NAJWYŻSZA IZBA KONTROLI

Delegatura w Bydgoszczy

LBY.410.12.1.2024

Krzysztof Maćkiewicz
Starosta Wąbrzeski
Starostwo Powiatowe w Wąbrzeźnie
ul. Wolności 44
87-200 Wąbrzeźno

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy
ul. Wały Jagiellońskie 12, 85-950 Bydgoszcz
T +48 52 567 58 00, F +48 52 567 58 60
lby@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Wąbrzeźnie[1], ul. Wolności 44, 87-200 Wąbrzeźno
Kierownik jednostki kontrolowanej	Krzysztof Maćkiewicz, Starosta Wąbrzeski, od 7 listopada 1998 r.[2]
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 w 2024 r.[3] (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina/Cyfrowy Powiat)
Podstawa prawna podjęcia kontroli	art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 roku o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Bydgoszczy
Kontroler	Robert Elwertowski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/91/2024 z 27 maja 2024 r.

(akta kontroli str. 1-4)

[1] Dalej: „Urząd" lub „Starostwo".
[2] Dalej: „Starosta".
[3] Zakończenie czynności kontrolnych: 23 sierpnia 2024 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: „ustawa o NIK".

II. Ocena ogólna kontrolowanej działalności[5]

OCENA OGÓLNA

W Urzędzie prawidłowo opracowano i wdrożono system zarządzania bezpieczeństwem informacji[6], jednak nie dokonywano przeglądów i aktualizacji dokumentów i polityk wchodzących w jego skład, co oceniono negatywnie. Właściwie zidentyfikowano wszystkie zbiory danych Urzędu podlegające zabezpieczeniu oraz prowadzono pełną inwentaryzację zasobów informatycznych. Umożliwiono Inspektorowi Ochrony Danych[7] wykonywanie obowiązków w sposób niezależny. Pozytywnie oceniono przeprowadzanie, w okresie objętym kontrolą, szacowania ryzyka w zakresie bezpieczeństwa teleinformatycznego.

Zabezpieczenia techniczne systemów informatycznych, przyjęte w Starostwie zapewniały ochronę przetwarzanych informacji przed nieuprawnionym dostępem. Ustawienie monitorów objętych badaniem zapewniało, że dane wyświetlane na ekranie nie były widoczne dla osób nieuprawnionych. Prawidłowo opracowano zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego oraz dokonywano na nim szyfrowania danych. Zarządzano pojemnością serwerów w sposób gwarantujący wydajność systemów a pomieszczenie serwerowni posiadało odpowiednie zabezpieczenia. Należycie tworzono i przechowywano kopie zapasowe zbiorów danych, programów i oprogramowania systemowego zapewniające ciągłość działania systemu informatycznego, jednak nie były one regularnie testowane, co uznano jako nieprawidłowe.

Urząd przeprowadził analizę ryzyka utraty integralności, dostępności lub poufności informacji oraz podjął działania adekwatnie do jej wyników. Opracowana procedura zgłaszania incydentów naruszenia bezpieczeństwa informacji została przedstawiona do zapoznania się i stosowania pracownikom Urzędu.

Pozostałe nieprawidłowości stwierdzone w toku kontroli dotyczyły:

- nieprzestrzegania procedury nadawania/zmiany/cofnięcia uprawnień do systemów informatycznych;
- nieopracowania planu odtworzeniowego oraz nieokreślenia akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych;
- nieprzeprowadzenia audytu wewnętrznego z zakresu bezpieczeństwa informacji;
- niezawierania w umowach z podmiotami zewnętrznymi zapisów zobowiązujących wykonawców do zachowania poufności.

Jako działania nieprawidłowe uznano również niezapewnianie szkoleń pracownikom Starostwa zaangażowanych w proces przetwarzania informacji.

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 z uwzględnieniem m.in. wymagań prawnych i wrażliwości na nieuprawnione ich

[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.

ujawnienie. Informacje będące w posiadaniu Starostwa i jednocześnie przetwarzane, w tym dane osobowe, zostały opisane w rejestrze czynności przetwarzania danych osobowych. Wyszczególniono i opisano środki służące zapewnieniu bezpieczeństwa informacji i danych osobowych dla trzech typów zabezpieczenia: technicznego, organizacyjnego i informatycznego.

(akta kontroli str. 160-182)

1.2 W Starostwie opracowano i wdrożono 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]. W jego skład wchodziły następujące dokumenty:

- Polityka Bezpieczeństwa Informacji i Danych Osobowych w Starostwie[10];
- Polityka Zarządzania Systemem Informatycznym w Starostwie[11];
- Procedura zarządzania incydentami z zakresu bezpieczeństwa systemów teleinformatycznych i informacji[12];
- Metodyka analizy ryzyka naruszenia praw i wolności osób fizycznych oraz oceny skutków dla ochrony danych w Starostwie[13];
- Regulamin funkcjonowania systemu monitoringu wizyjnego na terenie Starostwa[14].

Ww. procedury zostały przedstawione do zapoznania się i stosowania pracownikom Urzędu. Opracowanie i aktualizacje PBI powierzono firmie zewnętrznej, której pracownik pełnił również w Starostwie funkcję IOD. PBI i PZSI zawierały m.in.: zasady korzystania z sieci Internet; procedury nadawania, zmiany i cofnięcia uprawnień do systemów informatycznych oraz stosowane środki uwierzytelnienia; zasady korzystania z poczty elektronicznej, procedurę rozpoczęcia, zawieszenia i zakończenia pracy użytkowników sytemu; procedurę tworzenia kopii zapasowych wraz z miejscem i okresem ich przechowywania; zabezpieczenie sprzętu i systemu do przetwarzania danych; postępowanie ze sprzętem informatycznym, nośnikami danych, naprawą, serwisem sprzętu oraz utylizacją, zasady korzystania ze sprzętu mobilnego; postępowanie w przypadku naruszenia bezpieczeństwa informacji i ochrony danych osobowych; organizację audytów zgodności.

(akta kontroli str. 5-105)

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)[15]. Ww. dokumentacja została zatwierdzona przez Starostę i zakomunikowana pracownikom Urzędu.

[9] Dz.U. z 2024 r. poz. 773, dalej: „rozporządzenie KRI". Wcześniej, do 22 maja 2023 r. obowiązywało rozporządzenie Rady Ministrów z 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 2017 r. poz. 2247), dalej: „rozporządzenie KRI z 2012 r.".
[10] Załącznik nr 1 do Zarządzenia Starosty nr 43/2022 z 22 listopada 2022 r., dalej: „PBI".
[11] Załącznik nr 2 do Zarządzenia Starosty nr 43/2022 z 22 listopada 2022 r., dalej: „PZSI".
[12] Załącznik do Zarządzenia Starosty nr 28/2023 z 29 grudnia 2023 r., dalej: „PZI".
[13] Zatwierdzona 8 lutego 2023 r.
[14] Załącznik nr 3 do Zarządzenia Starosty nr 43/2022 z 22 listopada 2022 r.
[15] Dz. Urz. UE. L 2016 Nr 119, str. 1, ze zm., dalej: „RODO".

(akta kontroli str. 5)

1.4 W okresie objętym kontrolą w Urzędzie przeprowadzono szacowanie ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych.

(akta kontroli str. 122-141)

W PZI opisano klasyfikację incydentów oraz podział potencjalnych zdarzeń. Spośród nich wyodrębniono:

- zdarzenia losowe zewnętrzne, których występowanie mogłoby prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej. Ciągłość pracy systemów zostałaby zakłócona, nie doszłoby do naruszenia poufności danych: np. klęski żywiołowe, przerwy w zasilaniu;
- zdarzenia losowe wewnętrzne, w wyniku których mogłoby dojść do zniszczenia danych, zakłócenia ciągłości pracy systemu i naruszenia poufności danych: np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętu, błędy w oprogramowaniu;
- zdarzenia zamierzone, świadome i celowe, które stanowić mogłyby najpoważniejsze zagrożenie naruszenia poufności danych: np. nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu), danych z sieci wewnętrznej; nieuprawniony transfer danych; pogorszenie funkcjonowania sprzętu (działanie wirusów); bezpośrednie zagrożenie materialnych składników systemu (kradzież sprzętu).

(akta kontroli str. 93-105)

1.5-1.7 Polityka ciągłości działania została ustalona w PBI i PZSI oraz zakomunikowana pracownikom Starostwa. W celu zachowania ciągłości działania systemu informatycznego m.in. zabezpieczano sprzęt i system przed działaniem niebezpiecznego oprogramowania. Zastosowano urządzenia typu UPS[16], generator prądu chroniące przed skutkami awarii zasilania. Określono sposób tworzenia kopii, częstotliwość oraz miejsce i okres ich przechowywania. Wykonywano kopie zapasowe zbiorów danych, programów i narzędzi programowych do przetwarzania. oraz kopie zapasowe oprogramowania systemowego. Kopie zapasowe, wykonane na nośnikach zewnętrznych, przechowywane były w zamkniętym sejfie. Dostępnych było również sześć serwerów, na których przechowywano kopie w czterech różnych lokalizacjach.

W Urzędzie nie opracowano i nie testowano planu odtworzeniowego oraz nie określono akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych[17].

(akta kontroli str. 17-18, 59-60,183-187)

1.8 W okresie objętym kontrolą nie dokonywano przeglądów i aktualizacji dokumentów składających się na SZBI[18].

(akta kontroli str. 183)

1.9 Nadzór nad bezpieczeństwem informacji oraz zapewnienie ciągłości działania powierzono, wskazanemu w umowie z firmą zewnętrzną, informatykowi. Do jego zadań należało m.in.:

- stały nadzór nad oprogramowaniem sieciowym oraz infrastrukturą informatyczną Starostwa;

[16] Tj. zasilacz awaryjny (ang. uninterruptible power supply).
[17] Por. stwierdzone nieprawidłowości.
[18] Por. stwierdzone nieprawidłowości.

- zarządzanie systemem do przetwarzania danych osobowych;
- przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego;
- przydzielanie każdemu użytkownikowi identyfikatora oraz hasła do systemu oraz usuwanie kont użytkowników zgodnie z zasadami określonymi w polityce ochrony danych;
- sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

(akta kontroli str. 52-53, 113-120)

1.10 Wykonywanie funkcji IOD zostało powierzone wyznaczonemu pracownikowi firmy zewnętrznej w ramach umowy usługi. Do jego obowiązków należało m.in.:

- informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach na nich spoczywających;
- monitorowanie przestrzegania przepisów;
- podejmowanie działań zwiększających świadomość oraz szkolenia personelu uczestniczącego w operacjach przetwarzania danych;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;
- współpraca z organem wykonawczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

Analiza wykazała, że osoba pełniąca ww. funkcję posiadała odpowiednie kwalifikacje.

(akta kontroli str. 19, 106-110)

1.11 W Urzędzie umożliwiono IOD wykonywanie obowiązków w sposób niezależny. Zgodnie z zapisami PBI podlegał on bezpośrednio administratorowi, który wspierał IOD przy wypełnianiu przez niego zadań oraz zapewniał by nie otrzymywał on instrukcji od innego personelu. W działalności IOD nie występował konflikt interesów. Było to zgodne z art. 38 ust. 3 i 6 RODO.

(akta kontroli str. 18-19)

1.12 Do utrzymywania kontaktów z podmiotami krajowego systemu bezpieczeństwa wyznaczony został informatyk[19]. Dane ww. osoby zostały przekazane do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym, prowadzonego przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy[20] 7 kwietnia 2021 r. tj. w terminie, o którym mowa w art. 22 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[21]. Starosta podał, że osoby do utrzymywania ww. kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych

[19] 2 kwietnia 2021 r.
[20] Dalej: „CSiRT NASK".
[21] Dz.U. z 2024 r. poz. 1077, dalej: „ ksc".

przez jednostki podległe lub inne jednostki organizacyjne Starostwa, wyznaczali kierownicy tych jednostek.

(akta kontroli str. 111-112, 319)

1.13 Sporządzono wymagane w PBI i PZSI szczegółowe dokumenty wykonawcze. Procedury i instrukcje opisane zostały w treści ww. polityk lub stanowiły do nich załączniki i dotyczyły one m.in.: tworzenia kopii zapasowych, prowadzenia dziennika pracy informatyka; nadawania, zmiany i cofnięcia uprawnień; ewidencji przydzielanych identyfikatorów i adresów poczty elektronicznej; postępowania ze sprzętem informatycznym, nośnikami danych, naprawą, serwisem sprzętu oraz utylizacją; wydawania upoważnień do przetwarzania danych osobowych, zgłoszenia nowych czynności do rejestru wszystkich kategorii czynności przetwarzania danych przez procesora; zawierania umów powierzenia danych osobowych do przetwarzania; zgłaszania naruszeń ochrony danych.

(akta kontroli str. 11-79)

1.14 Oględziny[22] oprogramowania inwentaryzującego zasób sprzętu informatycznego[23] wykazały, że Urząd posiadł aktualne informacje o zasobie, tj. m.in. nazwę producenta, numer seryjny, typ i model, system operacyjny, lokalizację, komponenty/procesor, nazwę użytkownika.

(akta kontroli str. 188)

1.15 Starostwo przystąpiło do programu „Cyberbezpieczny Samorząd". 12 grudnia 2023 r. złożono wniosek o dofinasowanie dla projektu „Zakup środków i wdrożenie procedur zapewniających bezpieczeństwo w cyberprzestrzeni w Powiecie Wąbrzeskim". Wartość ww. zadania wynosiła 850,0 tys. zł. Zakres rzeczowy projektu obejmował m.in. przeprowadzanie dwóch szkoleń dla pracowników z zakresu cyberbezpieczeństwa; zakupy urządzeń i oprogramowania[24]; aktualizację polityki SZBI oraz przeprowadzenie dwóch zewnętrznych audytów bezpieczeństwa. Starosta podał, że pomiar poprawy bezpieczeństwa w związku z realizacją ww. projektu zostanie wykonany na podstawie wskazań podmiotu prowadzącego projekt oraz na podstawie ustaleń audytu końcowego.

Do dnia zakończenia kontroli nie podpisano umowy o dofinasowanie z Instytucją Zarządzającą.

(akta kontroli str. 199-239, 323)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie opracowano i nie testowano planu odtworzeniowego[25] oraz nie określono akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych, co uznano jako nierzetelne.

[22] Przeprowadzonych 9 lipca 2024 r.

[23] Do badania wytypowano 10 komputerów, jeden serwer, dwa laptopy, router i drukarkę.

[24] Urządzeń typu token do MFA w połączeniach VPN, switch-y klasy Enterprise, przetwornicy UPS zabezpieczającej punkty dostępu do sieci przed nagłą awarią prądu, zaawansowanych zasilaczy UPS, które będą wyposażone w porty komunikacyjne pozwalające na wysyłanie komunikatów o problemach z zasilaniem, klastra niezawodnościowego dwu lub trój węzłowego w celu zachowania ciągłości pracy oraz wdrożenia systemów zarządzania logami i podatnościami, serwera NAS, agregatu prądotwórczego o odpowiedniej mocy celem zabezpieczenia krytycznych punktów JST przed długotrwałą utratą zasilania prowadzącą do przerwania jego pracy, oprogramowania do automatyzacji procesów inwentaryzacji i monitoringu urządzeń w czasie rzeczywistym, aktualizacji dotychczasowej wersji oprogramowania AV do wersji z EDR i możliwością szyfrowania danych.

[25] Dotyczącego w szczególności: zasilania i topologii sieci, klastrów i macierzy dyskowych, systemów kopii zapasowych, systemów serwerów wirtualnych, urządzeń brzegowych.

(akta kontroli str. 183)

Starosta wyjaśnił, że Urząd planuje wdrożyć plan odtworzeniowy w najnowszej aktualizacji polityk w ramach projektu „Cyberbezpieczny samorząd". Testowane było jedynie zasilanie awaryjne i odtwarzanie działania systemów, ale nie zostało to udokumentowane.

(akta kontroli str. 318)

2. W latach w 2023-2024 (II kw.) w Urzędzie nie dokonywano przeglądów i aktualizacji dokumentów składających się na SZBI. Stanowiło to naruszenie § 19 ust. 2 pkt 1 rozporządzenia KRI (oraz § 20 ust. 2 pkt 1 rozporządzenia KRI z 2012 r.), zgodnie z którym zarządzanie bezpieczeństwem informacji przez podmiot publiczny, realizowane jest w szczególności poprzez zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

(akta kontroli str. 183)

Starosta wyjaśnił, że obowiązek zawarty w rozporządzeniu KRI nie określa ściśle żadnego okresu w jakim polityki podlegają przeglądowi i aktualizacji. W § 10 ust. 2 PBI określono, że polityka podlega przeglądowi raz na trzy lata oraz w sytuacjach wystąpienia incydentów związanych z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadkach istotnych zmian, dokonywana była jej aktualizacja.

(akta kontroli str. 318-319)

NIK zauważa, że przy dzisiejszym postępie technologicznym polityka bezpieczeństwa informacji powinna być poddawana przeglądom i ewentualnej aktualizacji nie rzadziej niż raz na 12 miesięcy. W trakcie kontroli ustalono, że aktualizacji wymaga lub zawiera nieaktualne informacje PZSI w zakresie: nadawania/obierania uprawnień w systemie informatycznym oraz przechowywania kopii zapasowych.

OCENA CZĄSTKOWA

W Urzędzie prawidłowo opracowano i wdrożono SZBI jednak nie dokonywano przeglądów i aktualizacji dokumentów i polityk wchodzących w jego skład, co oceniono negatywnie. 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 nierzetelne uznano: nieopracowanie planu odtworzeniowego oraz nieokreślenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych .

OBSZAR

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

Opis stanu faktycznego

2.1 Uprawnienia użytkowników pięciu komputerów stacjonarnych i pięciu laptopów objętych oględzinami nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania. Było to zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

(akta kontroli str. 188-198)

Starosta podał, że będące w posiadaniu Urzędu tablety oraz smartfony nie były wykorzystywane do przetwarzania informacji służbowych. Służyły one do połączeń służbowych oraz zabezpieczone były minimum czterocyfrowym kodem PIN.

(akta kontroli str. 319)

2.2 Analiza zakresów obowiązków, uprawnień i odpowiedzialności 15 pracowników Starostwa[26] wykazała, że wszyscy, 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. 275-314)

2.3. Badaniem objęto uprawnienia do dostępu systemów informatycznych trzech osób, które w okresie objętym kontrolą zakończyły zatrudnienie w Urzędzie. Stwierdzono, że w jednym przypadku konto nie zostało zablokowane, pomimo ustania stosunku pracy tej osoby[27].

(akta kontroli str. 188)

2.4 Zabezpieczenia techniczne systemów informatycznych, przyjęte w Starostwie w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem opisano w PBI i PZSI. W dokumentach tych podano m.in., że dostęp do systemu operacyjnego zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem hasła i loginu. Ponadto określono m.in. zasady korzystania z sieci Internet i poczty elektronicznej; procedury nadawania i cofnięcia uprawnień; rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników systemu. Na podstawie oględzin[28] 11 komputerów stacjonarnych oraz pięciu laptopów stwierdzono, że przy logowaniu do domeny systemu Windows, dla wszystkich urządzeń, konieczne było wprowadzenie hasła użytkownika. Polityka dotycząca ustawień haseł zarządzana była centralnie. Ustalono minimalną długość i zawartość hasła . Użytkownik systemu zobowiązany był do zmiany hasła nie rzadziej niż co 30 dni. Hasło powinno było się różnić od 12 poprzednio używanych.

Ponadto wytypowane do badania trzy programy informatyczne[29], przy logowaniu, dodatkowo wymagały wprowadzenia kolejnego hasła.

We wszystkich ww. przypadkach nie wystąpiło automatyczne logowanie do komputera lub programu informatycznego bez wprowadzenia hasła oraz przypadki loginów, których nazwa nie pozwala na bezpośrednie powiązanie z daną osobą

(akta kontroli str. 17-18, 54-58, 188-198)

2.5. W trakcie oględzin stwierdzono, że ustawienie wszystkich pięciu wybranych monitorów na stanowiskach obsługi interesantów w zakresie rejestracji pojazdów i wydawania prawa jazdy zapewniało, że dane wyświetlane na ekranie nie były widoczne dla osób nieuprawnionych. Było to zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI, a także z § 4 pkt 3 ppkt 28 PZSI.

(akta kontroli str. 188-198)

2.6. Zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego zostały opisane m.in. w § 4 pkt 11 PZSI. Podano w nich m.in., że pracownicy zobowiązani byli do transportu sprzętu mobilnego w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności transportowania sprzętu komputerowego w bagażu podręcznym lub specjalnej tobie do tego przeznaczonej; nie pozostawiania sprzętu/bagażu w przechowalniach oraz w widocznym miejscu w samochodzie;

[26] W tym czterech na stanowiskach kierowniczych; dwóch pracowników, którzy w okresie objętym kontrolą zmienili komórkę organizacyjną lub stanowisko; dziewięć osób, które miało dostęp do systemów informatycznych wykorzystywanych przez Urząd.

[27] Por. stwierdzone nieprawidłowości.

[28] Przeprowadzonych 9 lipca 2024 r.

[29] 1) EWOPIS wersja 9.06 Gobid Katowice (program do prowadzenia ewidencji gruntów, budynków i lokali; 2) FKB+ System Finansowo-Księgowy Księgowości Budżetowej wersja 3.62.652 Radix Sp. z o.o.; 3) System Płace+ wersja 4.82.259 Radix Sp. z o.o

ochrony sprzętu przed uszkodzeniami fizycznymi. Starosta podał, że bezpieczną pracę w formie zdalnej gwarantowało łączenie się użytkownika za pośrednictwem szyfrowanego połączenia VPN[30], poprzez logowanie unikalnym identyfikatorem i hasłem. Szyfrowanie połączenia wykorzystywało silne algorytmy, a podłączenie tunelu VPN było ograniczone tylko i wyłącznie do potrzeb pracowniczych danego użytkownika.

(akta kontroli str. 62-63, 319-320)

2.7 Oględziny pięciu laptopów[31] wykazały, że były one zabezpieczone szyfrowaniem i wymagały wprowadzenia odpowiedniej długości i jakości hasła.

(akta kontroli str. 188-198)

2.8 Serwery wykorzystywane przez Urząd zlokalizowane były w wyodrębnionym pomieszczeniu (serwerowni), do którego dostęp mieli informatyk oraz najwyższe kierownictwo Starostwa. Pomieszczenie posiadało odpowiednie zabezpieczenia i wyposażenie[32]. Prowadzona była ewidencja wejść i wyjść.

(akta kontroli str. 188-198)

2.9 Badaniem objęto cztery umowy zawarte z podmiotami zewnętrznymi na zakup sprzętu informatycznego oraz sprawowanie opieki autorskiej nad jednym z systemów informatycznych wykorzystywanym w Urzędzie. Analiza wykazała, że nie zawarto w nich zapisów zobowiązujących wykonawcę do zachowania w tajemnicy informacji do jakich może mieć dostęp w związku z realizacją umowy[33].

(akta kontroli str. 245-273)

2.10 Procedury i zasady postępowania ze sprzętem informatycznym i nośnikami danych w przypadku naprawy, serwisu lub utylizacji sprzętu zostały opisane w § 4 pkt 10 PZSI. Zgodnie z jego treścią bieżąca naprawa i konserwacja sprzętu informatycznego wykonywana była przez informatyka. W przypadku realizacji usług przez podmiot zewnętrzny naprawy wykonywane powinny być przy bezpośrednim nadzorze informatyka (w siedzibie Starostwa) lub po zawarciu umowy o powierzenie przetwarzania danych osobowych (poza jego siedzibą). Podano w nim również, że wycofany z eksploatacji sprzęt mógł być zbywany dopiero po uśnięciu danych i nieodwracalnym zniszczeniu nośników zawierających dane osobowe, a uszkodzone urządzenia mogą być przekazywane w celu utylizacji właściwym podmiotom, z którymi zawarto umowę powierzenia przetwarzania.

(akta kontroli str. 61-62)

2.11-2.12. W Urzędzie ustalono zasady tworzenia i przechowywania kopii zapasowych w celu zapewnienia ciągłości działania systemu informatycznego. W § 4 pkt 7 PZSI szczegółowo określono sposób i częstotliwość ich wykonywania, miejsce i okres przechowywania. Jako osobę odpowiedzialną za ich tworzenie wskazano informatyka. Na podstawie oględzin[34] stwierdzono, że kopie zapasowe zbiorów danych i oprogramowania wykonywane były codziennie od poniedziałku do piątku. Kopie przechowywane były w czterech lokalizacjach (trzy kopie online oraz kopia offline przechowywana w zamkniętym sejfie). Nie testowano regularnie sprawdzenia utworzonych kopii zapasowych danych i oprogramowania[35].

[30] Tj. wirtualna sieć prywatna (ang. virtual private network).
[31] Przeprowadzone 9 lipca 2024 r.
[32] Co potwierdziły przeprowadzone 9 lipca 2024 r. oględziny.
[33] Por. stwierdzone nieprawidłowości.
[34] Przeprowadzonych 9 i 16 lipca 2024 r.
[35] Por. stwierdzone nieprawidłowości.

(akta kontroli str. 59, 184-198)

2.13. Starostwo posiadało program do monitorowania zajętości pamięci serwerów. W przypadku wystąpienia problemów dotyczących pojemności serwerów informatyk otrzymywał maile z komunikatami i raportami. Ustalono, że zajętość dysków wynosiła[36]: serwera kopii zapasowych 69,4%; serwera fizycznego maszyn wirtualnych na pierwszej macierzy 74% oraz na drugiej 60,2%; serwera wirtualnego 59,5%.

(akta kontroli str. 184-187)

2.14. W Urzędzie zidentyfikowano i zabezpieczono pod kątem wpływu czynników zewnętrznych, kluczowe elementy infrastruktury i usługi informatyczne w celu zapewnienia ciągłości działania. M.in. fizyczne elementy infrastruktury IT były podtrzymywane przez UPS oraz podłączone były do agregatu prądotwórczego. Zastosowano również urządzenia sieciowe typu switch, zaporę sieciową oraz środki ochrony przed szkodliwym oprogramowaniem. Starosta podał, m.in., że odtworzenie infrastruktury z kopii zapasowych (w tym aplikacji i baz danych), przy ewentualnej awarii jednego z serwerów fizycznych wynosić będzie od jednej do czterech godzin[37].

(akta kontroli str. 17-18, 60, 161-162, 320-321)

Stwierdzone nieprawidłowości

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

1. W okresie od 1 września 2023 r. do 3 lipca 2024 r. konto jednego z byłych pracowników Urzędu, spośród trzech objętych badaniem, nie było zablokowane, pomimo ustania stosunku pracy tej osoby 31 sierpnia 2023 r. Było to niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI (oraz § 20 ust. 2 pkt 5 rozporządzenia KRI z 2012 r.) stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Ponadto, było to niezgodne z § 4 pkt 3 ppkt 22) PZSI tj. procedury nadawania, zmiany i cofnięcia uprawnień do przetwarzania danych w systemie informatycznym. Zgodnie z treścią ww. przepisu w przypadku konieczności cofnięcia lub zmiany uprawnień lub zmiany zakresu uprawnień do systemu informatycznego z związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończenia pracy i współpracy jego bezpośredni przełożony lub pracownik koordynujący działania danej osoby wnioskuje do informatyka o dokonanie tej czynności. Wzór wniosku o nadanie/cofnięcie uprawnień stanowił załącznik nr 4 do PZSI.

(akta kontroli str. 188-198)

Starosta wyjaśnił, m.in., że powyższa nieprawidłowość wynikła z niedopatrzenia, natomiast osoba ta po przejściu na emeryturę nie miała fizycznego dostępu do komputera i systemy informatyczne nie były w żaden sposób zagrożone. Starostwo planuje usprawnić komunikację pomiędzy działem kadr i administratorem systemów informatycznych.

(akta kontroli str. 319)

2. We wszystkich czterech umowach objętych badaniem, zawartych przez Starostwo, z podmiotami zewnętrznymi na zakup sprzętu informatycznego oraz sprawowanie

[36] Na podstawie oględzin 16 lipca 2024 r.

[37] System zarządzania tożsamością (Active Directory) – 1 h; system aplikacji i baz danych geodezyjnych – 4 h, (wszystkie systemy oprócz bazy skanów, która potrzebowała do otworzenia 24 h); system aplikacji i baz danych GEOPORTAL – 3 h; system aplikacji i baz dany księgowych – 3 h.

usługi opieki autorskiej nad jednym z systemów informatycznych wykorzystywanych w Urzędzie, nie zawarto zapisów zobowiązujących wykonawcę do zachowania w tajemnicy informacji do jakich może mieć dostęp w związku z realizacją umowy. Było to niezgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI (oraz § 20 ust. 2 pkt 10 rozporządzenia KRI z 2012 r.) który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(akta kontroli str. 245-272)

Starosta wyjaśnił, m.in., że nie umieszczano takich zapisów, ponieważ dotychczas nie dochodziło do sytuacji, w których taki dostęp mógłby uzyskać wykonawca. W celu zagwarantowania odpowiedniego poziomu bezpieczeństwa informacji, Urząd wdroży działania gwarantujące prawidłowe zabezpieczenie danych, m.in. stosując zapisy zobowiązujące wykonawcę do zachowania w tajemnicy informacji, do jakich może mieć on dostęp.

(akta kontroli str. 320)

3. W latach 2023-2024 (II kw.) w Urzędzie nie testowano regularnie sprawdzenia utworzonych kopii zapasowych danych i oprogramowania. Było to niezgodne z § 4 pkt 7 ppkt 10 PZSI, który stanowi, że w celu zweryfikowania poprawności wykonania kopii zapasowych wykonuje się testy odtwarzania.

(akta kontroli str.188-198)

Starosta wyjaśnił, m.in., że kopie zapasowe były na bieżąco weryfikowane i monitorowane na podstawie raportów, powiadomień i logów z wykonania kopii. Raporty, powiadomienia i logi wskazywały czy kopia została wykonana poprawnie. Kopie zapasowe były wielokrotnie odtwarzane – nie były to swoiste testy kopii zapasowych, a odtwarzanie na potrzeby produkcyjne. Starostwo wdroży plan testów kopii zapasowych i wprowadzi ten plan do polityk bezpieczeństwa, oraz będzie prowadzić na tę okoliczność dokumentację.

(akta kontroli str. 320)

NIK zauważa, że testowanie polega na sprawdzeniu, czy wykonana kopia zapasowa nie zawiera błędów oraz czy dane zostaną odtworzone w sposób prawidłowy.

OCENA CZĄSTKOWA

Zabezpieczenia techniczne systemów informatycznych, przyjęte w Starostwie zapewniały ochronę przetwarzanych informacji przed nieuprawnionym dostępem. Ustawienie monitorów objętych badaniem zapewniało, że dane wyświetlane na ekranie nie były widoczne dla osób nieuprawnionych. Prawidłowo opracowano zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego oraz dokonywano na nim szyfrowania danych. Zarządzano pojemnością serwerów w sposób gwarantujący wydajność systemów a pomieszczenie serwerowni posiadało odpowiednie zabezpieczenia. Prawidłowo tworzono i przechowywano kopie zapasowe zbiorów danych, programów i oprogramowania systemowego zapewniające ciągłość działania systemu informatycznego, jednak nie były regularnie testowane. Negatywnie oceniono również nieprzestrzeganie procedury nadawania/zmiany/cofnięcia uprawnień do systemów informatycznych oraz niezawieranie w umowach z podmiotami zewnętrznymi zapisów zobowiązujących wykonawców do zachowania poufności.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji.

Opis stanu faktycznego

3.1 W Urzędzie przeprowadzono analizę ryzyka[38] utraty integralności, dostępności lub poufności informacji, o której mowa w § 19 ust 2 pkt 3 rozporządzenia KRI. Analiza wykazała, że podjęto działania minimalizujące ryzyka, stosownie do wyników i zaleceń.

(akta kontroli str. 121-159)

3.2 Starostwo posiadało opracowaną procedurę zgłaszania incydentów naruszenia bezpieczeństwa informacji (PZI), której celem było zapewnienie, monitorowania zdarzeń związanych z bezpieczeństwem informacji oraz słabości systemów informacyjnych, a także możliwość zgłaszania i szybkiego podejmowania działań korygujących. Procedura została przedstawiona do zapoznania się i stosowania pracownikom Urzędu. Starosta podał, że w latach 2023-2024 (II kw.) nie wystąpiły przypadki incydentów z zakresu naruszenia bezpieczeństwa informacji.

(akta kontroli str. 90-105)

3.3 W latach 2023-2024 (II kw.) przeprowadzono po jednym szkoleniu w danym roku, tylko z zakresu ochrony danych osobowych. Przeszkolonych zostało 15 radnych powiatu oraz 17 osób spośród 65 zatrudnionych w Urzędzie[39]. W ww. okresie nie przeprowadzano szkoleń osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem zagadnień, o których mowa w § 19 ust. 2 pkt 6 lit. a) - c) rozporządzenia KRI (§ 20 ust. 2 pkt 6 lit. a) - c) rozporządzenia KRI z 2012 r.)[40].

(akta kontroli str. 240-244)

3.4 W okresie objętym kontrolą w Urzędzie nie przeprowadzano audytu wewnętrznego z zakresu bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI (§ 20 ust. 2 pkt 14 rozporządzenia KRI z 2012 r.)[41].

(akta kontroli str. 183)

Stwierdzone nieprawidłowości

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

1. W latach 2023-2024 (II kw.) nie przeprowadzano szkoleń pracowników Starostwa zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem zagadnień, o których mowa w § 19 ust. 2 pkt 6 lit. a) - c) rozporządzenia KRI (oraz § 20 ust. 2 pkt 6 lit. a) - c) rozporządzenia KRI z 2012 r.). Zgodnie z ww. przepisem szkolenie powinno uwzględniać m.in. następujące zagadnienia: zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawną, stosowanie środków zapewniających bezpieczeństwo informacji (np. szyfrowanie dysków, szyfrowanie kluczy USB, dostęp do systemów IT po podaniu hasła).

(akta kontroli str. 121, 240-244)

Starosta wyjaśnił, że pracownicy Starostwa byli szkoleni stanowiskowo w przypadkach obejmowania obowiązków oraz rozpoczęcia pracy z systemem informatycznym. Niestety brak już wcześniej wspomnianej dokumentacji dotyczącej nadawania uprawnień nie pozwala tego odpowiednio udowodnić. Ścisły plan szkoleń zostanie wprowadzony do Polityk Bezpieczeństwa Starostwa oraz szkolenia te będą

[38] W okresie od 11 do 18 grudnia 2023 r.
[39] Liczba użytkowników systemów informatycznych wg stanu na 31 grudnia 2023 r.
[40] Por. stwierdzone nieprawidłowości.
[41] Por. stwierdzone nieprawidłowości.

wykonywane minimum raz do roku. Ponadto przeprowadzenie szkoleń z ww. zakresu zostało zaplanowane w realizacji projektu Cyberbezpieczny Samorząd, co pokazuje potrzebę przeprowadzania takich szkoleń i świadomość Urzędu w tym zakresie.

(akta kontroli str. 321)

NIK zauważa, że szkolenia stanowiskowe nie wypełniają obowiązków określonych w rozporządzeniu KRI. Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów naruszenia bezpieczeństwa informacji. Szkolenia osób zaangażowanych w proces przetwarzania informacji powinny być prowadzone cyklicznie w związku ze zmieniającymi się zagrożeniami oraz stosowanymi zabezpieczeniami technicznymi i organizacyjnymi.

2. W latach 2023-2024 (II kw.) w Urzędzie nie przeprowadzano audytu wewnętrznego z zakresu bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI. Zgodnie z ww. przepisem przedmiotowy audyt powinien być przeprowadzany nie rzadziej niż raz na rok.

(akta kontroli str. 183)

Starosta wyjaśnił, że ww. audyt nie został przeprowadzony, ponieważ nie zostały zabezpieczone środki w budżecie Powiatu na ten cel. Niemniej, Starostwo zamierza taki audyt przeprowadzić.

(akta kontroli str. 322)

OCENA CZĄSTKOWA

Urząd prawidłowo przeprowadził analizę ryzyka utraty integralności, dostępności lub poufności informacji oraz podjął działania adekwatnie do jej wyników. Opracowana procedura zgłaszania incydentów naruszenia bezpieczeństwa informacji została przedstawiona do zapoznania się i stosowania pracownikom Urzędu, co NIK ocenia pozytywnie. Jako działania nieprawidłowe uznano niezapewnianie szkoleń pracownikom Starostwa zaangażowanych w proces przetwarzania informacji oraz nieprzeprowadzenie, wymaganego przepisami, audytu wewnętrznego z zakresu bezpieczeństwa informacji.

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

Najwyższa Izba Kontroli nie formułuje uwag.

Wnioski

1. Opracowanie planu odtworzeniowego oraz określenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych.
2. Dokonywanie przeglądów i aktualizacji dokumentów składających się na SZBI.
3. Prawidłowe nadawanie/zmiany/cofnięcia uprawnień do systemów informatycznych.
4. Uwzględnianie w umowach zawieranych z podmiotami zewnętrznymi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
5. Regularne testowanie kopii zapasowych.
6. Zapewnienie odpowiednich szkoleń pracowników Starostwa zaangażowanych w proces przetwarzania informacji.
7. Przeprowadzanie audytu wewnętrznego z zakresu bezpieczeństwa informacji.

V.Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w 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 wykonania wniosków

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

Bydgoszcz, 17 września 2024 r.

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

Kontroler
(-) Robert Elwertowski
główny specjalista kontroli państwowej