SG. 1710.1.2024

URZĄD MIEJSKI
w Koronowie
BIURO PODAWCZE OTRZYMAŁO
23. WRZ. 2024
zał. ..... data ..... nr 28512/24
podpis .....

NAJWYŻSZA IZBA KONTROLI
DELEGATURA W BYDGOSZCZY

LBY.410.12.4.2024

Pan
Patryk Mikołajewski
Burmistrz Koronowa
Urząd Miejski w Koronowie
Plac Zwycięstwa 1
86-010 Koronowo

WYSTĄPIENIE POKONTROLNE

P/24/004 Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Koronowie[1], Plac Zwycięstwa 1, 86-010 Koronowo
Kierownik jednostki kontrolowanej	Patryk Mikołajewski, Burmistrz Koronowa[2] od 7 listopada 2018 r.
Zakres przedmiotowy kontroli	Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w urzędzie i ich stosowanie
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia kontroli[3] (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina)
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 Bydgoszczy
Kontroler	Tomasz Klause, doradca techniczny, upoważnienie do kontroli nr LBY/88/2024 z 22 maja 2024 r. (akta kontroli str.1-4)

[1] Dalej: „Urząd".
[2] Dalej: „Burmistrz".
[3] Tj. do 13 września 2024 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie prawidłowo opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji[6]. Właściwie zidentyfikowano wszystkie zbiory danych Urzędu podlegające zabezpieczeniu oraz prowadzono pełną inwentaryzację zasobów informatycznych obejmującą ich rodzaj i konfigurację. Inspektorowi Ochrony Danych[7] umożliwiono wykonywanie obowiązków w sposób niezależny. Prawidłowo w okresie objętym kontrolą, szacowano ryzyka w zakresie bezpieczeństwa teleinformatycznego. Zabezpieczenia techniczne systemów informatycznych, przyjęte w Urzędzie zapewniały ochronę przetwarzanych informacji przed nieuprawnionym dostępem. Pomieszczenie serwerowni posiadało odpowiednie zabezpieczenia. Prawidłowo tworzono i przechowywano kopie zapasowe zbiorów danych, programów i oprogramowania systemowego zapewniające ciągłość działania systemu informatycznego. Prawidłowo opracowano i wdrożono zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego przy pracy zdalnej. Podejmowano prawidłowe działania w celu zapobiegania incydentom bezpieczeństwa informacji.

Za nieprawidłowe uznano:

- nieopracowanie planu odtworzeniowego oraz nieokreślenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych,
- nieprzestrzeganie Procedury kontroli dostępu do informacji obowiązującej w Urzędzie w zakresie likwidacji kont użytkowników,
- brak procedur monitorowania pojemności pamięci masowych (dysków twardych) istotnych z punktu widzenia zachowania ciągłości działania serwerów.

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

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. W Urzędzie zidentyfikowano zbiory danych podlegających zabezpieczeniu. Zbiorom danych przypisano odpowiednie poziomy ochrony, zgodne z ich rangą.

(akta kontroli str.72-81, 161-196)

1.2. Urząd posiadał opracowany i wdrożony SZBI, o którym mowa w § 19 ust. 1 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[9]. Nadrzędny dokument SZBI stanowiła Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Koronowie[10]. W ramach PBI ustanowiono instrukcje i procedury:

---

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

[6] Dalej: „SZBI".

[7] Dalej: „IOD";

[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] Dz.U. z 2024 r. poz. 773, dalej: „rozporządzenie KRI".

[10] Stanowiąca załącznik nr 1 do Zarządzeniem Burmistrza Koronowa nr OR-S.0050.157.2016 z 12 grudnia 2016 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Koronowie. Obowiązująca w toku kontroli wersja nr 4 z 17 grudnia 2020 r. Dalej: „PBI"

- Procedury kontroli dostępu do informacji[11],
- Ewidencja i klasyfikacja systemów informatycznych[12],
- Procedura tworzenia kopii zapasowych[13],
- Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji[14],
- Procedura zarządzania ryzykiem w bezpieczeństwie informacji[15],
- Instrukcja w zakresie profilaktyki antywirusowej[16],
- Instrukcja pracy na stanowisku wyposażonym w monitor i drukarkę[17],
- Zasady funkcjonowania wewnętrznego monitoringu budynków Urzędu (wyciąg z regulaminu pracy)[18],
- Instrukcja określająca zasady zabezpieczenia pomieszczeń i budynków Urzędu[19],
- Politykę ochrony danych osobowych w Urzędzie Miejskim w Koronowie[20].

Opracowanie i aktualizacje PBI powierzono Zespołowi ds. Bezpieczeństwa Informacji[21], w którego skład wchodzili:

- Inspektor Ochrony Danych (przewodniczący zespołu),
- Sekretarz Gminy,
- Kierownik Wydziału Organizacyjnego,
- Pełnomocnik ds. Ochrony Informacji Niejawnych,
- Inspektor Bezpieczeństwa Teleinformatycznego,
- Administratorzy Systemu.

Polityka bezpieczeństwa, wraz z ww. procedurami i instrukcjami, została zatwierdzona przez Burmistrza oraz przedstawiona do zapoznania się i stosowania pracownikom Urzędu.

(akta kontroli str. 52-160)

1.3. Sporządzone w Urzędzie dokumenty, polityki oraz procedury dotyczące ochronnych danych osobowych zawierały wymogi określone w art. 24 i art. 25 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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)[22]. Dokumentacja została zatwierdzona przez Burmistrza i zakomunikowana pracownikom Urzędu.

(akta kontroli str.135-160)

1.4. W okresie objętym kontrolą w Urzędzie przeprowadzono szacowanie ryzyka w zakresie bezpieczeństwa teleinformatycznego zgodnie z obowiązującą PZR. W dokumencie zostały ujęte ryzyka i zagrożenia dotyczące zachowania ciągłości działania systemów informatycznych.

---

[11] Załącznik nr 1 do PBI. Dalej „PKDI".
[12] Załącznik nr 2 do PBI. Dalej „EKSI".
[13] Załącznik nr 3 do PBI. Dalej „PKZ".
[14] Załącznik nr 4 do PBI. Dalej „PZI".
[15] Załącznik nr 5 do PBI. Dalej „PZR".
[16] Załącznik nr 6 do PBI. Dalej „IPA".
[17] Załącznik nr 7 do PBI.
[18] Załącznik nr 8 do PBI.
[19] Załącznik nr 9 do PBI.
[20] Załącznik nr 10 do PBI. Dalej „PDO".
[21] W Urzędzie jako Administratora Bezpieczeństwa Informacji powołano zespół. Dalej: „ZBI";
[22] Dz. Urz. UE. L 2016 Nr 119, str. 1, ze zm., dalej: „RODO".

(akta kontroli str.100-113,209-248)

1.5. W Urzędzie nie sporządzono odrębnej dokumentacji zawierającej polityki ciągłości działania.

Burmistrz wyjaśnił, że aspekty związane z zapewnieniem ciągłości działania są integralną częścią obowiązującej w jednostce PBI. W ramach PBI wdrożono szereg procedur, które skutecznie wspierają zachowanie ciągłości działania Urzędu. Do najważniejszych z nich należą: PKZ – regularne tworzenie kopii zapasowych krytycznych danych zapewnia ich dostępność w przypadku awarii lub innych zdarzeń losowych, PZI – zawiera wytyczne dotyczące identyfikacji, oceny i odpowiedzi na incydenty bezpieczeństwa, co pozwala na szybkie przywrócenie normalnego funkcjonowania Urzędu po wystąpieniu incydentu, PZR – systematyczna identyfikacja i ocena ryzyk związanych z bezpieczeństwem informacji oraz wdrażanie odpowiednich środków kontroli minimalizujących te ryzyk, co bezpośrednio wpływa na zdolność Urzędu do kontynuowania działalności.

Burmistrz nadmienił, że pozostałe procedury i polityki zawarte w PBI mają na celu zabezpieczenie infrastruktury informatycznej, ochronę przed zagrożeniami oraz zapewnienie zgodności z wymogami prawnymi. Procedury zaprojektowano tak, aby minimalizować ryzyko zakłóceń w działalności Urzędu i wspierać jego nieprzerwaną pracę. W konsekwencji tego podejścia aspekty związane z ciągłością działania są kompleksowo ujęte w ramach zintegrowanego SZBI.

1.6.-1.7. W okresie objętym kontrolą w Urzędzie nie sporządzono planu zachowania ciągłości działania oraz planów odtworzeniowych. Nie określono również akceptowalnego czasu przywrócenia ciągłości działania dla poszczególnych systemów informatycznych. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 163-171)

1.8. PBI oraz powiązane z nią dokumenty podlegały corocznym przeglądom Ostatni przegląd miał miejsce 21 grudnia 2023 r.

(akta kontroli str. 215-239, 779)

1.9. W okresie objętym kontrolą, zgodnie z PBI, nadzór nad bezpieczeństwem informacji oraz zapewnieniem ciągłości działania powierzono ZBI (o którym mowa w pkt 1.2). Do zadań Zespołu należało: monitorowanie funkcjonowania mechanizmów bezpieczeństwa informacji, właściwe postępowanie z incydentami związanymi z bezpieczeństwem informacji i przypadkami naruszenia zasad bezpieczeństwa informacji, dokonywanie corocznych przeglądów PBI i SZBI, opracowanie zmian w stosowanych dokumentach, procedurach i infrastrukturze technicznej. Członkowie zespołu posiadali odpowiednie kwalifikacje do realizacji powierzonych im zadań.

(akta kontroli str. 52-62, 992-1046)

1.10. Wykonywanie funkcji IOD w Urzędzie zostało powierzone, na podstawie umowy zlecenia, Audytorowi Wewnętrznemu Urzędu. IOD realizował zadania określone w art. 39 RODO. Osoba pełniąca ww. funkcję posiadała odpowiednie kwalifikacje zawodowe.

(akta kontroli str. 989-999)

1.11. Osoba wykonująca funkcję IOD, jak również Audytora Wewnętrznego w strukturze organizacyjnej Urzędu podlegała bezpośrednio Burmistrzowi, co zapewniało wykonywanie obowiązków w sposób należyty, niepowodujący konfliktów interesów.

(akta kontroli str. 5-51)

1.12. W kontrolowanym okresie Urząd dopełnił obowiązku wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[23] określonego w art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dane osoby wyznaczonej przekazano do Zespołu Reagowania na Incydentu Bezpieczeństwa Komputerowego prowadzonego przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z zachowaniem ustawnego terminu[24].

(akta kontroli str.202-208)

1.13. PBI nie definiowała wymogów odnośnie sporządzenia dokumentów wykonawczych. Wszystkie dokumenty, do których się odwoływała stanowiły załączniki do dokumentu głównego.

(akta kontroli str. 52-160)

1.14. Oględziny zapisów dla 15 urządzeń w oprogramowaniu inwentaryzującym zasób sprzętu informatycznego Urzędu[25] wykazały, że Urząd posiadał aktualne informacje o zasobie, tj. m.in. nazwę, numer inwentarzowy, numer seryjny, typ i model, system operacyjny, lokalizację, komponenty oraz nazwę użytkownika, zgodne ze stanem faktycznym. Dane odpowiadały zapisom w kartotece środków trwałych Urzędu.

(akta kontroli str.338-387)

1.15. Gmina Koronowo przystąpiła do programu *„Cyberbezpieczny Samorząd"*. Umowę o powierzenie grantu podpisano 16 maja 2024 r. Zakładała ona wydatkowanie w terminie 24 miesięcy dofinansowania w kwocie 850,0 tys. zł na poprawę cyberbezpieczeństwa w Urzędzie Miejskim w Koronowie oraz jednostkach podległych w obszarach organizacyjnym, kompetencyjnym i technicznym, tj. m.in. opracowanie, wdrożenie, przegląd i aktualizację SZBI, audyt zgodności z wymogami KRI, szkolenia z zakresu cyberbezpieczeństwa pracowników nie technicznych, kadry kierowniczej i osób odpowiedzialnych za utrzymanie i rozwój SZBI oraz szkolenia specjalistyczne dla pracowników IT, wymianę serwera i rozbudowę macierzy dyskowej, wymianę przełączników sieciowych, budową klastra UTM, zastosowanie systemu antywirusowego z funkcją firewall (EDR lub XDR), wykonanie testów penetracyjnych w Urzędzie i jednostkach podległych.

Cele i efekty projektu określono miernikami odnoszącymi się m.in. do liczby przeszkolonych pracowników, liczby systemów służących zwiększeniu poziomu bezpieczeństwa informacji, liczby podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST.

(akta kontroli str.795-797, 809-888)

Stwierdzone nieprawidłowości

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

1. W okresie objętym kontrolą w Urzędzie nie sporządzono dokumentacji zawierającej plany zachowania ciągłości działania i plany odtworzeniowe oraz nie określono akceptowalnego czasu przywrócenia ciągłości działania dla poszczególnych systemów informatycznych, co uznano jako nierzetelne.

---

[23] Zgłoszenie osoby do kontaktów z CSIRT NASK - 5 listopada 2020 r., zgłoszenie kolejnej osoby, po rozwiązaniu stosunku pracy z poprzednią - 12 czerwca 2023 r.

[24] Dz. U. z 2024 r., poz. 1077. Dalej: „ustawa o KSC".

[25] W Urzędzie do elektronicznej inwentaryzacji sprzętu i oprogramowania (CMDB) służącej do przetwarzania informacji obejmującej ich rodzaj i konfigurację wykorzystuje się moduł „Inventory" oprogramowana Axence nVision 15.

(akta kontroli str. 163-171)

Burmistrz wyjaśnił, że podejście pracowników Urzędu do ww. zagadnień bazuje przede wszystkim na analizie ryzyka oraz doborze odpowiednich zabezpieczeń. Nie bez znaczenia jest również bogate doświadczenie i wiedza naszego personelu odpowiedzialnego za administrowanie infrastrukturą Urzędu. Choć Urząd nie posiada formalnie zatwierdzonych planów zachowania ciągłości działania i planów odtworzeniowych, działania Urzędu w praktyce są solidnie ugruntowane w analizie ryzyka oraz w efektywnym doborze zabezpieczeń. Każdy projekt lub zakup związany z wdrożeniem nowego zabezpieczenia jest dokładnie analizowany pod kątem minimalizacji potencjalnych zagrożeń.

Ponadto Burmistrz wskazał, że opracowano Gminny Plan Zarządzania Kryzysowego, w którym są opracowane procedury na ewentualne wystąpienie różnego rodzaju sytuacji kryzysowych oraz Plan przemieszczenia i zapewnienia funkcjonowania Burmistrza Koronowa na Głównym Stanowisku Kierowania w Zapasowym Miejscu Pracy, który przewiduje przemieszczenie stanowisk pracy kluczowych dla funkcjonowania Urzędu na wypadek zagrożenia jego zniszczeniem do Zapasowego Miejsca Pracy Burmistrza Koronowa.

Burmistrz wyjaśnił również, że do każdego incydentu podchodzimy indywidualnie, biorąc pod uwagę szereg kluczowych czynników, które mają wpływ na efektywność i skuteczność przywracania systemów do działania. Wprowadzona przez Urząd strategia w zakresie ustalania akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych opiera się na dokładnej analizie każdego incydentu, z uwzględnieniem wymagań prawnych, znaczenia strategicznego systemów, dostępnych zasobów, priorytetów oraz najlepszych praktyk zarządzania IT. Takie podejście pozwala nam na skuteczniejsze zarządzanie incydentami i minimalizowanie ich negatywnego wpływu na działalność Urzędu.

Ponadto Burmistrz wyjaśnił, że w ramach realizowanego przez Urząd projektu grantowego „Cyberbezpieczny Samorząd" wzięto pod uwagę dostosowanie SZBI do obowiązujących wymagań norm i przepisów prawa. Jednym z jej elementów będzie Polityka ciągłości działania. Natomiast zadania związane z przebudową infrastruktury powinny uwzględnić również utworzenie dokumentacji umożliwiającej odtworzenie wdrażanej w ramach projektu infrastruktury.

(akta kontroli str. 163-171, 214, 275)

OCENA CZĄSTKOWA

W Urzędzie prawidłowo opracowano i wdrożono SZBI. Właściwie zidentyfikowano wszystkie zbiory danych Urzędu podlegających zabezpieczeniu i prowadzono pełną inwentaryzację zasobów informatycznych. Umożliwiono IOD wykonywanie obowiązków w sposób niezależny. Pozytywnie oceniono przeprowadzanie, w okresie objętym kontrolą, szacowania ryzyka w zakresie bezpieczeństwa teleinformatycznego. Jako stan nieprawidłowy uznano nieopracowanie planu odtworzeniowego oraz nieokreślenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych.

OBSZAR

2. Wdrożenie i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji oraz ciągłość działania

Opis stanu faktycznego

2.1. W Urzędzie wdrożono mechanizmy ograniczające możliwość instalacji nieautoryzowanego oprogramowania przez użytkowników systemu. Badanie 10 stacji roboczych[26] pod kątem możliwości instalacji zewnętrznego oprogramowania wykazało, że we wszystkich badanych przypadkach zadziałały odpowiednie mechanizmy blokujące. Ponadto na urządzeniach mobilnych z systemem Android (telefony komórkowe, tablety) wykorzystywanych w Urzędzie stosowano system zabezpieczeń klasy Mobile Device Management, który między innymi ogranicza użytkownikowi możliwość pobierania aplikacji nie autoryzowanych przez administratorów. Działania te były zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli str. 328-330, 979)

2.2. Analiza uprawnień do systemów, zakresów obowiązków oraz upoważnień do przetwarzania danych osobowych 15 pracowników Urzędu[27] wykazała, że wszyscy badani pracownicy, zgodnie z § 19 ust. 2 pkt 4 rozporządzenia KRI, uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań.

(akta kontroli str. 412-503)

2.3. W toku kontroli poddano analizie proces odbierania uprawnień 15 pracowników, którzy zakończyli stosunek pracy w okresie objętym kontrolą, a ich konta użytkowników powinny zostać zablokowane niezwłocznie po zakończeniu pracy w celu uniemożliwienia dostępu do systemów informatycznych Urzędu. Stwierdzono, że w dwóch przypadkach konta zostały zablokowane przed ustaniem stosunku pracy, w pozostałych przypadkach, pomimo ustania stosunku pracy, konta zostały zablokowane w terminach od trzech do 107 dni. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 326-327, 776-783)

2.4. W celu zapewnienia ochrony przetwarzanych w Urzędzie informacji przed nieuprawnionym dostępem stosuje się metody uwierzytelniania oparte na unikalnym identyfikatorze użytkownika oraz haśle o odpowiedniej złożoności. Dostęp do systemów operacyjnych stacji roboczych wszystkich pracowników Urzędu realizuje się na podstawie autoryzacji użytkownika w Active Directory[28]. Ustalono, że na serwerze AD Urzędu zdefiniowana jest polityka dotycząca złożoności i długości haseł. Wymuszono zmianę hasła po 30 dniach. System zapamiętuje trzy ostatnie hasła w celu uniemożliwienia ich powtórzenia. W Urzędzie dostęp do poszczególnych systemów dziedzinowych realizowany jest w większości za pomocą pojedynczego logowani SSO[29] w oparciu o uwierzytelnianie w AD. Szczegółowej analizie poddano trzy systemy informatyczne, z których dwa[30] posiadały odrębne metody uwierzytelniania, jeden[31] korzystał z mechanizmu SSO. W wszystkich badanych przypadkach zdefiniowane w systemach reguły dotyczące budowy haseł były odpowiednie i zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI oraz pkt. 6 PKDI[32].

(akta kontroli str.64-76, 279-284, 643-650)

---

[26] W tym pięciu komputerów stacjonarnych oraz pięciu komputerów przenośnych (laptoów).
[27] W tym trzech na stanowiskach kierowniczych.
[28] Serwer domenowy MS Windows Active Directory, dalej „AD".
[29] Single sign-on.
[30] BeSTi@ i @Pszok.
[31] KBiP Księgowość Budżetowa i Planowanie.
[32] Procedury Kontroli Dostępu do Informacji stanowiącej zał. nr 1 do PBI.

2.5. Oględziny sześciu stanowisk pracy realizujących zadania z wykorzystaniem aplikacji „Źródło" wykazały, że monitory stacji roboczych obsługujących aplikację usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione, zgodnie z wymogami § 19 ust. 2 pkt 7 rozporządzenia KRI oraz § 18 pkt 1 ppkt 8 PODO[33].

(akta kontroli str.135-160, 335-337)

2.6. Zasady gwarantujące bezpieczną pracę przy pracy zdalnej z wykorzystaniem informatycznego sprzętu mobilnego zostały zdefiniowane w pkt. 9 i 10 PKDI oraz zasadach bhp przy pracy zdalnej zgodnie z § 19 ust. 2 pkt 8 rozporządzenia KRI. Według ww. zasad zdalny dostęp do zasobów informatycznych Urzędu realizowany był poprzez szyfrowana wirtualną sieć prywatną VPN po poprawnej identyfikacji i uwierzytelnieniu zdalnego użytkownika. Urządzenia mobilne i nośniki danych wynoszone poza urząd podlegają szyfrowaniu, a użytkownicy są zobowiązani do ochrony ich przed uszkodzeniami, kradzieżą dostępem osób postronnych.

(akta kontroli str. 64-76, 776-783, 787-791)

2.7. Dane gromadzone na komputerach przenośnych Urzędu były szyfrowane. BIOS komputerów użytkowników skonfigurowany jest sposób wymuszający w pierwszej kolejności uruchamianie zaszyfrowanego systemu plików. Dostęp do BIOS zabezpieczony był hasłem znanym wyłącznie administratorom IT. Ponadto zastosowane polityki (GPO[34]) - po pięciu minutach bezczynności blokowały aktualnie zalogowanego użytkownika. Komputery wyposażone były w system antywirusowy oraz firewall.

(akta kontroli str.776-783)

2.8. Serwery oraz urządzenia aktywne sieci komputerowej Urzędu zlokalizowane były w dwóch wyodrębnionych, nieoznakowanych pomieszczeniach (serwerowniach), w dwóch odrębnych lokalizacjach, do których dostęp mieli wyłącznie informatycy Urzędu. Wprowadzono odpowiednie środki organizacyjne, fizyczne i techniczne[35] w celu zabezpieczenia informacji znajdujących się na serwerach Urzędu zgodnie z § 19 ust. 2 pkt 9 rozporządzenia w sprawie KRI. W pomieszczeniu zastosowano ponadto środki zabezpieczenia przed czynnikami środowiskowymi: klimatyzatory, czujniki dymu, czujniki zalania, UPS-y[36], urządzenia gaśnicze do sprzętu elektronicznego.

(akta kontroli str.286-325, 406-411)

2.9. Badaniem objęto cztery umowy[37] zawarte przez Urząd z podmiotami zewnętrznymi. W umowach zawierano zapisy dotyczące ochrony danych osobowych oraz zapisy zobowiązujące wykonawcę do zachowania w tajemnicy informacji, do jakich może mieć dostęp w ramach wykonywania umowy, innych niż dane osobowe zgodnie z wymogami § 19 ust. 2 pkt 10 rozporządzenia KRI. We wszystkich badanych przypadkach, zgodnie z zapisami umów, na okoliczność powierzenia przez Zamawiającego danych osobowych do przetwarzania zawierano umowy powierzenia przetwarzania danych osobowych.

(akta kontroli str. 651-676, 980-988)

---

[33] Polityka Ochrony Danych Osobowych w Urzędzie Miejskim w Koronowie stanowiącej załącznik nr 10 do PBI.

[34] GPO (Group Policy Objects) - zbiór reguł i ustawień określających zakres działania komputera oraz użytkowników danego komputera z MS Windows ustanawiany na serwerze AD.

[35] Co potwierdziły oględziny serwerowni dokonane w dniach 11 czerwca 2024 r. i 7 sierpnia 2024 r.

[36] Zasilacze awaryjne.

[37] Umowy: [1] na licencję aktualizacji (upgrade) oprogramowania EZD Proton, [2] serwis bieżący centrali telefonicznej (w tym administrowanie), [3] dzierżawę urządzeń drukujących, [4] na licencję aktualizacji oraz nadzór autorski nad oprogramowaniem BUDŻET, PODATKI, KSGZOB, PODATKI, DZIERŻAWY, REJESTRY, SELWIN z RWWIN, ŚRODKI TRWAŁE, AUTA, KASA, UŻYTKOWANIE, KADRY i PŁĄCE, UPK, OPLOK.

2.10. W okresie objętym kontrolą Urząd nie przekazywał sprzętu informatycznego poza jednostkę w celu serwisu lub zbycia.

(akta kontroli str.795-797)

2.11. W Urzędzie ustalono zasady tworzenia i przechowywania kopii zapasowych[38]. Określały one zakres tworzenia kopii zapasowych, częstotliwość ich wykonywania i okresy przechowywania oraz zasady testowania i odzyskiwania danych. Za wykonanie kopii zapasowych odpowiedzialny był administrator systemu.

(akta kontroli str. 82-88)

2.12. Na podstawie oględzin stwierdzono, że kopie zapasowe zbiorów danych i oprogramowania wykonywane były codziennie od poniedziałku do piątku automatycznie przy użyciu dedykowanego oprogramowania UDP[39], mechanizmu replikacji maszyn wirtualnych Hyper-V[40] oraz raz na tydzień w sobotę za pomocą skryptu PowerShell[41] na zewnętrzne szyfrowane dyski twarde zgodnie z regułami zawartymi w PBI. Kopie przechowywane były na macierzach dyskowych w dwóch lokalizacjach Urzędu. Kopia na zewnętrznych dyskach przechowywana była w wyodrębnionym pomieszczeniu w zamkniętym sejfie. Kopie zapasowe podlegały regularnemu testowaniu, a informacje o testach rejestrowane były w dzienniku pracy administratora[42]. Przeprowadzone w toku oględzin badanie odzyskiwania danych z kopii zapasowej dla jednego wybranego systemu zakończyło się pomyślnym odtworzeniem bazy.

(akta kontroli str.338-411)

2.13. Nie opracowano procedury monitorowania pojemności pamięci masowych (dysków twardych) istotnych z punktu widzenia ciągłości działania serwerów Urzędu. W wyniku oględzin zajętości przestrzeni dyskowych trzech wybranych serwerów Urzędu stwierdzono krytyczne (powyżej 80%) zajętości przestrzeni dyskowej przeznaczonej na dane. Szczegółowe ustalenia w tym zakresie zawarto w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 331-334, 776-797)

2.14. W Urzędzie zidentyfikowano i zabezpieczono pod kątem wpływu czynników zewnętrznych, kluczowe elementy infrastruktury i usługi informatyczne w celu zapewnienia ciągłości działania, poprzez m.in.: zdublowanie zasilania do serwerowni Urzędu, stosowanie redundantnych zasilaczy w serwerach, macierzach dyskowych i głównych switchach Urzędu, zastosowanie zasilaczy awaryjnych (UPS), stały monitoring obwodów elektrycznych serwerowni, zabezpieczenie zapasowych urządzeń aktywnych sieci, zastosowanie klastra wysokiej dostępności oraz macierzy RAID, zastosowanie replikacji maszyn wirtualnych znajdujących się w klastrze do innych serwerów w innej lokalizacji, wykonywanie kopii zapasowych.

(akta kontroli str. 209-213, 223-249, 275-278, 285-325)

Stwierdzone nieprawidłowości

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

1. W okresie objętym kontrolą nie zostały niezwłocznie zablokowane konta 13 z 15 pracowników, którzy zakończyli w tym czasie stosunek pracy. Zablokowanie kont

---

[38] Procedury tworzenia kopii zapasowych stanowiące załącznik nr 3 do PBI.

[39] Arcserve Unified Data Protection (UDP) 9.2.

[40] Hyper-V – oprogramowanie firmy Microsoft stosowane do wirtualizacji fizycznych maszyn będące elementem oprogramowania serwera MS Windows Server stosowanego w Urzędzie.

[41] PowerShell - System zarządzania i automatyzacji zadań oparty na linii poleceń zintegrowany z językiem skryptowym będący elementem oprogramowania systemowego MS Windows.

[42] W aplikacji HelpDesk pakietu oprogramowanie do zarządzania infrastrukturą IT – nVision.

nastąpiło w okresie od 3 do 107[43] dni od ustania stosunku pracy, tj. niezgodnie § 20 ust. 2 pkt 5 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[44] oraz zapisami pkt 4.2.10 Procedury kontroli dostępu do informacji stanowiącej załącznik nr 1 do PBI stanowiącej, że podstawą likwidacji konta jest rozwiązanie stosunku pracy. Pracownik ds. kadr lub inna osoba przez niego wyznaczona zobowiązana była zaznaczyć w dedykowanym systemie informatycznym, że rozwiązano stosunek pracy z pracownikiem. Na tej podstawie Administrator systemu powinien niezwłocznie cofnąć dostęp do systemów, do których pracownik posiadał uprawnienia i odnotować zaistniałą sytuację w systemie.

(akta kontroli str. 64-76, 326-327)

Burmistrz wyjaśnił, że sytuacja ta miała miejsce w 2023 r. W tym roku nastąpiły istotne zmiany w zespole odpowiedzialnym za utrzymanie systemów informatycznych. Długoletni informatyk, posiadający wieloletnie doświadczenie, zakończył współpracę z Urzędem. W jego miejsce pozostała osoba z krótszym stażem oraz został zatrudniony nowy, młody pracownik. Proces wdrożenia nowych pracowników wymagał znacznego nakładu pracy, w tym przygotowania ich do wykonywania obowiązków oraz przeprowadzenia odpowiednich szkoleń. W tym w szczególności zaangażowanie w proces wprowadzani i szkolenia nowych pracowników kierownika Wydziału Organizacyjnego, posiadającego wieloletnie doświadczenie w zarządzaniu systemami informatycznymi. To z kolei chwilowo wpłynęło na efektywność zarządzania tymi systemami. Burmistrz nadmienił, że pomimo chwilowych problemów, dane z tego roku pokazują, że wszystko wróciło do normy, a pracownicy nabrali niezbędnego doświadczenia.

(akta kontroli str. 776-783)

2. W Urzędzie nie opracowano procedur monitorowania pojemności pamięci masowych (dysków twardych) istotnych z punktu widzenia ciągłości działania serwerów Urzędu oraz w niewystarczający sposób monitorowano pojemności nośników dla zapewnienia właściwej wydajności systemu, co należy uznać za działanie nierzetelne. Oględziny zapełnienia przestrzeni dyskowych wybranych trzech serwerów[45] wykazały, że w we wszystkich badanych przypadkach zajętość partycji przeznaczonej na dane przekraczała 80%[46].

(akta kontroli str. 331-334, 776-797)

Burmistrz wyjaśnił, że zadania zawiązane z monitorowaniem przestrzeni dyskowej realizują administratorzy systemu w ramach swoich bieżących obowiązków, zwiększając przydziały dyskowe w miarę potrzeb. Wdrożony w zeszłym roku klaster wysokiej dostępności działający w oparciu o macierz dyskową umożliwił zwirtualizowanie środowiska serwerowego oraz spowodował dynamiczne zmiany w infrastrukturze IT. Biorąc pod uwagę powyższe, jak również planowaną w ramach programu „*Cyberbezpieczny Samorząd*", modernizację SZBI, w tym aktualizację dokumentacji i procedur oraz niniejszą

[43] Konta dwóch pracowników zablokowane zostały po trzech dniach, jednego po czterech, jednego po sześciu, dwóch po siedmiu, jednego po ośmiu, jednego po dziewięciu, jednego po 19, jednego 34, dwóch po 75 oraz jednego po 107 dniach.

[44] Dz.U. z 2017 r. poz. 2247, obowiązującego do 22 maja 2024 r.

[45] [1] serwera bazodanowego dla oprogramowania finansowo-księgowego, [2] serwera plików przechowującego foldery osobiste użytkowników i oprogramowanie finansowo-księgowe, [3] serwera obsługującego elektroniczny obieg dokumentów.

[46] Zajętość przestrzeni dyskowej przeznaczonej na dane serwera [1]: 82%, serwera [2]: 95%, serwera [3]: 96%.

kontrolę, planuje się w ramach realizacji ww. projektu również opracować odpowiednie procedury monitorowania pojemności pamięci masowych wykorzystywanych na serwerach i wytyczne w tym zakresie.
W odniesieniu do stwierdzonych krytycznych zajętości dysków stwierdził, że Urząd do przechowywania danych na serwerach korzysta z klastra mającego ograniczone zasoby przestrzeni dyskowej. W związku z powyższym przydział tej przestrzeni dla uruchomionych na klastrze maszyn wirtualnych następuje z uwzględnieniem tych ograniczeń. Na bieżąco analizowany jest przyrost danych w systemach informatycznych i dokonywane są niezbędne zmiany. Nie stwierdzono sytuacji aby zajętość dysków z danymi negatywnie wpłynęła na ciągłość działania pracujących na nich systemów. Dokonano szczegółowej analizy zajętości dysków twardych we wszystkich systemach zlokalizowanych w serwerowni Urzędu. W wyniku podjętych działań zwiększono dostępne miejsce m.in. dla serwera elektronicznego obiegu dokumentów (73%). Ponadto utworzono odrębną maszynę wirtualną dla oprogramowania co spowodowało zmniejszenie zajętości serwera plików do 88%. Przestrzeń ta obecnie wyłącznie do przechowywania folderów osobistych użytkowników oraz danych współdzielonych między użytkownikami. Pozostaje około 180GB wolnej przestrzeni na dane, co nie jest wartością krytyczną. Ponadto użytkownicy zostaną monitowani o przegląd i usunięcie zbędnych i dublowanych plików. W przypadku serwera bazodanowego dla oprogramowania finansowo-księgowego zajętość serwera na poziomie 82% była związana z faktem konieczności podniesienia wersji oprogramowania bazodanowego i przechowywania przez pewien czas danych z przed dokonania konwersji. Po usunięciu danych pojemność spadła do 49%.
Burmistrz nadmienił, że w ramach realizacji projektu grantowego „*Cyberbezpieczny Samorząd*" Gmina planuje rozbudowę przestrzeni dyskowej w posiadanej macierzy dyskowej.

(akta kontroli str. 776-797)

OCENA CZĄSTKOWA

Zabezpieczenia techniczne systemów informatycznych, przyjęte w Urzędzie zapewniały ochronę przetwarzanych informacji przed nieuprawnionym dostępem. Pomieszczenie serwerowni posiadało odpowiednie zabezpieczenia. Prawidłowo tworzono i przechowywano kopie zapasowe zbiorów danych, programów i oprogramowania systemowego zapewniające ciągłość działania systemu informatycznego. Prawidłowo opracowano i wdrożono zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego przy pracy zdalnej.

Stwierdzone nieprawidłowości polegały na nieprzestrzeganiu Procedury kontroli dostępu do informacji obowiązującej w Urzędzie w zakresie likwidacji kont użytkowników oraz braku procedur monitorowania pojemności pamięci masowych (dysków twardych) istotnych z punktu widzenia ciągłości działania serwerów.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie przeprowadzono analizę ryzyka utraty integralności, dostępności oraz poufności informacji, o której mowa w § 19 ust 2 pkt 3 rozporządzenia KRI na podstawie obowiązującej Procedury zarządzania ryzykiem w bezpieczeństwie informacji[47]. Analiza wykazała, że podjęto działania minimalizujące ryzyka, stosownie do wyników i zaleceń.

[47] Załącznik nr 5 do PBI.

(akta kontroli str. (100-113, 161-172, 209-214, 240-249)

3.2. Urząd opracował i wdrożył Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji[48], której celem jest zapewnienie, że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający niezwłoczne podjęcie działań korygujących. PBI wraz z niniejszą procedurą została przedstawiona do zapoznania się i stosowania pracownikom Urzędu. W Urzędzie prowadzono rejestr zgłaszanych incydentów związanych z bezpieczeństwem informacji. W okresie objętym kontrolą odnotowano osiem incydentów w tym zakresie[49]. Incydenty nie dotyczyły naruszenia ochrony danych osobowych. Dla wszystkich odnotowanych incydentów sporządzono odpowiednie raporty i dokonano zgłoszeń do CSIRT NASK[50] oraz podjęto odpowiednie działania zaradcze.

(akta kontroli str. 89-99, 741-775)

3.3. W kontrolowanym okresie pracownicy Urzędu uczestniczyli w czterech[51] szkoleniach z zakresu bezpieczeństwa informacji. Szkolenia dotyczyły: cyberbezpieczeństwa, ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego, podstawowych zasad cyberhigieny w pracy i życiu prywatnym oraz przeglądu systemu zarządzania bezpieczeństwem informacji.

(akta kontroli str.504-642)

3.4. W 2023 r., zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI, przeprowadzono w Urzędzie audyt wewnętrzny SZBI w zakresie legalności i aktualizacji oprogramowania[52], polityki uprawnień[53] oraz zapobiegania, wykrywania i reagowania na incydenty bezpieczeństwa. Sformułowano w jego wyniku zalecenia po audytowe (rekomendacje) oraz przyjęto harmonogram ich realizacji z uwzględnieniem realizowanego projektu grantowego „*Cyberbezpieczny Samorząd*".

(akta kontroli str.793-808)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK ocenia pozytywnie działania podejmowane w kontrolowanym okresie przez Urząd w celu zapobiegania incydentom bezpieczeństwa informacji.

---

[48] Załącznik nr 4 do PBI.

[49] Dotyczących: Podszywania się nadawcy w wiadomości e-mail pod Burmistrza lub bank w celu wyłudzenia środków, wiadomości e-mail z zainfekowanymi załącznikami, e-mail z próbą wyłudzenia danych logowania (informacja o wygaśnięciu hasła).

[50] CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie.

[51] [1] Szkolenie z cyberbezpieczeństwa w ramach projektu grantowego „Cyfrowa Gmina" (5-8.2022 r.) – uczestniczyło 79 pracowników z 93 (85%) pracowników Urzędu uczestniczących w procesie przetwarzania informacji.
[2] Szkolenie z ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego (5.04..2023 r. i 21.12.2023) - 21 pracowników z 93 (23%).
[3] Podstawowe zasady cyberhigieny w pracy i życiu prywatnym (16.11.2023 r.) – 18 pracowników z 93 (19%) .
[4] Przegląd zarządzania bezpieczeństwem informacji (21.12.2023 r.) – 16 pracowników z 93 (17%).

[52] Tj. weryfikacja legalności software'u.

[53] Realizowanej za pośrednictwem systemu GLADIUS.

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 uwagi i wnioski:

Uwagi

NIK nie formułuje uwag.

Wnioski

1. Opracowanie planów zachowania ciągłości działania i planów odtworzeniowych oraz określenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych.
2. Przestrzeganie procedury nadawania/zmiany/cofnięcia uprawnień do systemów informatycznych.
3. Opracowanie procedur monitorowania pojemności pamięci masowych istotnych z punktu widzenia ciągłości działania serwerów.
4. Prowadzenie audytu wewnętrznego w zakresie bezpieczeństwa informacji w sposób niezależny i obiektywny.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykorzystania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 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.

Bydgoszcz, 19 września 2024 r.

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy
p.o. Dyrektor
Tomasz Sobecki

Kontroler
Tomasz Klause
Doradca techniczny