyko wystąpienia pożaru wielkopowierzchniowego oceniono jako duże (prawdopodobieństwo wystąpienia: prawdopodobne, skutki wystąpienia: duże), a pożar miałby wpływ na zniszczenia w infrastrukturze przesyłu lub dystrybucji energii elektrycznej przechodzących przez tereny leśne.

(akta kontroli str. 228-235)

[30] W trakcie oględzin pracownik zalogował się na pocztę służbową - poczta.wp.pl.

Powyższą analizę ryzyka należy określić jako nierzetelną z uwagi na ocenę skutków wystąpienia ww. czynników środowiskowych jako mały (do 10 000 zł) w przypadku zalania, powodzi lub pożaru na zewnątrz budynku, bądź średni (od 1 000 zł do 100 000 zł) w przypadku pożaru wewnątrz budynku. W sytuacji, gdy mamy do czynienia ze zdarzeniami rodzącymi jedne z najbardziej kosztochłonnych w konsekwencji skutków, ocena ich odpowiednio na kwoty 10 000 zł i 100 000 zł jest nieadekwatna, zwłaszcza, że zgodnie z wyceną dokonaną na potrzeby zawarcia aktualnie obowiązującej umowy ubezpieczenia samą wartość odtworzeniową sprzętu elektronicznego wyceniono na 365 030,40 zł, zewnętrznych nośników danych, danych i oprogramowania na 30 000 zł, do tego dochodzą jeszcze koszty odtworzenia infrastruktury informatycznej.

(akta kontroli str. 5, 17-132, 140, 151-171, 228-235, 241-242, 262, 359, 364-365)

Burmistrz wyjaśnił: *Ocena zidentyfikowanych ryzyk pod kątem Prawdopodobieństwa, Skutków i ryzyka odnosi się do funkcjonowania urzędu.*
- Zalanie: oceniono, w związku z tym że Serwer, macierze dyskowe znajdują się na piętrze urzędu, na którym nie ma instalacji wodociągowej to też znikome jest zagrożenie wystąpienia problemu. Piętro jest również oddzielone poddaszem więc zalanie opadami atmosferycznymi bezpośrednio sieci teleinformatycznej nie jest zagrożone.
- Powódź: oceniono, że czym innym jest zagrożenie powodzią dla gminy w ramach planu Zarządzania Kryzysowego, a czym innym dla samego Urzędu. Plan Zarządzania Kryzysowego obejmuje cały obszar, tereny zalewowe, obszary nisko położone, sam fakt występowania akwenów. Natomiast budynek urzędu położony jest w jednym z najwyższych punktów. Dodatkowo wystąpienie powodzi jest procesem rozłożonym w czasie, umożliwiającym podjęcie dodatkowych działań zabezpieczających lub ewakuacyjnych.
- Pożar na zewnątrz budynku: w bezpośredniej styczności z obiektem Ratusza brak jest innych obiektów budowlanych. Pożar innych elementów np. pojazdu nie rodzi żadnych skutków dla funkcjonowania sieci teleinformatycznej.
(…)
Oceny są subiektywne i prawdopodobnie wcześniej nie doceniono tych ryzyk.
oraz
Skutek wystąpienia pożaru oceniono subiektywnie jako średni, ponieważ wzięto pod uwagę, że pożar może mieć najprawdopodobniej miejscowe wystąpienie oraz że zadziała system alarmowy i zostaną podjęte działania ratowniczo-gaśnicze prowadzące do likwidacji zagrożenia. Wycena do 100 000,00 zł odnosiła się do 2018 roku, gdzie były całkowicie inne koszty odtworzeniowe substancji.

(akta kontroli str. 242, 262, 359, 364-365*)*

Wyjaśnienia Burmistrza wskazujące, że analiza ryzyka uległa dezaktualizacji i nie została zaktualizowana również należy uznać za działanie nierzetelne i sprzeczne z standardem B.7 zawartym w Standardach kontroli zarządczej, stanowiącym, że nie rzadziej niż raz w roku należy dokonać identyfikacji ryzyka w odniesieniu do celów i zadań. W przypadku działu administracji rządowej lub jednostki samorządu terytorialnego należy uwzględnić, że cele i zadania są realizowane także przez jednostki podległe lub nadzorowane. W przypadku istotnej zmiany warunków, w których funkcjonuje jednostka, należy dokonać ponownej identyfikacji ryzyka.

(akta kontroli str. 359, 364-365)

W Załączniku nr 7 do Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Nowym Warpnie nie dokonano oceny wszystkich zidentyfikowanych w analizie rodzajów ryzyka, co również należy uznać za nierzetelne sporządzenie analizy

ryzyka, ponieważ jeżeli zidentyfikowano dane ryzyko, to zgodnie z standardem B.8. Standardów kontroli zarządczej, należy je poddać analizie (Zidentyfikowane ryzyka należy poddać analizie mającej na celu określenie prawdopodobieństwa wystąpienia danego ryzyka i możliwych jego skutków. Należy określić akceptowany poziom ryzyka).

(akta kontroli str. 17-132, 241-242, 262)

Burmistrz wyjaśnił: *w załączniku nr 7 do Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Nowym Warpnie wprowadzonej 24 maja 2018r przypuszczam, że nie dokonano oceny zidentyfikowanych rodzajów ryzyka w pierwotnym dokumencie poprzez przeoczenie. Natomiast wszystkie zidentyfikowane obszary podlegały ocenie i realizowane to było w ramach okresowych analiz ryzyka.*

(akta kontroli str. 17-132, 241-242, 262)

2. Nierzetelne realizowanie od 1 stycznia 2019 do 11 grudnia 2023[31] obowiązków wynikających z wprowadzonej 24 maja 2018 r. Załącznikiem nr 2 do rozdziału V Regulaminu Ochrony Danych Osobowych w Urzędzie polityki kluczy. W szczególności w Urzędzie nie prowadzono ewidencji dostępu (§ 4) do pomieszczeń oraz nie prowadzono ewidencji pobrań kluczy (§ 6). Powyższe działanie zwiększało ryzyko nieuprawnionego dostępu do pomieszczeń zawierających główne elementy infrastruktury.

(akta kontroli str. 5, 17-132, 140, 257-258, 344-345, 352)

Burmistrz wyjaśnił: *W urzędzie nie jest prowadzona ewidencja pobrań kluczy. Urząd jest bardzo mały, w którym funkcjonuje zaledwie 11 pomieszczeń w których mogą być wykonywane czynności urzędnicze. Pracownicy pobierają i zdają klucze do pomieszczeń w sekretariacie. Klucze są przechowywane w przeznaczonej na ten cel skrzynce, a ich wydawaniem zajmuje się pracownik sekretariatu. Skrzynka ta jest zamykana na klucz. Ze względu na fakt, że w urzędzie zatrudnionych jest tylko 13 urzędników nie ma problemu z identyfikacją kto pobiera klucz i do jakiego pomieszczenia. Procedura zarządzania kluczami przy najbliższej aktualizacji dokumentacji zostanie zmieniona i dostosowana do potrzeb.*

(akta kontroli str. 344-345, 352)

NIK zauważa, iż zgodnie z standardem C.13. Standardów kontroli zarządczej *Należy zadbać, aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby. Osobom zarządzającym i pracownikom należy powierzyć odpowiedzialność za zapewnienie ochrony i właściwe wykorzystanie zasobów jednostki.*

(akta kontroli str. 5, 17-132, 140, 257-258, 344-345, 352)

3. Niezabezpieczenie w sposób minimalizujący ryzyko nieuprawnionego dostępu do pomieszczeń, gdzie znajdują się główne elementy infrastruktury informatycznej (serwer i główny wyłącznik prądu) oraz nieokreślenie zasad wizytacji i dostępu do ww. pomieszczeń, co było działaniem nierzetelnym.

Na podstawie przeprowadzonych 20 listopada 2023 r. oględzin ustalono, że pomieszczenie zawierające główne elementy infrastruktury informatycznej (serwer) usytuowane było naprzeciwko schodów prowadzących na piętro z wejściem z holu znajdującego się na piętrze. Do pomieszczenia prowadziły otwarte drewniane drzwi wyposażone w standardowy zamek. Na drzwiach znajdowały się oznaczenia numerów pokoi oraz osób w nich pracujących.

Pomieszczenie to było pokojem przechodnim i zawierało przejście do kolejnego pokoju, w którym znajdowały się trzy stanowiska pracy. W pomieszczeniu zawierającym główne elementy infrastruktury informatycznej znajdowało się stanowisko komputerowe, regały na dokumenty oraz szafa meblowa (bez zamka),

[31] Dzień zakończenia czynności kontrolnych.

w której znajdował się serwer. Szafa meblowa była uchylona, znajdująca się w niej przeszklona szafa serwerowa również była uchylona, a w drzwiach do niej znajdował się klucz. Główny wyłącznik prądu był umiejscowiony na parterze budynku w bocznym korytarzu, do którego prowadziły otwarte drewniane drzwi z zamontowanym standardowym zamkiem. Wyłącznik znajdował się w miejscu ogólnodostępnym, w zamkniętej szafce z kluczem w drzwiczkach.

(akta kontroli str. 244-256, 345, 352-353, 355, 358, 363)

Ponadto w Urzędzie nie uregulowano kwestii dostępu do pomieszczeń zawierających główne elementy infrastruktury informatycznej (serwer) przez podmioty obce, jak również nie określono zasad ich wizytowania.

(akta kontroli str. 345, 352-353)

Burmistrz wyjaśnił: *Podmioty obce nie mają dostępu do pomieszczenia w którym znajduje się serwer. Ewentualni interesanci są przyjmowani wyłącznie w obecności urzędnika.*
W związku z tym, że serwer znajduje się w pomieszczeniu przechodnim do pomieszczenia – miejsca pracy urzędników, to ochrona fizyczna realizowana jest codziennie w związku z pobytem pracowników urzędu. Natomiast firma informatyczna minimum raz w tygodniu dokonuje przeglądu serwera.
Ze względu na bardzo małą ilość pomieszczeń w urzędzie i wskazanie do lokalizacji serwera na piętrze obiektu, na którym usytuowanych jest tylko 6 kancelarii – nie ma możliwości wydzielenia pomieszczenia tylko i wyłącznie na ten cel. Budynek Ratusza jest zabytkowy, co wskazałem w odpowiedzi do Ad.2 (przyp. Ratusz jest obiektem zabytkowym z XVII wieku, wpisanym do rejestru zabytków i ze względu na ochronę konserwatorską nie można dokonywać zmian w jego układzie.) i nie ma możliwości dokonywania jego przeróbek.
Brak możliwości zastosowania klimatyzacji wynika również z zabytkowego charakteru obiektu, braku możliwości umieszczania urządzeń na elewacji budynku.
W budynku znajduje się instalacja alarmowa ppoż. Gmina nie posiadała ani środków finansowych ani zgody konserwatora zabytków na wykonanie instalacji ppoż – gaszenie pożaru. Wewnątrz obiektu również drzwi nawiązują do charakteru budynku Dostępu dla podmiotów zewnętrznych do pomieszczenia nie ma (…). Pracownicy wykonując swoje obowiązki również stanowią ochronę fizyczną dla infrastruktury (…). Ze względów wskazanych (…)(przyp. powyżej) nie ma możliwości wydzielenia pomieszczenia tylko na ten cel. (…)Wyłącznik głównych elementów infrastruktury znajduje się w skrzynce na parterze budynku, która jest zamykana na klucz (znajduje się on w sekretariacie).Szafka jest zamykana na klucz. W dniu oględzin klucz znajdował się w szafce w związku z przygotowaniem do oględzin.

(akta kontroli str. 345, 352-353*)*

NIK zauważa, iż oględziny zostały zapowiedziane w taki sposób, że poinformowano kierownika jednostki, iż oględziny będą obejmowały budynek Urzędu (ze stanowiskami pracy) w zakresie objętym kontrolą – cyberbezpieczeństwo. Z uwagi na brak wcześniejszej wiedzy co do przedmiotu oględzin, Burmistrz nie mógł przygotować się do nich poprzez otworzenie przed oględzinami szafek zawierających wyłącznik głównych elementów infrastruktury.

(akta kontroli str. 355)

Taki stan faktyczny uznać należy za nierzetelne zabezpieczenie pomieszczeń zawierających główne elementy infrastruktury informatycznej, zwiększające ryzyko nieuprawnionego dostępu i niezgodne z powszechnie przyjętymi wytycznymi dotyczącymi pomieszczenia serwerowni (m.in. usytuowanie serwera w oddzielnym pomieszczeniu, ograniczony dostęp do pomieszczenia, w którym znajduje się serwer, zapewnienie odpowiednich warunków środowiskowych w ww. pomieszczeniu m.in. odpowiedniej czystości powietrza, jego wilgotności i temperatury zapewnianych

poprzez instalację klimatyzacji, wyposażenie ww. pomieszczenia w automatyczny system przeciwpożarowy oraz drzwi przeciwpożarowe i antywłamaniowe) oraz ze standardem B.8. w Standardach kontroli zarządczej, który stanowi, że należy zadbać, aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby. Osobom zarządzającym i pracownikom należy powierzyć odpowiedzialność za zapewnienie ochrony i właściwe wykorzystanie zasobów jednostki.

(akta kontroli str. 244-256, 345, 352-353, 355, 358, 363)

4. Niezapewnienie w okresie objętym kontrolą pracownikom szkoleń z zakresu cyberbezpieczeństwa. W latach 2019-2023 pracownicy Urzędu uczestniczyli w czterech szkoleniach z zakresu ochrony danych osobowych. W trzech z tych szkoleń podnoszono elementy tematyki bezpieczeństwa teleinformatycznego, tj. zagadnień dotyczących zabezpieczenia przekazywanych informacji, zagrożeń występujących podczas pracy z komputerem i możliwych do zastosowania zabezpieczeń podczas pracy z komputerem. Pomimo omówienia ww. tematyki szkolenia te nie były wprost nastawione na zagadnienia cyberbezpieczeństwa. W ww. szkoleniach wzięło udział 12 pracowników z 16 obecnie zatrudnionych osób na stanowiskach pracy z komputerem. Zatem czworo (25%) pracowników nie zostało przeszkolonych nawet w najmniejszym zakresie z przedmiotowego zagadnienia. Brak szkolenia, w którym temat bezpieczeństwa teleinformatycznego ujęty byłby w sposób wyczerpujący znajduje swoje odzwierciedlenie w wynikach przeprowadzonego w trakcie czynności kontrolnych testu z tego zakresu. Zatem niezapewnienie pracownikom szkoleń z zakresu bezpieczeństwa teleinformatycznego należy uznać za działanie nierzetelne i niezgodne z § 20 ust. 2 pkt 6 KRI, który stanowi: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: 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*.

(akta kontroli str. 5, 140, 172-197, 243, 263-264)

Burmistrz wyjaśnił: *W ramach szkoleń realizowanych przez IOD były poruszane kwestie związane z bezpieczeństwem teleinformatycznym. Nie było organizowanych natomiast szkoleń wyłącznie poświęconych cyberbezpieczeństwu. W ramach współpracy z obecnym podmiotem obsługującym urząd w zakresie informatycznym wdrażanych jest szereg rozwiązań technicznych i praktycznych. Również tematyka zagrożeń związanych z cyberbezpieczeństwem zostanie poddana bardziej wnikliwej uwadze*.

(akta kontroli str. 243, 264)

5. Niedokonywanie w latach 2019-2021 analizy potrzeb z zakresu cyberbezpieczeństwa i niezapewnianie środków na podnoszenie poziomu cyberbezpieczeństwa, co było działaniem nierzetelnym.

(akta kontroli str. 5, 140, 240, 261, 344, 351-352, 358, 363)

Burmistrz wyjaśnił: *Ze względu na trudną sytuację finansową gminy nie było nadwyżki środków umożliwiającej na większe wydatki inwestycyjne. Oceniono, że stosowane zabezpieczenia w zakresie cyberbezpieczeństwa zapewniają podstawy bezpiecznego działania. Ewentualne wydatki były realizowane na potrzeby, które były identyfikowane na bieżąco. (…).*

(akta kontroli str. 358, 363)

NIK zauważa, iż rzetelnym działaniem Burmistrza byłoby analizowanie potrzeb Urzędu z zakresu cyberbezpieczeństwa, a następnie uwzględnianie (adekwatnie do możliwości finansowych) ich w budżecie miasta. Powyższe pozwalałoby na systematyczne podnoszenie poziomu cyberbezpieczeństwa w Urzędzie, tym bardziej wobec pojawiających się możliwości zewnętrznego finansowania w ramach projektów, tj. Cyfrowa Gmina czy Cyberbezpieczny Samorząd.

6. Niezapewnienie przez Urząd adekwatnych zabezpieczeń przed cyberzagrożeniam. Na podstawie opinii Biegłego ustalono, iż Urząd stosuje wielowarstwowe zabezpieczenia w zakresie różnego rodzaju zagrożeń. W Urzędzie wykorzystywani UTM Fortigate 40F oraz ESET Endpoint Antivirus, które były adekwatne do potrzeb Urzędu.

Jednak pomimo posiadania powyższych rozwiązań Urząd nie wykorzystywał, w tym w zakresie UTM Fortigate 40F nie wdrożył polis z zakresu cyberbezpieczeństwa i nie monitorowano zdarzeń, a w zakresie ESET Endpoint Antivirus nie wszystkie komputery były podłączone do domeny.

Powyższe było niezgodne z § 20 ust. 2 pkt 7 KRI, który stanowi, *iż Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:*
a) monitorowanie dostępu do informacji,
b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

(akta kontroli str. 5, 140, 214-215, 242, 262-263, 347, 356-390)

Burmistrz wyjaśnił: *Ze względów finansowych zastosowano rozwiązania z ograniczonymi możliwościami. Urząd Gminy w Nowym Warpnie złożył wniosek w sprawie pozyskania funduszy w ramach programu „Cyberbezpieczny Samorząd" i liczy na środki, które pozwolą na zakup i zamontowanie dodatkowych urządzeń i modułów w zakresie cyberbezpieczeństwa i monitorowania zdarzeń.*

(akta kontroli str. 386, 390)

Wskazać należy, iż w opinii Biegłego powyższa nieprawidłowość może skutkować:

- unieruchomieniem infrastruktury, komputerów, serwerów, a w rezultacie do przestoju procesów operacyjnych,
- włączeniem komputerów do sieci typu „botnet", która może być wykorzystywana do działań przestępczych sterowanych z zewnątrz,
- ujawnieniem poufnych informacji lub uprawnień do innych systemów (np. systemów bankowych),
- zaszyfrowaniem informacji w celu wyłudzenia środków finansowych (tzw. ransomware),
- innymi skutkami wiążącymi się z ograniczeniem możliwości normalnego biznesowego wykorzystania systemów.

(akta kontroli str. 366-384)

7. Nieposiadanie przez Urząd w okresie objętym kontrolą zinwentaryzowanego środowiska informatycznego. Na podstawie opinii Biegłego z przeprowadzonych badań ustalono, iż przedstawione w trakcie kontroli zestawienie zinwentaryzowanego środowiska informatycznego nie było kompletne. Powyższe wynikało z faktu, iż

wykorzystywane przez Urząd oprogramowanie AXENCE obejmowało swoim działaniem jedynie 10 urządzeń (w Urzędzie było 16 stanowisk pracy z komputerem). Ponadto jednostka nie prowadziła – pomimo iż ww. oprogramowanie na to pozwalało – audytów obejmujących zainstalowane aplikacje pod kątem zgodności z prawem (w aspekcie np. legalności) oraz bezpieczeństwa (w zakresie eliminowania podatności związanych z brakiem wdrożenia nowych poprawek).

Powyższe było niezgodne z § 20 ust. 2 pkt 7 KRI, który stanowi, iż *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:*
a) monitorowanie dostępu do informacji,
b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.
Jak również § 20 ust. 2 pkt 2 KRI, który stanowi, iż *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

(akta kontroli str. 5, 140, 242, 262-263, 347, 356-390)

Burmistrz wyjaśnił: *W Urzędzie Gminy w Nowym Warpnie wszystkie stanowiska są monitorowane fizycznie raz w tygodniu przez informatyków. A stanowiska nie podłączone do oprogramowania przez przeoczenie, zostaną podłączone do programu centralnego zarządzania ESET w najbliższym czasie.*

W związku z kosztami finansowymi urząd zdecydował się w pierwszym etapie na wprowadzenie darmowego programu AXENCE (dla 10 stanowisk) w ramach dokładnego jego przetestowania. Pełna wersja zostanie zakupiona w przypadku uzyskania dofinansowania z projektu „Cyberbezpieczny Samorząd".

(akta kontroli str. 386, 390)

NIK zauważa, iż w opinii Biegłego powyższa nieprawidłowość może skutkować:

- brakiem ich zabezpieczenia oraz brakiem możliwości wychwytywania incydentów oraz reakcji w przypadku ich wystąpienia (np. nielegalne lub podatne na atak oprogramowanie).
- brakiem kontroli nad środowiskiem, pojawiającymi się podatnościami.
- wykorzystaniem przez atakujących i złośliwe oprogramowanie istniejących w systemach podatności.
- trudnościami w utrzymaniu systemów w codziennej eksploatacji.

(akta kontroli str. 366-384)

8. Nieopracowanie procedur i niemonitorowanie przez Urząd wykorzystywania usług chmurowych. W trakcie prowadzonych czynności kontrolnych NIK, Urząd wskazał, że nie korzysta z usług chmurowych. Przeprowadzona przez powołanego w trakcie kontroli biegłego analiza dowodów przekazanych przez Urząd, wykazała jednak, że Urząd korzystał z aplikacji Microsoft Onedrive oraz Azure Data Studio, które są związane usługami chmurowymi. Mimo posiadania przez Urząd urządzenia klasy UTM wyposażonego w moduły umożliwiające filtrowania ruchu z rozwiązaniami np. cloud storage, nie przedstawił dowodów w zakresie monitorowania zdarzeń w tym

obszarze, a więc nie przedstawiono dowodu, że rzeczywiście nie korzystał z danych przetwarzanych w modelu chmurowych. Urząd ponadto nie opracował regulacji, odnoszących się do bezpieczeństwa informacji w relacji z zewnętrznymi dostawcami, w tym dostawcami usług chmurowych oraz nie opracował kryteriów i mechanizmów ich weryfikacji pod względem prawnym i zabezpieczenia informacji, co mogło prowadzić do wielu istotnych ryzyk w kontekście bezpieczeństwa informacji przetwarzanych za pośrednictwem tego dostawcy oraz niezapewnienia odpowiedniej stabilności operacyjnej 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. 5, 140, 358-359, 366-390)

Burmistrz wyjaśnił: *Usługa chmurowa była automatycznie zainstalowana w momencie awarii oprogramowania office 2013 i nie została odinstalowana. Nie jest ona aktualnie wykorzystywana (pracownicy nie mają tam wprowadzonych loginów i haseł).Usługa ta zostanie w najbliższym czasie odinstalowana. To samo dotyczy oprogramowania Azure Data Studio.W urzędzie Gminy Nowe Warpno nie są wykorzystywane usługi chmurowe i w związku z tym nie zakupiono modułu do ich monitorowania. Natomiast usługi chmurowe o których mowa w pkt 7 zostaną odinstalowane.*

(akta kontroli str. 386, 390)

9. Niewyłączenie możliwości korzystania przez pracowników Urzędu z prywatnych skrzynek pocztowych na komputerach służbowych. Powyższe było działaniem nierzetelnym i zwiększało podatność Urzędu na naruszenia cyberbezpieczeństwa.

(akta kontroli str. 349)

Burmistrz wyjaśnił: *Pracownicy urzędu informowani byli o tym aby w czasie wykonywania obowiązków służbowych nie wykonywali czynności prywatnych – w tym mieści się również załatwianie korespondencji prywatnej. Nie oceniono aby niezbędne było całkowite blokowanie skrzynek mailowych. Nie były znane regulacje wprost określające taki zakaz. Natomiast były omawiane kwestie zagrożeń związanych z ewentualnym otworzeniem plików, potencjalnie niebezpiecznych.*

(akta kontroli str. 357, 362)

NIK zauważa, iż zgodnie z zasadami bezpiecznego użytkowania poczty elektronicznej[32], 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.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w badanym zakresie. Negatywną ocenę cząstkową uzasadnia brak przygotowana organizacyjnego i kadrowego do zapewnienie bezpieczeństwa teleinformatycznego. Powyższe potwierdzają stwierdzone nieprawidłowości, w szczególności obowiązywanie w Urzędzie w okresie objętym kontrolą nierzetelnej analizy ryzyka czynników środowiskowych mogących mieć wpływ na elementy infrastruktury informatycznej. Niezabezpieczenie w sposób minimalizujący ryzyko nieuprawnionego dostępu do

[32] Wynikające z 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

pomieszczeń, gdzie znajdują się główne elementy infrastruktury (serwer i główny wyłącznik prądu) oraz nieokreślenie zasad wizytacji ww. pomieszczeń. Niezapewnienie pracownikom szkoleń z zakresu bezpieczeństwa teleinformatycznego. Niewyłączenie możliwości korzystania przez pracowników Urzędu z prywatnych skrzynek pocztowych na komputerach służbowych. Niedokonywanie w latach 2019-2021 analizy potrzeb z zakresu cyberbezpieczeństwa i niezapewnianie środków na podnoszenie poziomu cyberbezpieczeństwa.

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:

Wnioski

1. Zapewnienie zgodności obowiązującego systemu zarządzania bezpieczeństwem informacji z normą PN-ISO/IEC 27001 i KRI.
2. Zapewnienie prawidłowego ustanowienia systemu zarządzania bezpieczeństwem 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. Przypisanie odpowiedzialności w zakresie weryfikacji systemów służących do wykrywania incydentów np. na styku z siecią Internet (na poziomie urządzenia klasy UTM).
6. Opracowanie i wdrożenie skutecznego mechanizmu zarządzania incydentami bezpieczeństwa informacji, w tym schematu zgłaszania incydentów do właściwego CSIRT.
7. Przeprowadzenie klasyfikacji krytyczności procesów i zasobów informatycznych Urzędu.
8. Opracowanie, wdrożenie i przestrzegania planu odtworzenia utraconych zasobów zapewniającego ciągłość działania.
9. Zapewnienie przeprowadzania w analizie ryzyka adekwatnej oceny skutków do zidentyfikowanych rodzajów ryzyka.
10. Zabezpieczenie głównych elementów infrastruktury informatycznej w sposób minimalizujący nieuprawniony dostęp.
11. Zapewnienie przestrzegania istniejącej w Urzędzie polityki kluczy.
12. Zapewnienie pracownikom szkoleń z zakresu cyberbezpieczeństwa.
13. Zapewnienie przez Urząd adekwatnych zabezpieczeń przed cyberzagrożeniami.
14. Zapewnienie posiadania przez Urząd zinwentaryzowanego całego środowiska IT.
15. 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 Burmistrza.
16. Wyłączenie możliwości korzystania przez pracowników z prywatnych skrzynek pocztowych na komputerach służbowych.
17. Zapewnienie przeprowadzania analizy potrzeb z zakresu cyberbezpieczeństwa i środków na ich realizację.

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 wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 30 dni 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, 9 stycznia 2024 r.

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

.....
podpis

Kontrolerzy
Adam Milczarek
Starszy inspektor kontroli państwowej

.....
podpis

Ewelina Kamińska-Nowicka
Specjalista kontroli państwowej

.....
podpis