NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.411.3.3.2023

Krzysztof Szwedo
Wójt Gminy Osina
Urząd Gminy Osina
Osina 62, 72-221 Osina

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 Osina[1], Osina 62, 72-221 Osina
Kierownik jednostki kontrolowanej	Krzysztof Szwedo, Wójt Gminy Osina[2], od dnia 22 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 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	Monika Ratowska, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/174/2023 z dnia 3 listopada 2023 r. (akta kontroli str.1-2)

[1] Dalej: Urząd.

[2] Dalej: Wójt.

[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 wdrożenia i przestrzegania polityki dotyczącej bezpieczeństwa teleinformatycznego. System Zarządzania Bezpieczeństwem nie był zgodny z normą PNEN ISO/IEC 27001. W okresie od dnia 28 sierpnia 2018 r. do dnia 13 lipca 2020 r. Urząd nie posiadał osoby, która byłaby wyznaczona i odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co było niezgodne z treścią art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[6]. Pomimo wyznaczenia osoby do pełnienia punktu kontaktowego dla właściwego CSIRT faktycznego zgłoszenia osoby dokonano w dniu 13 listopada 2023 r., co jest niezgodne z treścią art. 22 ust. 1 pkt 5 KSC. Urząd nie posiadał procedur, które pozwalałyby na zachowanie ciągłości działania.

Powyższą ocenę uzasadnia również negatywne ocenienie przygotowania organizacyjno-kadrowego Urzędu do zapewnienia bezpieczeństwa teleinformatycznego. Pracownicy na swoich stanowiskach pracy z komputerem mieli możliwość korzystania z prywatnej poczty elektronicznej, a podczas oględzin jedna osoba nie miała założonego hasła na swoim komputerze. Co prawda w Urzędzie przeprowadzano akcje edukacyjne, jednakże nie zapewniono pracownikom dostatecznej ilości szkoleń z zakresu cyberbezpieczeństwa.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[7] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1. W Urzędzie procedury regulujące najważniejsze kwestie związane z bezpieczeństwem informacji zostały określone w Zarządzeniu Nr 12/2018 Wójta Gminy Osina[8], w skład którego wchodziły m.in. Polityka Bezpieczeństwa Informacji, Instrukcja Zarządzania systemami informatycznymi w Urzędzie Gminy Osina, wykaz zabezpieczeń RODO. Dokumentacja stanowiła obowiązujący w Urzędzie System Zarządzania Bezpieczeństwem Informacji.[9]

(akta kontroli str. 83-131)

Odnośnie pisemnego harmonogramu przeglądów i aktualizacji Polityki Bezpieczeństwa Informacji Wójt wyjaśnił: *Nie posiadamy pisemnego harmonogramu przeglądów i aktualizacji Polityki Bezpieczeństwa Informacji, jednak te kwestie poruszane są regularnie, nie rzadziej niż raz na kwartał przynajmniej przez informatyka i sekretarza. Potwierdzeniem tego są regularnie dokonywane zakupy sprzętu, który poprawić ma bezpieczeństwo urzędu.*

---

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

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

[7] 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.

[8] Zarządzenie z dnia 14 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Osina zmienione Zarządzeniem Nr 40/2021 z dnia 30 września 2021 r.

[9] Dalej: SZBI.

(akta kontroli str. 450-451)

Obowiązujące w Urzędzie SZBI nie zostało poddane certyfikacji PN-EN ISO/IEC 27001. Wójt wyjaśnił: *Przepisy art. 5 ust.3 ustawy o normalizacji z dnia 12 września 2002 r. (Dz.U. z 2015 r. poz. 1483) stanowią, że stosowanie polskich norm jest dozwolone. W związku z powyższym, a także z uwagi na wysoki koszt, system zarzadzania bezpieczeństwem informacji w Urzędzie Gminy Osina nie został poddany certyfikacji ISO 27001. W zakresie bezpieczeństwa informacji Urząd stosuje się do wymogów przepisów 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 (Dz.U. z 2017r. poz. 2247).*

(akta kontroli str.5-6)

W wyniku szczegółowej analizy SZBI ustalono, że nie był zgodny z normą PN-EN ISO/IEC27001, co stanowiło naruszenie § 20 ust. 3 KRI. Powyższe zostało szczegóły opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 888-889)

2. Urząd 4 czerwca 2018 r. przeprowadził analizę ryzyka, utraty integralności, dostępności lub poufności informacji, która zawierała informacje na temat zagrożeń takich jak: zagrożenia ciągłości działania, danych, błędy ludzkie czy ataki zewnętrzne. Powyższa analiza została poddana aktualizacji 10 września 2019 r., 12 lutego 2020 r., 1 października 2020 r., 14 października 2021 r. oraz 1 grudnia 2022 r.

(akta kontroli str. 17-24)

W trakcie czynności kontrolnych NIK przedłożono dokumentację z przeprowadzenia następujących audytów:

- diagnoza cyberbezpieczeństwa z 1 sierpnia 2022 r.
- sprawozdanie z wykonanego audytu w zakresie ochrony danych osobowych w procesie rekrutacji oraz w okresie zatrudnienia pracowników z 26 października 2021 r.,
- sprawozdanie z wykonanego audytu w zakresie bezpieczeństwa informacji i ochrony danych osobowych z 1 października 2020 r.,
- sprawozdanie roczne 2022 - audyt w zakresie ochrony danych osobowych prowadzenie strony www oraz BIP z 15 grudnia 2022 r.,
- sprawozdanie roczne 2022 - audyt w zakresie ochrony danych osobowych w procesie transmitowania oraz nagrywania obrad Rady Gminy z 15 grudnia 2022 r.,
- sprawozdanie z wykonania audytu w zakresie bezpieczeństwa informacji i ochrony danych osobowych z 2 września 2019 r.

(akta kontroli str. 373-379,919-987)

Odnośnie przeprowadzenia analizy ryzyka utraty integralności, dostępności lub poufności informacji Wójt wyjaśnił: *Ocena ryzyka prowadzona jest dla każdego zidentyfikowanego podczas inwentaryzacji aktywa. W trakcie analizy ryzyka rozpatruje się prawdopodobieństwo wystąpienia zagrożenia, podatność aktywów na zagrożenia oraz skutki potencjalnych zagrożeń. Ponadto należy wziąć pod uwagę następstwa naruszenia lub utraty poufności, integralności i dostępności, które mogą nastąpić w wyniku działań umyślnych, przypadkowych oraz naturalnych.(…)*Wójt wyjaśnił, że *Po wprowadzeniu nowych systemów nie została przeprowadzona analiza ryzyka, ponieważ zaplanowaliśmy ją po uzyskaniu środków z programu Cyberbezpieczny samorząd. W dalszym ciągu jesteśmy w stanie wdrażania nowych systemów zabezpieczeń i po ich zakończeniu przeprowadzimy taką analizę. Na*

podstawie wcześniej przeprowadzonej analizy zakupiony został sprzęt minimalizujący ryzyko. Działania jakie zostały podjęte: zakupiono dysk twardy zewnętrzny do tworzenia kopii zapasowych. Zakupiono NAS do tworzenia kopii zapasowych. Zakupiono UPS do podtrzymania pracy serwera i NASa. Zakupiono komputery z systemem operacyjnym, który posiada wsparcie producenta, Zakupiono program antywirusowy (...), który pomaga zabezpieczyć przed wirusami. Zakupiono UTM (Fortigate) celem zabezpieczenia punktu brzegowego sieci. Zakupiono pakiety MS Office, które posiadają wsparcie producenta.

(akta kontroli str. 5-6, 7-16,17-24, 892)

3. Od dnia 28 sierpnia 2018 r. (daty wejścia w życie KSC) do dnia 13 lipca 2020 r. nie wyznaczono w Urzędzie osoby, która byłaby odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str.891)

Osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa wyznaczono 14 lipca 2020 r., a od dnia 20 lipca 2021 r. funkcję tę pełnił informatyk obsługujący Urząd. W trakcie czynności kontrolnych NIK, tj. 13 listopada 2023 r., Urząd dokonał zgłoszenia osoby kontaktowej do CSIRT NASK, co zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 29-33,132-133,386-388)

Odnośnie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[10] Wójt wyjaśnił: *Do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa wyznaczony został p. D. M. (porozumienie z dnia 14 lipca 2020 r. zmieniające zakres obowiązków pracownika), a następnie p. R. W. (§1 ust.3 pkt m umowy z dnia 20 lipca 2021 r.). Pan D. M. został wyznaczony (...) lecz nie przesłano tego zgłoszenia.*

(akta kontroli str. 5-6,384)

Ze złożonych dokumentów wynika, że wyznaczenie osoby do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa nie obejmowało swoim zakresem zadania publicznego zależnego od systemów informacyjnych realizowanych przez Gminę Osina oraz gminne jednostki organizacyjne.

(akta kontroli str. 385-388)

Odnośnie zgłoszenia osoby wyznaczonej do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa Wójt wyjaśnił: *Zgodnie z § 1 ust. 2 i ust. 3 lit. m umowy Nr SG.1330.1.2023 o Świadczenie Usług Informatycznych usługi świadczone przez pana R.W. „świadczone będą w Urzędzie Gminy Osina, Ośrodku Pomocy Społecznej w Osinie oraz Gminnej Bibliotece Publicznej w Osinie. W zakres usług wchodzić będzie utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wykonywanie innych obowiązków, które na podmiot publiczny nakłada ustawa o krajowym systemie cyberbezpieczeństwa." W zgłoszeniu do CSIRT NASK w punkcie „Nazwa podmiotu" wpisano „Urząd Gminy Osina" jako nazwę podmiotu wiodącego. Do zgłoszenia dołączono również umowę z panem W. Intencją było zgłoszenie wyznaczonej osoby kontaktowej dla wszystkich trzech jednostek podległych i nadzorowanych przez Gminę Osina.*

(akta kontroli str. 893)

4. W Urzędzie procedura związana z postępowaniem, w przypadku naruszenia ochrony danych (incydenty) została określona w rozdziale XI Polityki Bezpieczeństwa

[10] Zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U. 2023 poz.913.

Informacji. Na jej podstawie pracownicy zobowiązani byli do niezwłocznego powiadomienia o naruszeniu ochrony danych (nawet w przypadku, gdy istnieje tylko podejrzenie) Administratora Danych Osobowych. Incydenty i zdarzenia, o których pracownicy byli obowiązani zawiadamiać dotyczyły zewnętrznych zdarzeń losowych (pożar, kradzież), wewnętrznych zdarzeń losowych (awarie sprzętu IT, zgubienie danych, pomyłki informatyków lub samych użytkowników) i umyślnie spowodowanych incydentów (kradzież lub wyciek danych, ujawnienie informacji osobom nieupoważnionym).

(akta kontroli str. 100-101,227-229)

Na dzień 14 grudnia 2023 r. w rejestrze incydentów znajdowały się dwa wpisy, tj. z 20 września 2021 r. i 9 listopada 2023 r., które nie dotyczyły cyberbezpieczeństwa[11].

(akta kontroli str. 227-229, 315)

Odnośnie incydentów, w tym incydentów krytycznych Wójt wyjaśnił: *Incydenty zgłaszane są przez pracowników bezpośrednio administratorowi danych, następnie wpisywane są do rejestru incydentów. W Urzędzie Gminy Osina nie wystąpiły incydenty, które podlegały zgłoszeniu do CSIRT NASK.(...) W rejestrze incydentów odnotowano dwa incydenty. Nie były to incydenty krytyczne.* Wójt wyjaśnił *Pracownicy zgłaszali informatykowi podejrzane wiadomości e- mail, jednak nie są prowadzone statystyki w tym zakresie. W każdym przypadku informatyk przekazywał informację o sposobie dalszego postępowania.*

(akta kontroli str. 100-101,315,451).

Zgodnie z opinią biegłego brak incydentów nie musiał wiązać się z rzeczywistym ich brakiem, ze względu na brak ich monitorowania np. styku z siecią Internet i reakcji na zdarzenia zarejestrowane przez systemy klasy IPS. Urząd zakupił urządzenie klasy UTM (Fortigate), natomiast nie było ono jeszcze podpięte produkcyjnie.

(akta kontroli str. 876-878).

Na stronie BIP Urzędu udostępnione zostały informacje edukacyjne dotyczące cyberbezpieczeństwa wraz z odnośnikami do innych serwisów[12].

(akta kontroli str. 450-451,902-906)

5. W okresie objętym kontrolą jednostka nie opracowała i nie zaimplementowała planu zapewnienia ciągłości działania. Przedłożone na etapie czynności kontrolnych dokumenty nie potwierdzały również zidentyfikowania i udokumentowania krytycznych danych i operacji, co zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 878-880, 917)

6 W Urzędzie nie opracowano planu odtworzenia utraconych zasobów, oraz planu ciągłości działania, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 384)

W sprawie przeprowadzenia testów Odtwarzania utraconych zasobów Wójt wyjaśnił, że *W urzędzie nie ma adnotacji o przeprowadzonych testach odtwarzania utraconych zasobów. Przy zmianie serwera, która odbyła się rok temu przywracane były dane*

[11] Incydenty dotyczyły uszkodzenia dysków na serwerze oraz na stanowisku promocji.

[12] Np. cykl webinariów CEDUR w ramach World Inwestor Week organizowany przez Urząd Komisji Nadzoru Finansowego, który obejmował tematykę „Cyberbezpieczeństwo z perspektywy klienta usług finansowych- aspekty społeczne", „Cyberbezpieczeństwo w kontekście zagrożeń występujących w Internecie, w szczególności oszustw na urządzeniach mobilnych".

z kopii. W tym roku pozyskaliśmy środki na dodatkowe oprogramowanie, na którym będziemy wykonywać raz w roku sprawdzenie kopii, celem weryfikacji.

(akta kontroli str.,917)

W rozdziale V PBI Urząd wdrożył zasady tworzenia kopii zapasowych, na podstawie której *Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o specjalne oprogramowanie (codziennie). Kopie całościowe sporządzane są raz w tygodniu. Przechowywanych jest 12 kopii miesięcznych przez okres roku. Najstarsze kopie są nadpisywane w cyklu rotacyjnym. Kopie sporządzane na serwerze i dysku przenośnym. Dysk przenośny przechowywany jest w sejfie, do którego dostęp maja informatyk i Sekretarz Gminy. Informatyk sprawuje nadzór nad poprawnością wykonania kopii zapasowych na dysku przenośnym. Raz w roku sprawdzana jest poprawność wykonywanych kopii.*

(akta kontroli str. 96-97)

Odnośnie tworzenia kopii zapasowych Wójt wyjaśnił: *Serwerownię posiadamy tylko jedną, natomiast kopie zapasowe trzymamy także poza serwerownią w wyznaczonym miejscu. Nie opracowano szczegółowej procedury odzyskiwania danych. Kopie danych wykonuje informatyk w ramach świadczonych przez siebie usług.*

(akta kontroli str. 892)

7. W okresie objętym kontrolą Urząd nie zlecał tworzenia kopii zapasowych podmiotom zewnętrznym.

(akta kontroli str. 96-97,892)

8. W okresie objętym kontrolą Urząd zawarł pięć umów ubezpieczeniowych, w ramach których przedmiotem ubezpieczenia objęto m.in. sprzęt biurowy (komputery drukarki, faksy, skanery itp.), dane i oprogramowanie. Kwota ubezpieczeniowa obejmowała koszty wprowadzenia danych z kopii zapasowych, koszty ręcznego wprowadzenia danych z dokumentów w formie papierowej oraz koszty poniesione na odzyskanie danych przez wyspecjalizowane firmy z uszkodzonych dysków twardych i wymiennych nośników danych. Ochrona obejmowała również dane znajdujące się wyłącznie w pamięci komputera lub innego sprzętu elektronicznego. Suma ubezpieczenia, w aktualnie obowiązującej umowie, która została zawarta na okres od 1 stycznia 2023 r., do 31 grudnia 2024 r. wynosiła 40 000 zł. Kwota ubezpieczenia pokrywałaby straty majątkowe wynikające z konieczności odtworzenia systemów informacyjnych. Sprzęt biurowy (stacjonarny) ubezpieczono od wszystkich ryzyk na kwotę 150 137,11 zł, natomiast sprzęt biurowy przenośny (laptopy, skanery) ubezpieczono od wszystkich ryzyk na kwotę 263 963,95 zł. Urząd oszacował wartość księgową brutto sprzętu elektronicznego stacjonarnego na kwotę 96 841,57 zł, natomiast sprzętu przenośnego na kwotę 42 206,20 zł.

(akta kontroli str.6, 34-68,520-528,907-908)

Stwierdzone nieprawidłowości

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

1. Niezgodność SZBI z obowiązującą normą PN-ISO/IEC 27001 w zakresie- braku objęcia swoim zakresem struktury organizacyjnej, planowania działania, zasad procedury, procesów i zasobów.

Powyższe jest niezgodne z §20 ust.3 który stanowi, że *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, w tym (...) PN-ISO/IEC 27001 w odniesieniu do ustanawiania zabezpieczeń.

(akta kontroli str.83-131,888)

Wójt wyjaśnił: *Procedury wymagają aktualizacji w tym zakresie.*

(akta kontroli str.888)

2. Niewyznaczenie w Urzędzie w okresie od dnia 28 sierpnia 2018 r. do dnia 13 lipca 2020 r. osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Zgłoszenie osoby kontaktowej do CSIRT NASK wysłano w dniu 13 listopada 2023 r.
Powyższe niezgodne jest z art.21 ust.1 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. 385-388 *)*

Wójt wyjaśnił: *Przed 14 lipca 2020 r. nie wyznaczono osoby do utrzymania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.*

(akta kontroli str. 891)

3. Niezgłoszenie w okresie od 4 sierpnia 2021 r. do 12 listopada 2023 r. osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co stanowiło naruszenie art. 22 ust. 1 pkt 5 KSC. W Urzędzie pomimo wyznaczenia osoby do pełnienia punktu kontaktowego dla właściwego CSIRT faktycznego zgłoszenia osoby dokonano w dniu 13 listopada 2023 r. , co jest niezgodne z treścią art. 22 ust. 1 pkt 5 KSC. *Podmiot publiczny (...) realizujący zadanie publiczne zależne od systemu informacyjnego przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby (...) obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.*

(akta kontroli str.385-388)

Wójt wyjaśnił: *(…) D.M. został wyznaczony w umowie o pracę jako osoba kontaktowa z CSIRT NASK, lecz nie przesłano tego zgłoszenia.*

(akta kontroli str. 384)

4. 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 (…).
Na podstawie opinii biegłego ustalono, że Urząd nie przedstawił dowodów na posiadanie zdolności skutecznego odtworzenia procesów operacyjnych w ustalonych, akceptowalnych ramach czasowych, co wskazuje na potencjalne braki w przygotowaniach na sytuacje awaryjne lub kryzysowe. Ponadto nie przedstawiono dokumentów potwierdzających zidentyfikowania i udokumentowania krytycznych danych i operacji. Umowa zawarta z informatykiem określała wymaganie dotyczące podjęcia czasu interwencji na nagłe awarie, ale bez określonego czasu ich usunięcia.

Usługodawca nie został w umowie zobowiązany wprost do przestrzegania Polityki Bezpieczeństwa Informacji Urzędu.

(akta kontroli str.867-885)

Wójt wyjaśnił: *Aktualnie nie posiadamy pisemnego planu odtworzenia utraconych zasobów. Odtworzenie danych jest możliwe tylko na zasobach zapisanych na serwerze. Tworzona jest kopia zapasowa baz danych wszystkich programów oraz plików zapisanych przez użytkowników w przypisanych dla nich folderach. W Urzędzie nie ma adnotacji o przeprowadzonych testach odtwarzania utraconych zasobów. Przy zmianie serwera, która odbyła się rok temu przywracane były dane z kopii. W tym roku pozyskaliśmy środki na dodatkowe oprogramowanie, na którym będziemy wykonywać raz w roku sprawdzanie kopii, celem weryfikacji. (…) Nie posiadamy pisemnego planu ciągłości działania, natomiast sytuacjach kryzysowych na bieżąco rozwiązujemy problemy związane z zachowaniem ciągłości działania*

(akta kontroli str.316,384,917)

5. Brak przeprowadzenia w latach 2021-2023 nie rzadziej niż raz na rok audytów bezpieczeństwa informacji, co jest niezgodne z treścią §20 ust.2 pkt. 14 KRI zgodnie z którym *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (...) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.* Urząd przedstawił dwa audyty w zakresie bezpieczeństwa informacji i ochrony danych osobowych (audyt rozszerzony o KRI) za wrzesień 2019 r. i październik 2020 r. Audyty były przeprowadzane przez B.K., który na podstawie umowy cywilnoprawnej pełni w Urzędzie rolę IODO.

(akta kontroli str.373-379,996)

Wójt wyjaśnił: *W Urzędzie przeprowadzane były audyty poszczególnych obszarów działania.*

(akta kontroli str.917)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w badanym zakresie. Ocena negatywna uzasadniona jest nieprawidłowością wskazującą na niezgodność obowiązującego w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji z normą PN-EN ISO/IEC 27001. W okresie od dnia 28 sierpnia 2018 r. do dnia 13 lipca 2020 r. W Urzędzie nie było odpowiedzialnej osoby wyznaczonej do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Pomimo wyznaczenia osoby do pełnienia punktu kontaktowego dla właściwego CSIRT, Urząd nie zgłosił w terminie 14 dni osoby kontaktowej. Zgłoszenie zostało wysłane dopiero w dniu 13 listopada 2023 r. Urząd nie posiadał pisemnego planu odtworzenia utraconych zasobów, co wskazuje na potencjalne braki w przygotowaniach na sytuacje awaryjne lub kryzysowe. Ponadto Urząd nie prowadził okresowych analiz ryzyka utraty integralności.

OBSZAR

2. Przygotowanie organizacyjno – kadrowe urzędu do zapewnienia bezpieczeństwa teleinformatycznego.

Opis stanu faktycznego

1. W Urzędzie poddano analizie ryzyka mogące mieć wpływ na elementy infrastruktury informatycznej, a dotyczące m.in. ataków zewnętrznych w postaci pożaru (wewnątrz i na zewnątrz budynku) określając jego prawdopodobieństwo jako niskie (podejmowanie działań nie jest konieczne).

(akta kontroli str. 11,17)

W Urzędzie główne elementy infrastruktury umieszczone zostały w pomieszczeniu piwnicznym. Wokół serwera wybudowano murek mający chronić przed ewentualnym zalaniem. Serwerownia nie była monitorowana przed zalaniem, nad serwerownią nie znajduje się instalacja wodna. Z Gminnego Planu Zarządzania Kryzysowego[13] wynika, że zagrożenie powodzią określono jako małe z uwagi na rzeźbę terenu, na którym znajduje się Gmina oraz niewielką powierzchnię wód.

(akta kontroli str.360,364-372,450,728,891)

2. Urząd posiadał zabezpieczenie w przypadku przerw w dostawie prądu w postaci urządzeń podtrzymujących napięcie (UPS).

(akta kontroli str. 6)

Wójt wyjaśnił: *(…)UPSy, pozwalają na zapisanie pracy i zamknięcie komputerów w przypadku przerw w dostawie prądu..* W sprawie planowanej długości podtrzymywania napięcia Wójt wyjaśnił, *że (...) od 10 do 15 minut. Niestety niektóre UPSy nie podtrzymują pracy komputera przez taki czas, dlatego zaplanowany jest zakup nowych UPSów z projektu Cyberbezpieczny Samorząd.*

(akta kontroli str. 450)

W Urzędzie wykorzystywane są następujące UPS przy komputerach pracowników: Green Cell zasilacz awaryjny UPS 1000VA 600WA Power Proof oraz Green Cell zasilacz awaryjny UPS 600VA 360W Power Proof oraz UPS podtrzymujący pracę serewera: UPS Cyber Power USV 1500VA (OR 1500ERM1U).

(akta kontroli str.909-913)

W Urzędzie główne elementy infrastruktury posiadały dwa wyłączniki zasilania, jeden znajdował się na zewnątrz budynku, a drugi wewnątrz. Wyłączniki były zabezpieczone przed przypadkowym użyciem – były zamykane na klucz, posiadały szybkę.

(akta kontroli str. 5-6,450)

3. Na podstawie przeprowadzonych w dniu 12 grudnia 2023 r. oględzin ustalono, iż główne elementy infrastruktury były należycie zabezpieczone przed nieuprawnionym dostępem, w szczególności poprzez umieszczenie serwerowni w schronie pod budynkiem Urzędu zabezpieczonej metalowymi drzwiami. Drzwi do pomieszczenia zamykane są na pancerne, metalowe drzwi oraz dwie zasuwy.

(akta kontroli str. 355-356,360,364-372)

Odnośnie wskazań dotyczących umieszczenia serwera w pomieszczeniu piwnicznym Wójt wyjaśnił: *Nie posiadamy dokumentów potwierdzających dokonywanie analizy umieszczenia serwerowni w piwnicy, natomiast była ona dokonywana w trakcie ustalenia jej lokalizacji. Został wylany fundament wokół serwera, który zabezpiecza go przed ewentualnym zalaniem. (...) Umieszczenie serwerowni w piwnicy uznane zostało za jego optymalną lokalizację.*

(akta kontroli str. 450,355-356)

W budynku Urzędu nie istniały sformalizowane zasady kontroli ruchu. Powyższe opisane zostało szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.355)

[13] Opracowany przez Wójta Gminy Osina, na podstawie art. 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U.2023 poz.122)

W budynku nie zamieszczono graficznych planów sytuacyjnych, w tym takich, na których były oznaczenia głównych elementów infrastruktury. Pomieszczenie zawierającego główne elementy infrastruktury było zabezpieczone w sposób minimalizujący nieuprawniony dostęp do niego poprzez zamontowanie pancernych, metalowych drzwi zamykanych na klucz i dwie zasuwy.

(*akta* kontroli str.493-498)

4. W Urzędzie nie były opracowane wykazy umiejętności niezbędne dla poszczególnych stanowisk. Wójt wyjaśnił: *Umiejętności pożądane na danym stanowisku pracy określane są w momencie zwolnienia stanowiska pracy i ogłoszenia naboru na to stanowisko. Wówczas określane są wymagania niezbędne oraz wymagania dodatkowe, które spełniać powinni kandydaci składający oferty na to* stanowisko.

(akta kontroli str.210)

W okresie objętym kontrolą pracownicy uczestniczyli w szkoleniu z zakresu cyberbezpieczeństwo przeprowadzonego w ramach projektu grantowego „Cyfrowa Gmina", ponadto w szkoleniu dotyczącym zagadnień związanych z pishingiem, a także Inspektor IODO przeprowadzał szkolenie dla nowych pracowników Urzędu. Powyższe zostało opisane szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 336, 453-470,514,515-519)

13 osób z 16 osób pracujących w Urzędzie na stanowiskach pracy z komputerem poddanych zostało testowi wiedzy z zakresu cyberbezpieczeństwa. Pytania były wielokrotnego wyboru i dotyczyły bezpieczeństwa w sieci, cyberzagrożeń oraz reakcji na przypadki incydentów. Średnio pracownicy rozwiązali test na 62,1%, z czego najniższy wynik wyniósł 36,7%, a najwyższy 83,3%.

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

- szyfrowania plików- cztery osoby udzieliły prawidłowej odpowiedzi.
- podjęcia środków ostrożności na wypadek kradzieży smartfona lub tabletu podejmowanych będąc jeszcze w jego posiadaniu – trzy osoby udzieliły poprawnej odpowiedzi,
- tworzenia bezpiecznego hasła- cztery osoby udzieliły poprawnej odpowiedzi,
- identyfikacji, czy na komputerze znajduje się wirus- jedna osoba udzieliła poprawnej odpowiedzi,
- nieostrożnego korzystania z serwisów społecznościowych- jedna osoba udzieliła poprawnej odpowiedzi.

(akta kontroli str. 442-449)

5. W wyniku przeprowadzonych oględzin pięciu stanowisk pracy z komputerem, ustalono, że w widocznych miejscach pracownicy nie mieli zamieszczonych haseł z danymi do logowania. Wszyscy pracownicy potrafili zablokować komputery. Jeden pracownik nie posiadał hasła do komputera, pozostałe cztery osoby logowały się do systemu poprzez wpisanie hasła zawierającego od sześciu do 11 znaków.

(akta kontroli str.355-356,361,363)

6. Za zapewnienie bezpieczeństwa informatycznego od 20 lipca 2021 r. w Urzędzie odpowiadał zewnętrzny podmiot który świadczył usługi na podstawie umowy cywilnoprawnej[14]. Posiadał on zaświadczenia i certyfikaty potwierdzające jego umiejętności zawodowe m.in. Certyfikat inżyniera Comodo ITSM, uczestnictwa

[14] Umowa o świadczenie Usług Informatycznych SG.1330.1.2021 zawarta 20 lipca 2021 r.

w szkoleniu „Nie daj się cyberzbójom”, a także zaświadczenia potwierdzające odbycie kursów „Praktyczny wireshark”, „Sztuka walki cyberbezpieczeństwa - FortiSOAR”, „FortiEDR/SIEM” „FortiDeceptor”, „FortiRecon”.

Do zadań ww. usługodawcy należało m.in.:

- administrowanie systemami, sieciami informatycznymi, teleinformatycznymi i telefonicznymi, w tym archiwizowanie zasobów elektronicznych,
- wdrażanie nowych systemów informatycznych i teleinformatycznych,
- zabezpieczanie w sprzęt informatyczny i teleinformatyczny oraz jego bieżące utrzymanie, w tym możliwość zabrania komputera celem naprawy poza siedzibą jednostki,
- organizacja szkoleń pracowników w zakresie wykorzystania zainstalowanego sprzętu i oprogramowania komputerowego,
  wsparcie przy obsłudze programów użytkowych,
  ochrona systemów i sieci teleinformatycznych dotyczących informacji niejawnych i współpraca w tym zakresie z Pełnomocnikiem do spraw ochrony informacji niejawnych,
- badanie ewentualnych naruszeń w systemie zabezpieczeń danych,
- utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wykonywanie innych obowiązków, które na podmiot publiczny nakłada ustawa o krajowym systemie cyberbezpieczeństwa,
- diagnostyka problemów i przedstawianie propozycji rozwiązań.

(akta kontroli str.29-33,845-866)

W Urzędzie obsługę informatyczną zapewnia podmiot zewnętrzny Wójt wyjaśnił: *Nie posiadamy informatyka zatrudnionego na umowę o pracę. Obsługę informatyczną świadczy firma zewnętrzna.(…) Zatrudnienie informatyka na umowę o pracę wiąże się z dodatkowymi kosztami ponoszonymi przez pracodawcę. Zawarcie umowy z firmą zewnętrzną uznane zostało za korzystniejsze finansowo, przy zachowaniu tej samej jakości usług. Na rynku nie ma informatyków chętnych do zatrudnienia na umowę o pracę z urzędem, gdyż również dla nich atrakcyjniejsze są cywilnoprawne formy świadczenia usług. (…) Wcześniej był, i jest nadal, informatykiem również w szkole podstawowej prowadzonej przez gminę i jego praca była wysoko oceniana przez dyrekcję szkoły.*

(akta kontroli str. 29-33,316, 512)

7. Wójt wyjaśnił: *Zapotrzebowanie do budżetu na kolejny rok zgłaszają wszyscy pracownicy w zakresie swoich stanowisk, w tym również w zakresie cyberbezpieczeństwa. Jednak wydatki w tym zakresie ujmowane są w budżecie w rozdziale 75023 administracja publiczna wraz z innymi wydatkami nie związanymi z cyberbezpieczeństwem. Nie jest więc możliwe „wydzielenie” kwot przeznaczonych ściśle na cyberbezpieczeństwo.*
W Urzędzie korzystano z zewnętrznego źródła finansowania cyberbezpieczeństwa Wójt wyjaśnił, że *W 2023 r. korzystaliśmy z programu „Cyfrowa gmina” nr POPC.05.01.00-00-001/21-00 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020. Wysokość grantu wynosiła 100.000 zł.* Ponadto Gmina złożyła wniosek do programu rządowego „Cyberbezpieczny Samorząd”.

(akta kontroli str.209,471-488)

W okresie objętym kontrolą na wymianę sprzętu informatycznego, oprogramowanie oraz zapewnienie ciągłości działania wydatkowano:

- w 2019 r. kwotę 3 676,62 zł, 6 339,00 zł oraz 302,00 zł;
- w 2020 r. kwotę 8 904,00 zł, 1 599,00 zł oraz 0 zł;

- w 2021 r. kwotę 39 147,11 zł, 9 559,00 zł oraz 3 522,30 zł;
- w 2022 r. kwotę 3 048,25 zł, 5 629,00 zł oraz 1 676,65 zł;
- w 2023 r. kwotę 33 854,81 zł, 11 711,53 zł oraz 971,70 zł.

(akta kontroli str. 209)

8. Urząd zakupił program antywirusowy, licencja programu została udzielona na 12 miesięcy do dnia 23 lutego 2024 r., a ochroną objętych zostało 30 stanowisk pracy.

(akta kontroli str. 316,389)

9. Na podstawie opinii biegłego ustalono, że Urząd wykorzystywał aplikacje w nieaktualnych wersjach ze znanymi podatnościami (np.7-Zip), gdzie wybrane podatności oznaczone zostały jako krytyczne i umożliwiają np. zdalne wykonanie kodu lub przejęcie kontroli nad systemem. Powyższe zostało szczegółowo opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.882)

W sprawie posiadania zinwentaryzowanego środowiska informatycznego Wójt wyjaśnił, że *Do lipca 2023 r. Urząd posiadał na 4 komputerach system operacyjny Windows 7, który nie posiadał wsparcia producenta. (...) Posiadamy komputery z najnowszym systemem operacyjnym Windows 11, na serwerze Windows Serwer 2022, Microsoft Office 2016,2019 i 2021, które posiadają wsparcie producenta. Posiadamy również umowy, które obejmują aktualizację i wsparcie techniczne następujących programów: Prefeko, Info System, Korelacja.*

(akta kontroli str. 316,384,392-440)

Urząd nie dysponował adekwatną ochroną na warstwie brzegu sieci, ograniczając się do podstawowego routera. Urząd zakupił urządzenie klasy UTM, które ma potencjał znaczącego wzmocnienia bezpieczeństwa sieciowego. Nie dokonano wdrożenia tego urządzenia, w związku z powyższym zabezpieczenie Urzędu sprowadzało się jedynie do hosta końcowego, a na poziomie sieci brakowało dodatkowej warstwy ochronnej.

(akta kontroli str.881)

10. W Urzędzie dotychczas nie korzystano z usług chmurowych. Wójt wyjaśnił, że *Planowany czas wdrożenia chmury wraz z oprogramowaniem od firmy Acronis to grudzień 2023 r. Będzie tam przechowywana kopia danych z serwera.* Odnośnie rozważenia korzystania z prowadzonego przez Ministerstwo Cyfryzacji Systemu Zapewniania Usług Chmurowych wójt wyjaśnił, że *(...) Gmina nie wdrożyła tej usługi. Przyjrzymy się funkcjonalnościom tej usługi i jeśli jest to możliwe rozważymy jej wdrożenie.*

(akta kontroli str. 316-317)

Na podstawie opinii biegłego ustalono, iż Urząd nie opracował regulacji odnoszących się do bezpieczeństwa informacji w relacji z zewnętrznymi dostawcami, w tym dostawcami usług chmurowych, w tym nie opracował kryteriów i mechanizmów ich weryfikacji pod względem prawnym i zabezpieczenia informacji. Mogło to prowadzić do wielu istotnych ryzyk w kontekście bezpieczeństwa informacji przetwarzanych za pośrednictwem tego dostawcy oraz niezapewnienia odpowiedniej stabilności operacyjnej Jednostki kontrolowanej. Ponadto, w ocenie biegłego, brak monitorowania wykorzystywania przez pracowników z aplikacji lub platform pracujących w modelu cloud, mogło doprowadzić do wycieku danych.

(akta kontroli str.884)

11. Na komputerach służbowych istniała możliwość zalogowania się na prywatną skrzynkę pocztową. Odnośnie wykorzystywania prywatnych skrzynek do celów służbowych Wójt wyjaśnił, że *Nie posiada wiedzy na temat wykorzystywania prywatnych skrzynek do celów służbowych. Nie posiada systemu DLP. (...) nie posiada logów, które wskazywałyby próby dostępu do poczty prywatnej.*

(akta kontroli str. 451,909)

Na podstawie pięciu pism skierowanych z Urzędu do petentów ustalono, że w każdym przypadku wskazywane były maile służbowe Urzędu tj. sekretarz@osina.pl, budownictwo@osina.pl finanse1@osina.pl

(akta kontroli str. 499-511)

Stwierdzone nieprawidłowości

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

1. Nieokreślenie w Urzędzie w okresie objętym kontrolą zasad wizytowania pomieszczeń zawierających główne elementy infrastruktury. Powyższe oceniane jest jako działania nierzetelne, które zwiększa podatność Urzędu na zagrożenie cyberbezpieczeństwa.

(akta kontroli str.529)

Odnośnie zasad wydawania kluczy do pomieszczeń Wójt wyjaśnił: *Obecnie nie posiadamy procedur określających zasady dostępu do pomieszczeń i postępowania z kluczami. Pracownicy zostali zaznajomieni z zasadami bezpieczeństwa na wstępnych szkoleniach organizowanych przez Inspektor Ochrony Danych Osobowych[15]. IODO i Sekretarz na bieżąco kontrolują zachowania pracowników względem bezpieczeństwa dostępu do pomieszczeń.* Ponadto Wójt wyjaśnił, że *Klucze do pomieszczeń biurowych pobierane są przez pracowników urzędu ze skrzynki znajdującej się w sekretariacie. Po zakończeniu pracy są one tam odkładane. Skrzynka posiada kod, który znany jest jedynie pracownikom urzędu.* W sprawie dostępu do pomieszczeń przez podmioty obce Wójt wyjaśnił, że *Sprzątanie urzędu, w tym pomieszczenia, w którym zlokalizowana jest serwerownia, przeprowadzane jest przez pracownika Urzędu Gminy Osina, nie przez zewnętrzne firmy sprzątające*. (…) *Klucze od pomieszczeń piwnicznych, które znajdują się w serwerowni znajdują się u Sekretarza Gminy, który wydaje je informatykowi. Jeśli z pomieszczeń skorzystać chcą inne osoby odbywa się to przy obecności sekretarza lub informatyka. (...) Nie określono zasad wizytowania pomieszczeń w Urzędzie. Biura, w których pracują urzędnicy Urzędu Gminy Osina, są dostępne dla interesantów w godzinach pracy urzędu. Oczywiście wstęp do tych pomieszczeń jest możliwy podczas obecności pracowników. Podczas ich nieobecności biura są zamykane na klucz.*

(akta kontroli str.316-317, 355,357,362,369, 370,450, 529)

2. Niezapewnienie w okresie objętym kontrolą pracownikom systematycznych szkoleń z zakresu cyberbezpieczeństwa, co było niezgodne z § 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 następujących działań: zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich*

[15] Dalej: IODO.

(akta kontroli str.336,-337,473,514).

Odnośnie planu szkoleń dla pracowników Wójt wyjaśnił, że *potrzeby szkoleniowe zgłaszane są na bieżąco przez pracowników w miarę pojawianie się nowych zagadnień/ obowiązków, które wymagają pozyskania nowej wiedzy. (...) Wszystkim pracownikom przesłano na adresy mailowe szkolenie dotyczące zasad współpracy z Inspektorem Ochrony Danych Osobowych.- w 2022 r. odbyło się szkolenie zagadnień związanych z phishingiem, przesłano także na maila szkolenie dotyczące zasad współpracy z IODO,- w 2019 r. pracownikom przesłano materiał szkoleniowy dotyczący najważniejszych zasad przetwarzania danych osobowych. Informacje podnoszące wiedzę pracowników w zakresie danych i cyberbezpieczeństwa przekazywane są na adresy e mail pracowników przez IODO. Dotyczą takich zagadnień, jak tworzenie bezpiecznego hasła, cyberbezpieczeństwo w sieci, przypadki naruszenia danych i ataków na inne urzędy nowe obowiązki związane z RODO, sposoby zabezpieczania danych itp. W poszczególnych latach ich ilość przedstawiała się następująco: w 2023 r.- 10 maili, w 2022 r. – 10 maili, w 2021 r. – 4 maile, w 2020 r.- 2 maile, w 2019 r.- 10 maili.*

(akta kontroli str.210,318-351,453-470, 473, 512,514)

W okresie objętym kontrolą 21 pracowników wzięło udział w szkoleniu dotyczącym zagadnień związanych z phishingiem, w szkoleniu z zakresu cyberbezpieczeństwa zorganizowanego w ramach projektu „Cyfrowa Gmina". Dodatkowo Urząd prowadził wobec swoich pracowników kampanie edukacyjne.. Powyższe w ocenie NIK jest niewystarczającą realizacją obowiązku zapewnienia szkoleń pracownikom, tym bardziej wobec pojawiających się zagrożeń w zakresie cyberbezpieczeństwa. Ponadto NIK zauważa, iż przesyłanie materiałów szkoleniowych nie może zostać uznane za realizację ww. obowiązku.

(akta kontroli str. 473,514)

3. . Wykorzystywanie aplikacji w nieaktualnych wersjach, np.: 7-Zip, WinRar Firebird, które posiadały podatnościami, w tym podatności krytyczne i które umożliwiały np. zdalne wykonanie kodu lub przejęcie kontroli nad systemem. Ponadto ustalono, że Urząd korzystał z różnego rodzaju aplikacji służących dom przejęcia kontroli nad komputerem, w różnych wersjach - TeamViewer Any Desk.

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. 882)

Odnośnie wykorzystywania nieaktualnych aplikacji Wójt wyjaśnił, że *W wykazie oprogramowania, które otrzymał biegły, zostały zawarte wszystkie programy, które były oraz są zainstalowane -na naszych komputerach. Aktualnie na żadnym komputerze w Urzędzie Gminy nie jest zainstalowany WinRar. Jeżeli chodzi o Firebird, to firma obsługująca urząd będzie robić aktualizację w lutym br. Program 7-Zip, jak i reszta zainstalowanych programów, zostaną zaktualizowane do nowszych wersji.*

(akta kontroli str.917)

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.

4. Niewyłączenie możliwości korzystania przez pracowników Urzędu z prywatnych skrzynek pocztowych na komputerach służbowych. W ocenie NIK powyższe działanie jest nierzetelne i zwiększało podatność Urzędu na zagrożenie cyberbezpieczeństwa. NIK zauważa, że zasady bezpiecznego użytkowania poczty elektronicznej[16], wskazują, że komputerów służbowych nie powinno używać się do spraw prywatnych (w szczególności do czytania prywatnej poczty elektronicznej). Powyższe działanie może narażać Urząd na otworzenie wiadomości zawirusowanych. Należy wskazać, że Urząd nie obejmuje swoimi zabezpieczeniami prywatnych skrzynek pocztowych swoich pracowników.

(akta kontroli str.998)

Odnośnie objęcie zabezpieczeniami prywatnych skrzynek pocztowych Wójt wyjaśnił, że *Nie były blokowane strony Internetowe, ponieważ nie posiadaliśmy urządzenia, które mogłoby nam to zapewnić. Od nowego roku zostanie wdrożone urządzenie, które będzie blokowało strony internetowe.*

(akta kontroli str. 891)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia działalność Urzędu w zakresie przygotowania organizacyjnego i kadrowego do zapewnienia bezpieczeństwa teleinformatycznego. W badanym okresie pracownicy nie mieli zapewnionych systematycznych szkoleń z zakresu cyberbezpieczeństwa. Nie określono zasad wizytowania pomieszczeń zawierających główne elementy infrastruktury. Nie wyłączono 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:

Wnioski

1. Zapewnienie zgodności obowiązującego systemu zarzadzania bezpieczeństwem informacji z normą PN-EN ISO/IEC 27001.
2. Zapewnienie aktualności danych oraz terminu zgłoszenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
3. Opracowanie planu odtworzenia utraconych zasobów, w tym dokonanie zidentyfikowania i udokumentowania krytycznych danych i operacji.
4. Zapewnienie przeprowadzania corocznych audytów oraz zapewnienie braku konfliktów interesów audytora prowadzącego audyt systemu zarzadzania bezpieczeństwem informacji.

[16] 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

5. Zapewnienie pracownikom systematycznych szkoleń z zakresu cyberbezpieczeństwa.
6. Zapewnienie zasad wizytowania pomieszczeń zawierających główne elementy infrastruktury.
7. Stosowanie procedur systematycznego monitorowania i zarządzania aktualizacjami oprogramowania.
8. 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 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, 12 stycznia 2024 r.

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

.....
podpis

Kontroler
Monika Ratowska
Główny specjalista kontroli państwowej

.....
podpis
podpis