NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA.410.14.6.2024

Pan
Leszek Bizoń
Starosta Wodzisławski
ul. Bogumińska 2
44-300 Wodzisław Śląski

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
T +48 32 784 42 00, F +48 32 784 42 30
lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Wodzisławiu Śląskim, ul. Bogumińska 2, 44-300 Wodzisław Śląski[1].
Kierownik jednostki kontrolowanej	Leszek Bizoń, Starosta Wodzisławski od 21 listopada 2018 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, tj. do dnia 9 września 2024 r. (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontrolerzy	1. Jacek Kordanowski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/115/2024 z dnia 22 maja 2024 r. 2. Marta Florczykiewicz-Cymara, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/116/2024 z dnia 22 maja 2024 r. 3. Szymon Gruca, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/117/2024 z dnia 22 maja 2024 r. (akta kontroli str. 1-6)

[1] Dalej: Starostwo lub Urząd.
[2] Dalej: Starosta.
[3] Dz.U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W Starostwie prawidłowo opracowano i wdrożono procedury mające na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych, procedury te były aktualizowane. Zapewniono również odpowiednie zasoby kadrowe dla zachowania bezpieczeństwa informacji i ciągłości działania z jednoczesnym przypisaniem obowiązków / odpowiedzialności w tym zakresie.

Pomimo wynikającego z przyjętych procedur obowiązku testowania scenariuszy postępowania w przypadku awarii serwerów bądź awarii elementów aktywnych sieci informatycznej, testy te przeprowadzono dopiero w toku kontroli NIK (tj. po 16 miesiącach od przyjęcia ww. procedur); niezgodnie z obowiązującymi regulacjami dokonano również udostępnienia wszystkim pracownikom Starostwa szczegółowych zasad zarządzania środowiskiem informatycznym.

Starostwo, prawidłowo wdrożyło przyjęte rozwiązania organizacyjne w zakresie ochrony bezpieczeństwa informacji. Wykorzystywane w Starostwie systemy informatyczne oraz osprzęt informatyczny były zabezpieczane hasłami dostępu; pomieszczenia krytycznej infrastruktury informatycznej (serwerownie) były zabezpieczone przed dostępem osób postronnych, serwery Starostwa były zabezpieczone przed nagłą utratą zasilania w urządzenia podtrzymujące zasilanie.

Znajdujące się na wyposażeniu Starostwa komputery były chronione oprogramowaniem obejmującym m.in. ochronę systemu plików, system zapobiegania włamaniom (IPS), ochronę przed atakami z sieci (IDS), firewall, ochronę dostępu do stron internetowych i poczty e-mail.

Dostęp do pomieszczeń i systemów informatycznych został ograniczony do osób upoważnionych; w jednej z serwerowni Starostwa nie dokonywano wymaganych procedurami wpisów o osobach niebędących pracownikami Starostwa, które przebywały w serwerowni pod nadzorem upoważnionego pracownika. Pomieszczenia serwerowni oraz narzędzia informatyczne, w tym systemy informatyczne zostały zabezpieczone kontrolą dostępu. W dwóch poddanych oględzinom pomieszczeniach serwerowni znajdowały się materiały łatwopalne, co zwiększało ryzyko utraty danych bądź przerwania ciągłości operacji na skutek pożaru.

W Starostwie zapewniono bezpieczeństwo danych m.in. poprzez sporządzanie i przechowywanie kopii zapasowych, które były poddawane testowaniu oraz identyfikację kluczowych elementów infrastruktury informatycznej.

W Jednostce prowadzono również analizy ryzyka w zakresie zapewnienia ciągłości działania oraz przeprowadzono stosowne audyty. Pracownicy Starostwa byli przeszkoleni w zakresie zapewnienia bezpieczeństwa informacji. Starostwo prowadziło również rejestr incydentów oraz dokumentację z tym związaną.

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

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR 1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych.

1.1. W Starostwie zidentyfikowano 94 zbiory przetwarzanych danych podlegające zabezpieczeniu; zbiory te pozostawały, w części, w wyłącznej administracji przez Starostowo lub Powiatowy Zespół do Spraw Orzekania o Niepełnosprawności albo były zasobami powierzonymi gdzie głównym administratorem zbioru danych był podmiot zewnętrzny; wszystkim zbiorom nadano odpowiedni poziom ochrony.

(akta kontroli str. 19-21)

Jak wyjaśnił Starosta cyt. *(…) zbiorom nadano poziomy bezpieczeństwa w systemie informatycznym zgodnie z uchylonym już Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Celem ujednolicenia oraz zastosowania tożsamych poziomów bezpieczeństwa w systemie informatycznym dla zbiorów danych osobowych utworzonych po uchyleniu w/w rozporządzenia w Starostwie Powiatowym stosuje się nomenklaturę stosowaną w rozporządzeniu z dnia 29 kwietnia 2004 r.*

(akta kontroli str. 11)

1.2. W Starostwie, zgodnie z § 20 ust. 1 w związku z ust. 3 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[6], opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji (SZBI).

W okresie od 25 maja 2018 r. do 22 stycznia 2023 r. obowiązywała Polityka Bezpieczeństwa Informacji w Starostwie Powiatowym w Wodzisławiu Śląskim[7] przyjęta zarządzeniem nr 28/2018 Starosty z dnia 25 maja 2018 r; zarządzeniem nr 9/2023 Starosty z dnia 23 stycznia 2023 r. dokonano jej aktualizacji.

(akta kontroli str. 22-71)

Pracownicy i kadra kierownicza Starostwa zostali zapoznani z PBI za pośrednictwem Systemu Obiegu Dokumentów (SOT) oraz wewnętrznej sieci Intranetowej w dniach wejścia w życie tych procedur. Przypomnienie zasad bezpieczeństwa informacji nastąpiło również za pośrednictwem wewnętrznej sieci intranetowej w dniach: 9 listopada 2021 r., 16 lutego 2022 r. oraz 12 lutego 2024 r.

(akta kontroli str. 72-112)

[5] 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.

[6] Dz.U. z 2017 r., poz. 2247 obowiązujące do dnia 22 maja 2024 r. Od 23 maja 2024 r. zastąpione przez rozporządzenie Rady Ministrów z dnia 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 (Dz.U. z 2024, poz. 773), dalej KRI.

[7] Dalej: PBI.

Wykonanie zarządzeń dot. PBI zostało powierzone Sekretarzowi Powiatu. Do obowiązków Sekretarza, zgodnie z PBI należało proponowanie Administratorowi szczegółowych procedur i zabezpieczeń określających środki techniczne i organizacyjne pozwalające zapewnić bezpieczeństwo informacji oraz ograniczenie do akceptowalnego poziomu ryzyka naruszenia praw lub wolności osób, których dane przetwarzane są w Starostwie. Procedury PBI przewidywały również nadzór Sekretarza m.in. nad: fizycznym zabezpieczeniem pomieszczeń, w których przechowywane są przetwarzane dane, właściwym zarządzaniem hasłami użytkowników, systemami antywirusowymi i innymi zabezpieczeniami, nad wykonywaniem kopii zapasowych, obiegiem dokumentów, prawidłowością archiwizacji oraz usuwania danych osobowych, zapewnieniem dostępu osób zatrudnionych przy przetwarzaniu danych osobowych, ustawieniem monitorów komputerowych, dokumentacją opisującą sposób przetwarzania danych osobowych, nad doskonaleniem PBI i SZBI oraz nad procesem analizy ryzyka na potrzeby określenia odpowiednich środków technicznych i organizacyjnych pozwalających zapewnić akceptowalny poziom bezpieczeństwa przetwarzanych danych, w tym osobowych.

(akta kontroli str. 22-71)

W Starostwie opracowano następujące procedury, które wraz z PBI stanowiły system zarządzania bezpieczeństwem informacji:

- Zabezpieczenia fizyczne – obowiązująca od 25 maja 2018 r.,
- Zabezpieczenia sprzętowe, informatyczne i telekomunikacyjne - obowiązująca od 25 maja 2018 r.,
- Nadawanie i rejestrowanie uprawnień do systemów informatycznych – obowiązująca od 25 maja 2018 r.,
- Uwierzytelnianie w systemach informatycznych, wersja druga – obowiązująca od 1 grudnia 2021 r.,
- Utrzymanie i ewidencja systemów informatycznych – obowiązująca od 25 maja 2018 r.,
- Kopie zapasowe, wersja pierwsza – obowiązująca do 25 maja 2018 r., wersja druga – obowiązująca od 20 marca 2023 r.,
- Zarządzanie sprzętem komputerowym i oprogramowaniem – obowiązująca od 25 maja 2018 r.,
- Korzystanie z Internetu i poczty elektronicznej – obowiązująca od 25 maja 2018 r.,
- Przetwarzanie danych osobowych w ramach projektów finansowanych ze środków zewnętrznych – obowiązująca od 8 października 2018 r.,
- Wykorzystanie systemów informatycznych przy pracy zdalnej, wersja druga – obowiązująca od 30 marca 2020 r.,
- Zarządzanie ciągłością działania – obowiązująca od 24 stycznia 2023 r.

Powyższe procedury zostały zatwierdzone przez Starostę i zakomunikowane pracownikom poprzez ich zamieszczenie w wewnętrznym intranecie; procedura *Zarządzanie ciągłością działania,* zawierająca informacje w zakresie lokalizacji i rodzajów serwerów oraz urządzeń/elementów sieci aktywnej Urzędu, została udostępniona wszystkim pracownikom, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

Każdy nowy pracownik zatrudniany w Starostwie odbywał szkolenie w ramach którego zapoznawał się z przepisami o ochronie danych osobowych

oraz obowiązującym w Starostwie systemem zarządzania bezpieczeństwem informacji, w tym z PBI.

(akta kontroli str. 112-171)

1.3. W Starostwie sporządzono dokumentację w zakresie ochrony danych osobowych, która stanowiła element składowy PBI, zawarto w niej zasady przetwarzania danych osobowych, w tym zasady wydawania upoważnień do ich przetwarzania, a także informacje o zasadach szkolenia osób zaangażowanych w proces przetwarzania danych osobowych.

PBI zawierało informację, o prowadzonych przez Starostwo rejestrach czynności przetwarzania danych osobowych (RCP) oraz rejestrze kategorii czynności przetwarzania dokonywanych w imieniu administratora (RKCP).

PBI zawierała również informacje dotyczące realizacji przez Starostwo obowiązku informacyjnego w stosunku do osób, których dane były przetwarzane.

(akta kontroli str. 57-58, 65-69)

1.4. W dniu 15 lutego 2023 r. Starosta zaakceptował dokument pn. *Analiza ryzyka ogólnego i ocena skutków dla przetwarzania danych (DPIA) w Starostwie Powiatowym w Wodzisławiu Śląskim*[8]. Dokumentem tym wprowadzono do Jednostki procedurę szacowania ryzyka w stosunku do aktualnie prowadzonych, jak i planowanych operacji przetwarzania danych osobowych. Zgodnie z informacjami zaprezentowanymi w Analizie, proces szacowania ryzyka oparto na normach ISO PN-EN ISO/IEC 27002:2017, ISO PN-EN ISO/IEC 27005:2014-01 oraz w oparciu o Wytyczne Grupy Roboczej dotyczących oceny skutków dla ochrony oraz pomagających ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679 z dnia 4 października 2017 r.

W ramach Analizy Starostwo dokonało identyfikacji aktywów w podziale na aktywa podstawowe i wspierające na które składały się zdefiniowane odpowiednio:

- informacje oraz operacje przetwarzania,
- sprzęt, nośniki danych (papierowe i elektroniczne), oprogramowanie, okablowanie, personel i lokalizację.

Jednostka zidentyfikowała również zagrożenia, które usystematyzowała w ośmiu grupach: 1/ zniszczenia fizyczne (pożar, zalanie, zanieczyszczenie, poważny wypadek, zniszczenie urządzeń lub nośników, pył, korozja, wychłodzenie); 2/ zjawiska naturalne (zjawiska klimatyczne, zjawiska sejsmiczne, zjawiska wulkaniczne, zjawiska pogodowe, powódź), 3/ utrata podstawowych usług (awaria systemu klimatyzacji lub dostaw wody, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego), 4/ zakłócenia spowodowane promieniowaniem (promieniowanie elektromagnetyczne, promieniowanie cieplne, impuls elektromagnetyczny), 5/ naruszenia bezpieczeństwa informacji (przechwycenie sygnałów na skutek zjawiska interferencji, szpiegostwo zdalne, podsłuch, kradzież nośników lub dokumentów, kradzież urządzenia, odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników, ujawnienie, dane z niewiarygodnych źródeł, manipulowanie urządzeniem, sfałszowanie oprogramowania, detekcja umiejscowienia, 6/ awarie techniczne (awaria urządzenia, niewłaściwe funkcjonowanie urządzeń, przeciążenie systemu informacyjnego, niewłaściwe funkcjonowanie oprogramowania, naruszenie zdolności utrzymania systemu informacyjnego, 7/ nieautoryzowane działania (nieautoryzowane użycie urządzeń, nieuprawnione kopiowanie oprogramowania, użycie fałszywego lub skopiowanego

[8] Dalej: Analiza.

oprogramowania, zniekształcenie danych, nielegalne przetwarzanie danych), 8/ naruszenia bezpieczeństwa funkcji (błąd użytkowania, naruszenie praw, fałszowanie praw, odmowa działania, naruszenie dostępności personelu).

W Starostwie zidentyfikowano również podatność wystąpienia zdarzenia w organizacji według skali od 1 do 4, gdzie 1, to zdarzenie nieprawdopodobne, a 4 to zdarzenie niemal pewne; zidentyfikowano również według czterostopniowej skali skutki zdarzeń wraz z opisem ich następstw. Poziom wyliczanego ryzyka stanowił iloczyn wartości przypisanej prawdopodobieństwu wystąpienia zdarzenia oraz skutków jakie wywołało.

(akta kontroli str. 174-248)

Jak wskazał Starosta, cyt. (…) *w celu zachowania ciągłości działania oraz zapewnienia optymalnego bezpieczeństwa informacji w starostwie przeprowadzono szacowanie ryzyka ogólnego i oceny skutków dla przetwarzania danych. Proces szacowania ryzyka poprzedzono identyfikacją aktywów organizacji, zagrożeń dla aktywów, zabezpieczeń stosowanych w organizacji, podatności (prawdopodobieństwa) oraz następstw (skutków) mogących wystąpić zdarzeń. W ramach identyfikacji aktywów we współpracy z naczelnikami i kierownikami starostwa zidentyfikowano czynności przetwarzania, które stanowią obszar ryzyka mający wpływ na bezpieczeństwo informacji w tym na ciągłość działania systemów informatycznych. Wśród aktywów (czynności przetwarzania) wskazano 82 czynności przetwarzania danych osobowych uwzględnionych w „Rejestrze Czynności Przetwarzania" zgodnie z art. 30 RODO oraz 36 czynności przetwarzania stanowiących inny obszar ryzyka niż przetwarzanie danych osobowych. W/w czynności przetwarzania danych osobowych poddano analizie zgodnie z wytycznymi Grupy Roboczej art. 29 WP 248 rew.01 17/PL w celu podjęcia decyzji o konieczności oceny skutków dla przetwarzania danych. Następnie sklasyfikowano i przydzielono podobne operacje przetwarzania do ustalonych grup przetwarzania. Do szacowania ryzyka wybrano metodę CRAMM – popularną metodę jakościową która sprowadza się do iloczynu prawdopodobieństwa (podatności) wystąpienia zdarzenia i wielkości jego skutków. Atrybuty wykorzystywane w procesie szacowania ryzyka to poufność, integralność i dostępność. Wraz z aktywami pomocniczymi (sprzęt, nośniki danych, personel, itd.), zidentyfikowanymi zagrożeniami (awarie, zniszczenia, naruszenia, zjawiska naturalne, itd.) w oparciu o w/w atrybuty zestawiono macierz w celu dokonania analizy i oceny ryzyka. Na postawie wyliczonego w ten sposób ryzyka podjęto decyzję o próbie jego redukcji. W tym celu wystosowano zalecenie co do postępowania z ryzykiem w wyniku czego powstał „Plan postępowania z ryzykiem ".*

(akta kontroli str. 13)

1.5. W Starostwie, od 24 stycznia 2023 r., obowiązywała procedura *Zarządzanie ciągłością działania*. Zgodnie z zapisami ww. procedury działania przewidziane w scenariuszach planu ciągłości działania w zakresie systemów informatycznych wykonują pracownicy Biura Informatyki.

(akta kontroli str. 159-171, 500-502)

1.6. Integralną częścią procedury *Zarządzanie ciągłością działania* stanowiły załączone do niej scenariusze postępowania w przypadku awarii serwera oraz infrastruktury aktywnej sieci.

Scenariusz postępowania w przypadku awarii zawierał informacje o lokalizacji serwerów (nazw, adresów IP, systemów operacyjnych oraz VM) w poszczególnych budynkach Starostwa. W scenariuszu opisano działania jakie należy podejmować w przypadku awarii każdego z tych serwerów. Warianty postępowania obejmowały

samodzielne podjęcie prób rozwiązania problemu (np. w oparciu o kontekstowy system pomocy lub instrukcję czy też odtworzenie bazy danych z kopii zapasowej), usuwanie awarii w porozumieniu z gwarantem w ramach długoterminowej usługi gwarancyjnej bądź powiadomienie serwisu gwarancyjnego (scenariusz zawierał dane kontaktowe do serwisów).

Scenariusz postępowania w przypadku awarii sieci zawierał spis urządzeń (switch) wraz ze wskazaniem ich lokalizacji. W scenariuszu wskazano ścieżkę do serwera na którym znajdowały się pliki konfiguracyjne do aktywnych urządzeń; przewidywał on również zasady postępowania w przypadku awarii switchy, routerów, konwerterów światłowodowych i łącza internetowego.

W scenariuszach nie określono akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych urzędu.

Jak wskazał Starosta, (…) *w praktyce przyjmuje się, że działanie zmierzające do przywrócenia ciągłości działania systemów informatycznych są podejmowanie niezwłocznie po stwierdzeniu dysfunkcji systemu informatycznego. W umowach na usługi serwisowe świadczone przez podmioty zewnętrzne w praktyce stosuje się zapisy dotyczące czasu reakcji serwisu lub wymaganego czasu usunięcia problemu.*

(akta kontroli str. 159-171)

W zawartej przez Starostwo, z zewnętrznym dostawcą, umowie dzierżawy[9] łącza światłowodowego między budynkami Starostwa określono czas reakcji na zgłoszenie awarii jako bezzwłoczny, a maksymalny czas usunięcia awarii w przypadkach szczególnie złożonych określono na sześć godzin. Z kolei w zawartej umowie[10] na usługę przedłużenia gwarancji dla serwera Starostwa czas reakcji na awarię określono na następny dzień roboczy

(akta kontroli str. 466-473)

Ponadto w procedurze SZBI - *Kopie zapasowe,* wskazano, że kopie zapasowe danych przechowywanych na serwerach sieciowych są wykonywane i przechowywane przez ASI.

(akta kontroli str. 156-158)

Zgodnie z zawartym przez Starostwo - Powiatowe Centrum Zarządzania Kryzysowego w Wodzisławiu Śląskim (PCZK) z dostawcą energii elektrycznej porozumieniem[11] z dnia 25 października 2021 r., dostawca zobowiązał się do przekazywania PCZK mających lub mogących mieć istotne znaczenie dla zarządzania kryzysowego na obszarze powiatu wodzisławskiego zagrożeń. Informacje te zostały określone jako: awarie skutkujące przerwami w dostarczaniu energii elektrycznej, przerwy w dostarczaniu takiej energii, innych zagrożeń poprawnego funkcjonowania gospodarki i bezpieczeństwa obywateli powiatu. W ramach PCZK, zgodnie z porozumieniem, funkcjonowało stanowisko Dyżurnego PCZK, któremu dostawca energii elektrycznej zobowiązany był podawać informacje w zakresie przewidywanego czasu wznowienia dostarczenia energii elektrycznej w miejscu zdarzenia.

(akta kontroli str. 474-485)

[9] Nr WOA.2635.31.2023 z dnia 5 grudnia 2023 r.
[10] Nr WOA.042.4.7.2023 z dnia 13 maja 2024 r.
[11] Nr WOZ.5533.6.2021.

1.7. Zgodnie z pkt 6 procedury *Kopie zapasowe* w przypadku negatywnego wyniku testu kopii zapasowej ASI wykonuje kopie ponownie i ponownie ją sprawdza, aż do uzyskania pozytywnego wyniku testu kopii zapasowej.

(akta kontroli str. 156-158)

Rejestr kancelaryjny prowadzony przez Starostwo zawierał zestawienie protokołów z odtwarzania kopii zapasowych. Analiza wybranych protokołów z tych czynności wykazała, że zawierały one informacje o odtwarzanym nośniku, użytym do tego oprogramowaniu, danych odtwarzanej kopii zapasowej, miejscu odtworzenia, jego rodzaju i rezultacie, a także dacie odtworzenia i testującym.

(akta kontroli str. 249-256)

Jak wyjaśnił Starosta, (…) *zgodnie z procedurą SZBI: Kopie zapasowe, (…) w Starostwie wykonuje się kopie kompletnych maszyn wirtualnych oraz plików z udziałów sieciowych znajdujących się na hostach. (…). Testowanie odbywa się cyklicznie po wykonaniu kopii miesięcznych i polega na odtworzeniu kompletnej maszyny wirtualnej z kopii oraz dokonaniu próby jej uruchomienia na zapasowym serwerze, a w przypadku plików z udziałów sieciowych na odtworzeniu pliku z kopii i dokonaniu próby odczytu pliku. Pomyślne uruchomienie odtworzonej z kopii maszyny wirtualnej jest jednoznaczne z odzyskaniem działania maszyny w przypadku utraty ciągłości jej działania związanej np. z awarią serwera. Pomyślne odczytanie odtworzonego z kopii pliku na udziale sieciowym jest jednoznaczne z możliwością jego udostępnienia właściwemu użytkownikowi. Powyższe działania są zgodne ze scenariuszem postępowania w przypadku awarii serwera określonym w załączniku do procedury SZBI: Zarządzanie ciągłością działania.*

(akta kontroli str. 14)

Zgodnie z punktem 6 procedury *Zarządzanie ciągłością działania,* poszczególne scenariusze planów ciągłości testowane są w celu weryfikacji pod kątem poprawności działania przewidzianego scenariusza.

Od dnia obowiązywania Procedury *Zarządzanie ciągłością działania,* tj. 24 stycznia 2023 r., do czasu wszczęcia kontroli, nie przeprowadzano testów żadnego ze scenariuszy planów ciągłości działania, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 159-161)

W trakcie prowadzonej kontroli, tj. w dniach 5 i 6 czerwca 2024 r. przeprowadzono testy, w ramach których zasymulowano awarię:

- systemu udostępniającego usługi ewidencji gruntów GEOINFO i.EGIB; weryfikacji poddano również aktualność wskazanego w scenariuszu numeru telefonu,
- utraty dostępu do Internetu WiFi na Sali Prezydenckiej, awarię routera do udostępnienia sieci Internet; weryfikacji poddano również aktualność wskazanego w scenariuszu numeru telefonu.

Powyższe zostało udokumentowane stosownymi notatkami służbowymi na których podpisali się wykonujący test – Główny administrator baz danych, nadzorujący test - Kierownik Biura Informatyki oraz zatwierdzający test – Sekretarz Powiatu.

(akta kontroli str. 464-465)

1.8. Zgodnie z § 17 obowiązującej PBI analizę ryzyka utraty integralności, dostępności lub poufności informacji przeprowadza się co najmniej raz w roku w terminie do dnia 20 listopada każdego roku.

(akta kontroli str. 63)

W dniu 7 sierpnia 2023 r. Sekretarz Powiatu, działając na podstawie § 15 ust. 3 lit. m PBI dokonał okresowej analizy ryzyka utraty integralności, dostępności, lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko. W wyniku analizy wskazał na zasadność sformalizowania procedur opisujących zasady szacowania oraz progi akceptowalności ryzyka oraz na konieczność uwzględnienia w budżecie Projektu *Cybernetyczny Samorząd wydatku na* zaktualizowanie dokumentacji w powyższym zakresie.

(akta kontroli str. 325)

W dniu 19 kwietnia 2024 r. Starostwo opracowało i wysłało do Państwowego Instytutu Badawczego NASK tzw. Ankietę Dojrzałości Cyberbezpieczeństwa w JST; ankieta zawierała dane z zakresu zarządzania, SZBI, ochrony danych, monitorowania zdarzeń (incydentów), reagowania na incydenty, odtwarzania danych, infrastruktury i komunikacji.

(akta kontroli str. 315-324)

W okresie objętym kontrolą, w dniu 20 marca 2023 r. została zaktualizowana, obowiązująca w ramach SZBI, procedura *Kopie zapasowe*.

(akta kontroli str. 134-136, 156-158)

1.9. W Starostwie, za bezpieczeństwo informacji oraz zapewnienie ciągłości działania odpowiedzialny był Sekretarz Powiatu.

(akta kontroli str. 44)

Zgodnie z zakresem czynności i odpowiedzialności Sekretarza Powiatu w zakresie jego obowiązków należało m.in.: zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, nadzór nad bezpieczeństwem informacji i zapewnieniem ich ciągłości działania, kontrolowanie dostępu do danych osobowych. Sekretarz potwierdził przyjęcie do stosowania nałożonych obowiązków w dniu 19 marca 2019 r.

Sekretarz Powiatu posiadał odpowiednie kompetencje w tym zakresie.

(akta kontroli str. 532-536, 659)

Ponadto za zapewnienie bezpieczeństwa informacji przetwarzanych w systemach informatycznych Starostwa w zakresie stosowania technicznych środków ochrony był odpowiedzialny Administrator Systemu Informatycznego, tj. kierownik działu informatyki. Zgodnie z zakresem czynności i odpowiedzialności kierownika działu informatyki należało m.in.: zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, kontrolowanie dostępu do danych osobowych, a także koordynowanie działań Starostwa w zakresie stosowanych rozwiązań informatycznych oraz administrowanie infrastrukturą informatyczną i systemami baz danych Starostwa. Kierownik potwierdził przyjęcie do stosowania nałożonych obowiązków w dniu 20 sierpnia 2015 r.

Kierownik działu informatyki (ASI) posiadał odpowiednie kompetencje w tym zakresie.

1.10. W Starostwie został wyznaczony inspektor ochrony danych[12].

IOD wykonywał swoje obowiązki na podstawie zawieranych ze Starostwem umów zleceń i posiadał odpowiednie doświadczenie do sprawowania tej funkcji. Od 11 sierpnia 2008 r. pełnił funkcję Administratora Bezpieczeństwa Informacji, a od 25 maja 2018 r.

(akta kontroli str. 332-361)

Do zakresu obowiązków IOD zgodnie z zapisami PBI należało: informowanie Administratora, podmiotów przetwarzających oraz pracowników, stażystów, praktykantów i innych osób upoważnionych do przetwarzania danych osobowych, o obowiązkach spoczywających na nich na podstawie RODO oraz innych przepisów Unii lub krajowych o ochronie danych i doradzanie im w tej sprawie; monitorowanie przestrzegania RODO, innych przepisów Unii lub krajowych o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym w zakresie podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty; udzielanie na żądanie Administratora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania; współpraca z Prezesem Urzędu Ochrony Danych Osobowych; pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach; pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO; prowadzenie rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania; przygotowywanie upoważnień do przetwarzania danych osobowych i prowadzenie rejestru tych upoważnień; prowadzenie rejestru procedur i zabezpieczeń SZBI; prowadzenie rejestru umów powierzenia danych związanych z zadaniami realizowanymi przez Starostwo; prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych, współpraca z ASI w doskonaleniu Polityki i SZBI, w tym inicjowanie i aktualizacja rozwiązań w zakresie bezpieczeństwa informacji; wspieranie Administratora w dokonywaniu oceny skutków dla ochrony danych; przedstawianie propozycji reakcji na stwierdzone incydenty bezpieczeństwa w zakresie ochrony danych osobowych w kontekście RODO; udział w procesu analizy ryzyka na potrzeby określenia odpowiednich środków technicznych i organizacyjnych pozwalających zapewnić akceptowalny poziom bezpieczeństwa przetwarzania danych w tym danych osobowych; przedstawianie propozycji reakcji na zidentyfikowane ryzyka.

(akta kontroli str. 59)

1.11. Zatrudniony w Starostwie IOD, w okresie objętym kontrolą, wykonywał swoje obowiązki na podstawie cywilnoprawnych umów zleceń zawartych w dniach 2 stycznia 2023 r., 27 marca 2023 r. oraz 2 stycznia 2024 r.

(akta kontroli str. 342-346, 348-352, 355-360)

1.12. Starostwo uchwałą nr 1444/2022 z dnia 28 września 2022 r. wyznaczyło pracownika Biura Informatyki jako odpowiedzialnego za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki

[12] Dalej: IOD.

organizacyjne Powiatu Wodzisławskiego. Powyższe było zgodne z art. 21 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[13].

W dniu 6 października 2022 r. wypełniono formularz zgłoszeniowy osób do CSIRT NASK. Zgłoszenie zawierało m.in. dane osoby kontaktowej oraz jej usytuowanie i zestawienie jednostek organizacyjnie podległych (domy pomocy społecznej, domy dziecka, placówki opiekuńczo-wychowawcze, zarząd dróg, szkoły itp.). Zgłoszenie zostało zarejestrowane pod nr 1845556. W dniu 13 października 2022 r. wydrukowany formularz zgłoszeniowy podpisany przez Wicestarostę został wysłany do NASK za pośrednictwem skrzynki ePUAP. Powyższe było zgodne z art. 22 ust. 1 pkt 5 ustawy o ksc.

(akta kontroli str. 362-374)

1.13. PBI nie zawierała wymienionego katalogu dokumentów, które powinny być sporządzone w ramach zapewnienia bezpieczeństwa informacji; dokumentacja taka w postaci odrębnych procedur została kompletnie sporządzona i wdrożona jako element SZBI.

(akta kontroli str. 44-71, 112)

1.14. Oględziny w zakresie inwentaryzacji sprzętu informatycznego przeprowadzone na podstawie badania dziesięciu komputerów, jednego serwera, dwóch laptopów, routera i jednej drukarki[14] wykazały, że Starostwo posiada aktualne informacje o posiadanych zasobach informatycznych obejmujące m.in. ich rodzaj, konfigurację, lokalizację oraz osoby odpowiedzialne. Jednostka prowadzi w formie elektronicznej rejestr zasobów informatycznych w programie komputerowym. Działanie takie wypełniało wymogi o których mowa w § 19 ust. 2 pkt 2 rozporządzenia KRI.

(akta kontroli str. 434-450)

Jak wyjaśnił Starosta, (…) *w okresie od 1 stycznia 2023 r. do 28 czerwca 2023 r., zgodnie z procedurą SZBI: Utrzymanie i ewidencja systemów informatycznych, część: Przyjęcie nowego sprzętu IT i wprowadzenie zmian w zakresie sprzętu i oprogramowania na stanowisku pracy pkt 4, 5 elektroniczny rejestr zasobów teleinformatycznych prowadzono w ramach rejestru metryk komputerów w systemie obiegu dokumentów. (…). W okresie od 29 czerwca 2023 r. do 31 grudnia 2023 r. prowadzono czynności związane z wdrożeniem zakupionego oprogramowania do zarządzania infrastrukturą teleinformatyczną (…) i przeniesienia do tego oprogramowania metryk komputerów. W tym czasie równolegle prowadzono elektroniczny rejestr zasobów teleinformatycznych prowadzony w ramach rejestru metryk komputerów w systemie obiegu dokumentów. W okresie od 1 stycznia 2024 r. elektroniczny rejestr zasobów informatycznych jest prowadzony w ramach systemu (…).*

(akta kontroli str. 16)

1.15. Starostwo w dniu 12 października 2023 r. złożyło wniosek o przystąpienie do Programu Cyberbezpieczny Samorząd. W dniu 21 marca 2024 r. Starostwo podpisało z Centrum Projektów Polska Cyfrowa umowę na powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0070/FERC.02.02-CS.01-001/23/2024. Wartość dofinansowania w ramach umowy wynosiła 829 894,33 zł, z czego 697 111,23 zł stanowił wkład UE a 132 783,09 zł stanowił wkład Budżet Państwa. Wkład własny Starostwa przewidziany umową wynosił 102 464,67 zł. W ramach tej umowy Starostwo zaplanowało nabycie sprzętu m.in.:: serwerów, UPS dla serwera,

[13] Dz.U.2023, poz. 913 ze zm. Dalej: ustawa o ksc.
[14] Dobranych w sposób celowy.

UPSów stanowiskowych, centralnego UPSa, agregatu prądotwórczego, nośników RDX na kopie zapasowe oraz przełączników zarządzalnych, oprogramowania: serwisów dla UTM, licencji Windows Server 2022, dodatkowej licencji Virtualnego Hosta, oprogramowania do zarządzania płatnościami, oprogramowania klasy PAM oraz zakupu lekcji z cyberbezpieczeństwa i RODO na platformę szkoleniową Moodle (dla pracowników) oraz usług: wsparcia dla usługi chmurowej dla przechowywania kopii zapasowych. Okres realizacji umowy ustalono na 24 miesiące liczone od dnia 20 marca 2024 r. Pomiar poprawy cyberbezpieczeństwa Starostwa w związku z realizacją ww. umowy ma być dokonywany przy zastosowaniu mierników wskazanych w załączniku nr 9 do Regulaminu Konkursu Grantowego.

(akta kontroli str. 381-423)

W ramach realizacji ww. grantu założyło następujące wartości poszczególnych wskaźników do osiągniecia:

- liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (w podziale na kobiety/mężczyźni) – czterech mężczyzn[15],
- liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym (w podziale na kobiety/mężczyźni) – 193 kobiety, 29 mężczyzn[16],
- liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – dwie sztuki[17],
- liczba użytkowników nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – 222 osoby[18],
- liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – jeden[19],
- liczba JST wspartych w zakresie cyberbezpieczeństwa – jeden[20],
- liczba podmiotów wspartych w zakresie cyberbezpieczeństwa – jeden[21],

[15] Zgodnie z zapisami załącznika nr 9 do Regulaminu Konkursu Grantowego: Grantobiorca powinien objąć co najmniej jedną osobę z grupy pracowników IT. W ramach wniosku o dofinansowanie wskazano, że ramach projektu planuje się zakup i organizację specjalistycznych szkoleń dla informatyków SP w zakresie oprogramowania związanego z systemami do zapewniania cyberbezpieczeństwa. W Starostwie Powiatowym w Wodzisławiu Śląskim zatrudnionych jest czterech informatyków.

[16] Zgodnie z zapisami załącznika nr 9 do Regulaminu Konkursu Grantowego: Grantobiorca powinien objąć tym wskaźnikiem co najmniej 1 osobę spoza grupy pracowników IT. W ramach wniosku o dofinansowanie wskazano, zakup i organizację szkoleń (online oraz stacjonarnych) w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa u wszystkich pracowników Urzędu. Na moment opracowania wniosku o dofinansowanie w Starostwie Powiatowym w Wodzisławiu Śląskim zatrudnionych było 226 pracowników.

[17] Zgodnie z zapisami załącznika nr 9 do Regulaminu Konkursu Grantowego: Grantobiorca zobowiązany jest do objęcia tym wskaźnikiem co najmniej jednego systemu. W ramach wniosku o dofinansowanie wskazano: zakup oprogramowania do zarządzania podatnościami subskrypcja na dwa lata oraz zakup oprogramowania klasy Privileged Access Management

[18] Pracownicy Starostwa korzystać będą z platformy szkoleniowej w zakresie cyberbezpieczeństwa dla pracowników.

[19] Wskaźnik obejmuje liczbę podmiotów wspartych w JST (projektem objęte jest Starostwo).

[20] Wskaźnik obejmuje liczbę wspartych JST w projekcie, którym udzielono wsparcia w celu zwiększenia poziomu cyberbezpieczeństwa.

[21] Wskaźnik obejmuje liczbę podmiotów, które wdrożyły rozwiązania w obszarze cyberbezpieczeństwa, w celu zapobiegania i reagowania na incydenty w systemach informacyjnych. W ramach projektu w Starostwie zostaną wdrożone rozwiązania w obszarze cyberbezpieczeństwa, w celu zapobiegania i reagowania na incydenty w systemach informacyjnych.

– liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych – jeden[22].

Stwierdzone nieprawidłowości

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

1. W Starostwie od dnia wprowadzenia do stosowania *Procedury zarządzania ciągłością działania*, tj. od 24 stycznia 2023 r. do 4 czerwca 2024 r., nie przeprowadzono testów żadnego ze scenariuszy planów ciągłości działania, o których mowa w punkcie 6 tej procedury, co było działaniem nierzetelnym.

Obowiązek przetestowania scenariusza postępowania w przypadku awarii serwera oraz scenariusza postępowania w przypadku awarii elementu aktywnego sieci wynikał z punktu 6 procedury *Zarządzanie ciągłością działania*, zgodnie z którym poszczególne scenariusze planów ciągłości testowane są w celu weryfikacji pod kątem działania przewidzianego scenariusza oraz aktualności wymaganych osób i zasobów koniecznych do ich realizacji. Procedura zarządzania ciągłością działania nie wskazywała terminów na przeprowadzenie ww. testów, jednak - w ocenie NIK - zaniechanie tych czynności przez ponad 16 miesięcy nie zapewniało realizacji celu[23], dla których przedmiotową Procedurę ustanowiono.

W ww. okresie nie była również weryfikowana aktualność numerów telefonów kontaktowych producentów/serwisów sprzętu informatycznego.

(akta kontroli str. 159-161)

W dniach 5 i 6 czerwca 2024 r., tj. dopiero w trakcie prowadzonej kontroli NIK przeprowadzono ww. testy. Jak wyjaśnił Sekretarz Powiatu, wcześniej takie testy nie były prowadzone z uwagi na niedopatrzenie, wskazał również, że *planowana jest coroczna kontynuacja przeprowadzania testów scenariuszy ciągłości działania.* Powyższe wyjaśnienia potwierdził również Starosta.

(akta kontroli str. 660-661, 777)

2. Procedura *Zarządzanie ciągłością działania* została udostępniona wszystkim pracownikom Urzędu[24], pomimo, że dostęp do niej winien być ograniczony z uwagi na informacje w niej zawarte obejmujące lokalizację i rodzaj serwerów oraz urządzeń/elementów sieci aktywnej Urzędu. Powyższe stworzyło ryzyko, że informacje zawarte w tym dokumencie mogą zostać wykorzystane do przełamania ustanowionych zabezpieczeń. Było to niezgodne z § 19 ust. 2 pkt 7 oraz § 19 ust. 2 pkt 11 rozporządzenia KRI, które obligują kierownictwo podmiotów publicznych do zapewnienia właściwej ochrony przetwarzanych informacji oraz ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji. Ponadto stanowiło to naruszenie zasad określonych w załączniku A normy ISO 27001 punkt A.5.1.1, według której szczegóły techniczne zawarte w PBI winne zostać udostępnione wyłącznie odpowiedzialnym pracownikom (nie podlegają one publikacji).

(akta kontroli str. 500-502)

[22] Wskaźnik obejmuje liczbę instytucji, którym udzielono wsparcia w celu rozwoju lub istotnej modernizacji usług, produktów i procesów cyfrowych w kontekście działań e-administracji.

[23] Celem Procedury była minimalizacja zakłóceń w realizacji działalności statutowej w związku z dysfunkcją systemu informatycznego Urzędu.

[24] W dniu 29 maja 2024 r. procedura została zamieszczona w wewnętrznej sieci intranet.

Jak wyjaśnił Starosta, procedura *Zarządzanie ciągłością działania* dotyczy działań podejmowanych przez pracowników Biura Informatyki. (…) procedury te zostały opublikowane w intrenecie dla zachowania kompletności publikacji procedur.

(akta kontroli str. 462)

Jak wyjaśnił Sekretarz Powiatu (…) *procedura Zarządzanie ciągłością działania, została opublikowana w intranecie w trakcie prowadzonej kontroli. W momencie złożenia pisma NIK o wyjaśnienia dotyczące zaznajomienia pracowników Starostwa z procedurami SZBI, przez nieuwagę, poleciłem opublikowanie wszystkich procedur w intranecie dostępnym dla pracowników Starostwa. Procedura Zarządzanie ciągłością działania jest procedurą dotyczącą działań jakie faktycznie powinni podejmować pracownicy Biura Informatyki; procedura ta została w dniu dzisiejszym usunięta z intranetu a wszelkie jej aktualizacje będą dostępne jedynie dla pracowników Biura Informatyki (…).*

(akta kontroli str. 797-807)

OCENA CZĄSTKOWA

W Starostwie podjęto prawidłowe działania w zakresie opracowania i wdrożenia procedur mających na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych; procedury podlegały przeglądom i aktualizacji. W Jednostce prowadzone były również analizy ryzyka w zakresie zapewnienia ciągłości działania. W Starostwie przez 16 miesięcy od przyjęcia w styczniu 2023 r. do stosowania procedury *Zarządzanie ciągłością działania* nie przeprowadzono testów scenariuszy planów ciągłości działania, takie testy odbyły się dopiero w toku kontroli NIK; niezgodnie z obowiązującymi regulacjami dokonano również udostępnienia wszystkim pracownikom Starostwa szczegółowych zasad zarządzania środowiskiem informatycznym.

OBSZAR

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

2.1. Na podstawie oględzin dziesięciu komputerów[25] ustalono, że nie jest możliwe zainstalowanie na nich oprogramowania testowego na kontach ich użytkowników[26].

(akta kontroli str. 701-706)

Zgodnie z wyjaśnieniami Starosty, w Starostwie wykorzystywane były przez radnych powiatowych tablety w systemie eSesja. Na tabletach były przetwarzane jedynie dane z systemu eSesja, które są danymi publicznymi. Tablety wraz z oprogramowaniem systemowym Android oraz zainstalowaną aplikacja eSesja były przekazywane użytkownikom na podstawie umowy.

Stosownie do zapisów § 7 pkt 1 umowy użytkownik w przypadku zamiaru instalacji dodatkowego oprogramowania lub zmiany domyślnej konfiguracji jest zobowiązany do konsultacji z pracownikiem Biura Informatyki. Starosta wskazał, że do dnia udzielenia wyjaśnień nie było przypadku zwrócenia się przez użytkownika tabletu z takim wnioskiem.

(akta kontroli str. 737-738)

Zasady korzystania ze służbowych telefonów komórkowych zostały uregulowane w Zarządzeniu nr 119/2022 Starosty Wodzisławskiego z dnia 29 listopada 2022 r. w sprawie zasad korzystania ze służbowych telefonów komórkowych.

[25] Trzech laptopów oraz siedmiu komputerów stacjonarnych użytkowanych przez pracowników Starostwa.
[26] System wyświetla monit o podniesienie uprawnień do poziomu administratora.

Zgodnie z § 6 pkt 6 ww. Zarządzenia zabronione zostało przechowywanie na służbowych telefonach komórkowych danych istotnych dla Starostwa, w tym w szczególności danych osobowych, również tych, co do których pracownik posiada uprawnienie do ich przetwarzania, jak również informacji objętych tajemnicą służbową. W przypadku odebrania przez pracownika na telefonie wiadomości zawierających te dane pracownik został zobligowany do ich niezwłocznego usunięcia z pamięci telefonu, po zapoznaniu się z ich treścią.

W Zarządzeniu zobligowano również pracowników m.in. do korzystania z oprogramowania antywirusowego, wymuszania blokady ekranu na telefonie, regularnego korzystania z wbudowanych w telefonie funkcji związanych z optymalizacją, oczyszczaniem pamięci i skanowaniem bezpieczeństwa, a także nieinstalowaniem obcego oprogramowania.

(akta kontroli str.750-762)

Ponadto, Starosta wskazał, że z zabezpieczeń technicznych przy udziale pracownika Biura Informatyki na smartfonach służbowych została aktywowana wykupiona, u operatora sieci komórkowej, dodatkowa usługa *Ochrona Internetu;* zainstalowano aplikację pełniąca funkcję oprogramowania antywirusowego.

(akta kontroli str. 738)

2.2. W ramach SZBI w Starostwie w okresie objętym kontrolą obowiązywała procedura *Nadawanie i rejestrowanie uprawnień do systemów informatycznych*. Procedura obejmowała m.in. opis obowiązków zarówno komórki IT, jak i kierownictwa jednostki, które powinno decydować o uprawnieniach pracowników, a w przypadku zmian zadań realizowanych przez pracownika powinno bezzwłocznie występować o zmianę uprawnień w systemie IT.

(akta kontroli str. 120-125)

Na próbie obejmującej 15 pracowników urzędu[27], wykonujących zadania w systemach informatycznych ustalono, że pracownicy posiadali stosowne uprawnienia, które były zgodne z realizowanymi czynnościami zapisanymi w ich zakresach obowiązków co było zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI. Nie stwierdzono przypadków polegających na nieuzasadnionym rozszerzeniu uprawnień pracownika. Prowadzone dla każdego z pracowników tzw. karty KUSI zawierały informację o administratorach systemu nadawania uprawnień; wszyscy administratorzy systemów byli pracownikami wydziału informatyki. W przypadku jednej pracownicy, która zmieniła w okresie objętym miejsce pracy (zmiana wydziału), uprawnienia do systemów informatycznych nadane w związku z zatrudnieniem w poprzednim wydziale zostały cofnięte w momencie zmiany stanowiska pracy; w tym samym momencie zostały nadane nowe uprawnienia.

(akta kontroli str. 770-772)

2.3. Zgodnie z pkt. 4 obszaru *Zmiana lub odebranie uprawnień w systemie informatycznym* Procedury *Nadawanie i rejestrowanie uprawnień do systemów informatycznych*, w przypadku zakończenia pracy lub stażu w urzędzie Kierownik Biura Informatyki odbiera użytkownikowi wszystkie uprawnienia w systemach informatycznych, po czym podpisuje kartę obiegową.

(akta kontroli str.120-125)

Analiza kart obiegowych 15 pracowników, którzy odeszli z pracy w okresie objętym kontrolą oraz analiza zapisów w systemie informatycznym tzw. kart KUSI, z których wynikały daty cofnięcia uprawnień w systemach informatycznych potwierdziła

[27] W tym 13 osób na stanowiskach kierowniczych, jednej osoby, która zmieniły stanowisko pracy w urzędzie i jednej, która przeszła do innej komórki organizacyjnej urzędu.

zastosowanie ww. Procedury w przypadku wszystkich analizowanych osób. Cofnięcie uprawnień do systemów następowało w momencie sporządzenia kart obiegowych pracowników. Było to zgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI.

(akta kontroli str.773-774)

2.4.Zgodnie z procedurą *Uwierzytelnianie w systemach informatycznych*[28], do uwierzytelnienia użytkownika w systemach stosuje się hasła lub specjalne karty.

W przypadku systemów operacyjnych i oprogramowania, systemów zarzadzania infrastrukturą sieciową oraz systemów obsługi urządzeń peryferyjnych użytkownicy zostali zobowiązani do stosowania złożonych haseł.

(akta kontroli str.126-129)

W wyniku przeprowadzonych oględzin systemów informatycznych Starostwa ustalono, że użytkowane przez Starostwo systemy były zabezpieczone zgodnie z obowiązującymi procedurami.

Oględziny trzech systemów informatycznych Starostwa nie posiadających integracji z usługą AD w celu uwierzytelnienia, wykazały, że wymagania dotyczące haseł były zgodne z przyjętą w Systemie Zarządzania Bezpieczeństwem Informacji *procedurą 2.8.4 Uwierzytelnianie w systemach informatycznych,* w zakresie w jakim umożliwił to producent oprogramowania. Powyższe działania były zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 722-726)

2.5. Oględziny siedmiu stanowisk pracy znajdujących się w referatach Praw Jazdy oraz Rejestracji Pojazdów wykazały, że monitory usytuowane były w odległości co najmniej 2,5 metra od miejsca w którym mógł znajdować się petent. Stanowiska komputerowe były odgrodzone od klientów trwałą przegrodą w postaci ciągu biurek oraz na stałe zamocowaną szybą. Monitory komputerów były ustawione w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe działania spełniały wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str.727-730)

2.6. W Starostwie zgodnie z § 19 ust. 2 pkt 8 rozporządzenia KRI ustanowiono procedurę dotyczącą *Wykorzystania systemów informatycznych przy pracy zdalnej*[29]. Procedura opisywała działania mające na celu zapewnienie bezpiecznej pracy zdalnej, w tym zasady korzystania ze sprzętu informatycznego minimalizujące ryzyko kradzieży informacji, w tym m.in. modele wykorzystania sprzętu służbowego w pracy zdalnej, modele wykorzystania sprzętu prywatnego w pracy zdalnej, bezpieczeństwo przetwarzania przy pracy zdalnej oraz obowiązki pracownika w zakresie ochrony danych związane z wykonywaniem pracy w formie zdalnej.

W ramach przyjętych zasad każdy pracownik podejmujący się pracy zdalnej był zobowiązany do podpisania oświadczenia o znajomości i konieczności przestrzegania procedury. Procedura została również udostępniona w intranecie.

(akta kontroli str. 149-155)

W okresie objętym kontrolą pracę zdalną wykonywały tylko dwie osoby. Badanie dokumentacji związanej z wykonywaniem pracy zdalnej[30] przez te osoby wykazało,

[28] Obowiązująca w Starostwie od 1 grudnia 2021 r.

[29] Procedura Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Wodzisławiu Śląskim, wersja 2, obowiązująca od 30 marca 2020 r.

[30] Wniosek pracownika o wykonywanie pracy zdalnej okazjonalnej, oświadczenie w związku z podjęciem pracy zdalnej oraz porozumienie w sprawie okazjonalnej pracy zdalnej.

że złożyły one stosowne oświadczenia o przeszkoleniu z procedury ochrony danych osobowych i zasad poufności w trakcie pracy zdalnej.

(akta kontroli str. 779-796)

2.7. Dostęp do znajdujących się na wyposażeniu Starostwa laptopów możliwy był tylko po zalogowaniu się na indywidualne konto domenowe użytkownika; stosowano również szyfrowanie dysku laptopa. Laptopy były chronione specjalistycznym oprogramowaniem.

(akta kontroli str. 664-669)

2.8. Oględzinom poddano trzy serwerownie zlokalizowane w trzech różnych obiektach Starostwa. Serwerownie znajdowały się w wyodrębnionych i odpowiednio zabezpieczonych klimatyzowanych pomieszczeniach. Powyższe było zgodne z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

W każdym pomieszczeniu serwerowni znajdowały się zasilacze UPS podtrzymujące ciągłość zasilania serwerów. We wszystkich serwerowniach znajdowały się ewidencje wejść/wyjść do tych pomieszczeń gdzie odnotowywano daty, godziny i cel wizyt. W jednej serwerowni ewidencja wejść/wyjść była prowadzona niezgodnie z procedurą Zabezpieczenia fizyczne, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

W dwóch poddanych oględzinom serwerowniach były przechowywane łatwopalne materiały – kartony, w których znajdowały się urządzenia elektroniczne, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 678-700)

2.9. Badaniu poddano cztery umowy zawarte z podmiotami zewnętrznymi dotyczące zakupów: wdrożenia centralnego systemu wykonywania, przechowywania i odtwarzania kopii zapasowych, systemu zarządzania backupem danych, oprogramowania zintegrowanego systemu zarządzania bezpieczeństwem i infrastrukturą oraz usług w zakresie świadczenia asysty technicznej oprogramowania. Wszystkie z ww. umów zawierały zapisy o zobowiązaniu wykonawcy do zachowania tajemnicy lub zachowaniu poufności informacji do jakich mógł mieć dostęp w związku z realizowaniem umowy, co było zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli str.763-769)

2.10. Jak wyjaśnił Starosta, *(…) nie opracowano procedury dotyczącej przekazywania sprzętu poza jednostkę. W praktyce występuje jedna sytuacja, w której sprzęt jest przekazywany poza jednostkę. Dotyczy to wycofanych z użycia w starostwie komputerów, które są przekazywane do szkoły*. Wskazał, że przed przekazaniem komputery są pozbawiane danych na dyskach poprzez: nadpisywanie danych na całym dysku, tworzenie jednej nowej partycji obejmującej cały dysk lub formatowanie dysku. Ponadto wskazał, że *(…) komputery są przekazywane z wyczyszczonym w ww. sposób dyskami bez instalacji jakiegokolwiek oprogramowania, bez myszy i klawiatur. Wycofane z użycia komputery są przestarzałe i nie nadają się do używania produkcyjnego w szkole. Zgodnie z deklaracją szkoły mają służyć w pracowni komputerowej do ćwiczeń związanych z budową komputera i jego komponentów.*

(akta kontroli str. 665)

Kierownik Biura Informatyki oraz Administrator Systemów Informatycznych Starostwa wyjaśnił, że *(…) jeżeli chodzi o naprawy gwarancyjne sprzętu komputerowego to w razie awarii serwera ma być ona realizowana na miejscu zgodnie z warunkami umowy zawartej z dostawcą, a w przypadku uszkodzenia dysku twardego*

i stwierdzenia potrzeby jego wymiany na nowy, uszkodzony dysk nie podlega zwrotowi. W okresie objętym kontrolą nie mieliśmy awarii serwera. Natomiast jeżeli chodzi o naprawy gwarancyjne laptopów lub komputerów stacjonarnych to w takich przypadkach przekazywane są one do serwisu bez twardych dysków. Jeżeli awarii uległ twardy dysk takiego sprzętu, taki dysk jest niszczony i wymieniany na nowy.

(akta kontroli str.731-732)

2.11. W ramach zapewnienia ciągłości działania w Starostwie ustalono zasady przechowywania kopii zapasowych w ramach procedury *Kopie zapasowe* stanowiącej załącznik 2.8.6 do Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Wodzisławiu Śląskim.

(akta kontroli str.156-158)

Zgodnie z obowiązującą w Starostwie procedurą *Zabezpieczenia sprzętowe, informatyczne i telekomunikacyjne,* urządzenia, dyski lub inne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji miały być pozbawiane wcześniej zapisu tych danych a w przypadku braku takiej możliwości były one uszkadzane w sposób uniemożliwiający ich odczytanie; w przypadku ich przekazywania podmiotowi nieuprawnionemu do przetwarzania danych były one wcześniej pozbawiane zapisu w sposób uniemożliwiający ich odzyskanie.

(akta kontroli str. 116-119, 670-672)

2.12. Zasady tworzenia, przechowywania i testowania kopii zapasowych w Starostwie uregulowano procedurą *Kopie zapasowe.*

Kopie zapasowe były wykonywane zgodnie ze schematem i harmonogramem opisanym w ww. procedurze. Wykonane kopie zapasowe były na bieżąco testowane w sposób automatyczny, protokół był zapisywany do Rejestru odtwarzania kopii zapasowych.

W toku oględzin Kierownik Biura Informatyki przeprowadził próbne odzyskanie pliku z najstarszej kopii zapasowej dostępnej na serwerze NAS. Odzyskany plik otworzył się prawidłowo.

Nagrane nośniki zewnętrzne były przechowywane w sposób zapewniający ich ochronę.

(akta kontroli str. 156-158, 673-675, 707-717)

2.13. Przeprowadzone oględziny procesu monitorowania pojemności nośników pamięci systemów Starostwa wykazały, że w jednostce kontrolowanej użytkowanych było kilka serwerów fizycznych.

Zajętość dysków serwerów była monitorowana w systemie powiadamiającym o przekroczeniu zdefiniowanych parametrów, w tym zajętości dostępnej przestrzeni dyskowej.

Oględzinom poddano trzy serwery fizyczne, dla których Kierownik Biura Informatyki wygenerował raporty zajętości dysków. Na poszczególnych serwerach znajdowało się wolne miejsce, i tak:

- serwer 1, zajęte miejsce: dysk C: 21%, dysk D: 72%,
- serwer 2, zajęte miejsce: dysk C: 51%,
- serwer 3, zajęte miejsce: dysk C: 21%, dysk D: 15%.

W Starostwie nie opracowano procedury dotyczącej monitorowania pojemności nośników pamięci.

(akta kontroli str.718-721)

2.14. W serwerowniach Starostwa zastosowano rozwiązania umożliwiające zabezpieczenie informacji przed nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem. Zapewniono ochronę fizyczną pomieszczeń serwerowni.

(akta kontroli str. 162-171, 666, 678-700)

Stwierdzone nieprawidłowości

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

1. W jednej z serwerowni Starostwa w ewidencji wejść/wyjść nie odnotowywano przebywania osób niebędących pracownikami Biura Informatyki i, co było niezgodne z pkt 4, część 3 Dostęp do serwerowni procedury *Zabezpieczenia fizyczne*.

   Zgodnie z procedurą *Zabezpieczenia fizyczne* - Dział *Dostęp do serwerowni*, pkt 4, przebywanie w serwerowniach osób niebędących pracownikami starostwa w Biurze Informatyki jest odnotowywane przez pracownika nadzorującego pracę tych osób w zeszycie wejść do serwerowni.

   (akta kontroli str. 115)

   Osobą uprawnioną do nadzorowania przebywania osób niezatrudnionych w Starostwie w pomieszczeniu serwerowni był Główny Administrator Danych Osobowych Starostwa.

   (akta kontroli str.733-734)

   W wyniku przeprowadzonych, w dniu 25 czerwca 2024 r., oględzin jednej z serwerowni Starostwa ustalono, że ostatni wpis w zeszycie wejść do strefy przetwarzania danych osobowych (serwerowni) został odnotowany w dniu 13 sierpnia 2019 r.

   (akta kontroli str. 691-700)

   Główny Administrator Danych Osobowych wyjaśnił, że w okresie od ostatniego wpisu w zeszycie wejść do serwerowni Starostwa przebywały w serwerowni osoby trzecie. Wskazał, że (…) *pod moim nadzorem wykonywali tam prace serwisowe pracownicy zewnętrznych firm. Prace dotyczyły serwisu klimatyzacji oraz instalacji przeciwpożarowych. Takie prace odbywają się co roku.* Jako przyczynę braku odnotowywania takich wejść w zeszycie wskazał niedopatrzenie.

   (akta kontroli str.733-734)

   Jak wyjaśnił Starosta (…) *wpisów w książce wejść nie dokonywano przez niedopatrzenie. Pracownicy odpowiedzialni za brak ww. wpisów zostali pouczeni o konieczności dokonywania wpisów w książce wejść.*

   (akta kontroli str.777)

2. W dwóch serwerowniach Starostwa znajdowały się materiały łatwopalne – kartony[31]. Było to niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

   (akta kontroli str.685-700)

   Jak wyjaśnił Starosta (…) *w serwerowniach (…) znajdowały się chwilowo materiały łatwopalne przez nieuwagę. Niezwłocznie po oględzinach zostały one uprzątnięte co potwierdza załączona dokumentacja zdjęciowa. Pracownicy odpowiedzialni*

[31] Co ustalono w trakcie przeprowadzonych w dniu 25 czerwca 2024 r. oględzin tych pomieszczeń.

za niedopatrzenie zostali poinstruowani przez Sekretarza Powiatu o konieczności zachowania czystości (szczególnie w odniesieniu do materiałów łatwopalnych) w serwerowni.

(akta kontroli str. 777)

NIK wskazuje, że z uwagi na fakt, że na dyskach serwerów, zgromadzonych w serwerowniach i centrach przetwarzania danych, przechowywane są informacje dotyczące najważniejszych sfer działalności Starostwa, łatwopalne materiały podnoszą ryzyko utraty takich danych w wyniku ewentualnego pożaru.

OCENA CZĄSTKOWA

Starostwo przyjęło i wdrożyło rozwiązania organizacyjne w zakresie ochrony bezpieczeństwa informacji. Dostęp do pomieszczeń i systemów informatycznych był ograniczony jedynie do osób upoważnionych; z tym, że w jednej z serwerowni nie dokonywano wymaganych procedurami wpisów o osobach niebędących pracownikami Starostwa, które przebywały w serwerowni pod nadzorem upoważnionego pracownika. Pomieszczenia serwerowni oraz narzędzia informatyczne, w tym systemy informatyczne były zabezpieczone kontrolą dostępu; w dwóch poddanych oględzinom pomieszczeniach serwerowni znajdowały się materiały łatwopalne (kartony), co zwiększało ryzyko utraty danych w wyniku ewentualnego pożaru.

W Starostwie zapewniono bezpieczeństwo danych osobowych również poprzez sporządzanie i przechowywanie kopii zapasowych, które były poddawane testowaniu; zidentyfikowano również kluczowe i podlegające ochronie elementy infrastruktury informatycznej.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji.

3.1. Zgodnie z § 17 PBI[32], analizę ryzyka utraty integralności, dostępności lub poufności informacji przeprowadza się co najmniej raz w roku w terminie do dnia 20 listopada każdego roku.

(akta kontroli str. 63)

Integralną częścią dokumentacji związanej z szacowaniem ryzyka była, przedstawiona Staroście do zapoznania w dniu 22 sierpnia 2023 r., dokumentacja dotycząca:

- *klasyfikacji czynności przetwarzania*, w której zidentyfikowano aktywa (informacje i czynności przetwarzania) oraz określono czy występują dla nich kryteria wystąpienia oceny skutków (DPIA) oraz czy wymagana jest ocena skutków,
- *grupowania podobnych czynności przetwarzania* gdzie usystematyzowano podobne czynności przetwarzania w ramach trzech grup,
- *ocena ryzyka dla przetwarzania danych osobowych* gdzie wskazano zagrożenia dla poszczególnych grup, obliczono według wzoru poziom ryzyka przed wprowadzeniem działań naprawczych oraz wskazano zamierzony do osiągnięcia cel (redukcja).

(akta kontroli str. 174-235)

[32] W wersji obowiązującej od 23 stycznia 2023 r. W PBI obowiązującym od 25 maja 2018 r. zapis dotyczący analizy ryzyka znajdował się w § 14.

W wyniku przeprowadzonego przez IOD szacowania ryzyka sporządzony został *Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń*. Plan ten zawierał zestawienie zidentyfikowanych aktywów wraz z przyporządkowanymi im kategoriami i rodzajami zagrożeń oraz odpowiadającymi zaleceniami; zawierał również wskazanie poziomu ryzyka po wprowadzeniu działań naprawczych. Wyznaczono roczny termin realizacji Planu.

(akta kontroli str. 236-248)

3.2. Obowiązki pracowników Starostwa w zakresie zgłaszania incydentów cyberbezpieczeństwa lub naruszenia bezpieczeństwa informacji (w tym osobowych) zostały uregulowane w § od 23 do 27 PBI; w § 15 tego dokumentu zdefiniowano role i odpowiedzialność poszczególnych osób w Starostwie za zgłaszanie incydentów naruszenia bezpieczeństwa informacji.

(akta kontroli str. 58-62, 68-71)

Zgodnie z wpisami do prowadzonego w Starostwie w formie elektronicznej *Rejestru incydentów*[33], w okresie objętym kontrolą wystąpiły dwa incydenty naruszenia bezpieczeństwa informacji. Rejestr zawierał 19 kolumn, w których wpisywane były m.in.: tytuł incydentu, data i godzina zgłoszenia, dane zgłaszającego, miejsce, status, okoliczności naruszenia i jego charakter, możliwe konsekwencje naruszenia oraz zastosowane i proponowane środki bezpieczeństwa, a także informacje o powiązanych zasobach.

Stwierdzone incydenty dotyczyły kradzieży telefonu komórkowego z biurka pracownika Starostwa (incydent z 5 kwietnia 2023 r.) oraz omyłkowej wysyłki załącznika do wnioskującego o udzielenie informacji publicznej (incydent z dnia 24 stycznia 2024 r.). W związku z incydentami, Sekretarz powiatu, w dniach 7 kwietnia 2023 r. oraz 30 stycznia 2024 r. przeprowadził z pracownikami odpowiedzialnymi za wystąpienie incydentu rozmowy dyscyplinujące udokumentowane stosownymi notatkami służbowymi. Pismem z dnia 26 stycznia 2024 r. poinformowano również odbiorcę omyłkowo wysłanych załączników o konieczności trwałego ich usunięcia oraz o braku możliwości przetwarzania danych osobowych zawartych w tych załącznikach w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których te dane dotyczą.

W związku z zaistniałymi zdarzeniami, przy użyciu narzędzia informatycznego Kalkulator wagi naruszeń ochrony danych osobowych IOD dokonał szacowania ryzyka naruszenia praw lub wolności osób fizycznych, gdzie określono takie ryzyko na niskim poziomie; w związki z drugim incydentem w dniu 30 stycznia 2024 r. wysłano do Prezesa Urzędu Ochrony Danych Osobowych zgłoszenie naruszenia ochrony danych osobowych. Powyższe było zgodne z obowiązującymi w Starostwie procedurami oraz przepisami rozporządzenia Parlamentu Europejskiego z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[34].

(akta kontroli str. 543-563)

3.3. Zgodnie z zapisami § 21 PBI[35], każdy pracownik, stażysta, praktykant przed przystąpieniem do realizacji powierzonych mu zadań odbywa szkolenie wprowadzające z zakresu bezpieczeństwa informacji i ochrony danych osobowych, przeprowadzone przez IOD lub inną wskazaną przez niego osobę oraz podpisuje zobowiązanie do zachowania poufności oraz oświadczenie potwierdzające

[33] Dalej: Rejestr.

[34] Dz.U.UE.L.2016.119.1

[35] W poprzedniej wersji PBI był to § 18.

zapoznanie się z obowiązującymi w Starostwie zasadami bezpieczeństwa informacji i ochrony danych osobowych, ich zrozumienie i zobowiązanie do ich przestrzegania. Ponadto w przyjętych regulacjach wskazano, że każdy pracownik, stażysta, praktykant przed rozpoczęciem przetwarzania danych osobowych w oparciu o upoważnienie Administratora zapoznaje się z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO, co poświadcza stosownym oświadczeniem.

(akta kontroli str. 65)

W wyniku badania notatek służbowych z tzw. przekazania informacji dotyczących ochrony danych osobowych 18 pracownikom, stażystom bądź praktykantom Starostwa zatrudnionych albo odbywających staż lub praktykę w okresie objętym kontrolą ustalono, że na potrzeby szkoleń zapoznawano zatrudnionych z przygotowanym przez IOD materiałem informacyjnym dotyczącym zasad ochrony danych osobowych obowiązujących w Starostwie, co potwierdzali podpisami.

Szkolenia obejmowały swoim zakresem: przepisy o ochronie danych osobowych (m.in. RODO, ustawa o ochronie danych osobowych, regulacje wewnętrzne w zakresie ochrony danych; podstawowe pojęcia związane z ochroną danych – dane osobowe, przetwarzanie, zbiór danych; odpowiedzialność karna za nieprzestrzeganie danych osobowych); zapisy Polityki Bezpieczeństwa Informacji obowiązującej w Starostwie (m.in. podstawowe zasady bezpieczeństwa informacji; podstawowe zasady przetwarzania danych osobowych; podstawy przetwarzania danych osobowych; obowiązki pracowników, stażystów i praktykantów w zakresie ochrony danych osobowych; incydenty bezpieczeństwa i naruszenie ochrony danych osobowych; realizacja obowiązku informacyjnego; realizacja praw osób, których dane dotyczą; konsekwencje naruszenia PBI i SZBI) oraz zasady wynikające z Systemu Zarządzania Bezpieczeństwem Informacji (m.in. zabezpieczenia fizyczne; zabezpieczenia sprzętowe, informatyczne i telekomunikacyjne; uwierzytelnianie w systemach informatycznych; kopie zapasowe; zarządzanie sprzętem komputerowym i oprogramowaniem; korzystanie z Internetu i poczty elektronicznej).

(akta kontroli str. 534-653)

Jak wskazał Starosta, *(…) wszyscy pracownicy starostwa uczestniczący w procesie przetwarzania informacji zostali przeszkoleni w tym zakresie. Po rozpoczęciu obowiązywania RODO (25.05.2018 r.) w dniu 20 i 25 czerwca 2018 r. przeprowadzono szkolenie dla wszystkich pracowników starostwa z zakresu RODO, Polityki Bezpieczeństwa Informacji oraz procedur SZBI. (…) Po każdym szkoleniu sporządzana jest notatka (…) Na wewnętrznym intranecie znajdują się materiały szkoleniowe z zakresu bezpieczeństwa informacji w celu możliwości samokształcenia się pracowników. (…)*Starosta wskazał również, że *(…) każdy z pracowników starostwa dopuszczony do przetwarzania danych przynajmniej raz został przeszkolony z zakresu bezpieczeństwa informacji. (…) Wszyscy pracownicy starostwa uczestniczący w procesie przetwarzania informacji są przeszkoleni z zakresu bezpieczeństwa informacji. Wskazał również, że (…) w ramach projektu Cyberbezpieczny Samorząd zaplanowano szkolenia z zakresu bezpieczeństwa informacji, w tym cyberbezpieczeństwa dla wszystkich pracowników starostwa.*

(akta kontroli str. 539)

3.4. W okresie objętym kontrolą w Starostwie przeprowadzono okresowy audyt w zakresie bezpieczeństwa informacji. (na podstawie umowy nr WOA.042.1.22.2022 z dnia 31 marca 2023 r.). Audytor wydał pozytywną ocenę dla Starostwa, sporządzając *Ocenę zgodności z KRI/UoKSC* z dnia 9 maja 2023 r. oraz *Ocenę wybranych aspektów bezpieczeństwa systemów informatycznych* z dnia 9 maja 2023 r. W ramach Oceny zgodności z KRI/UoKSC najniższe oceny odnotowano

w zakresie zarządzania podatnościami systemów, gdzie audytor wskazał, że nie wdrożono procedur w tym zakresie.

(akta kontroli str. 289-313)

Po zakończonym audycie Starostwo, w dniu 10 grudnia 2023 r., złożyło wniosek o dofinansowanie w ramach do Programu *Cybernetyczny Samorząd*, gdzie w punkcie 13 wniosku wskazano przeznaczenie dofinansowania m.in. na zakup oprogramowania do zarządzania podatnościami. Kierownik Biura Informatyki, w dniu 22 kwietnia 2024 r. wystosował do Wydziału Organizacyjno-Administracyjnego Starostwa: opis przedmiotu do zamówienia oraz projekt umowy w związku z zakupem oprogramowania do zarządzania podatnościami. Do zakończenia kontroli NIK zakup nie został zrealizowany.

(akta kontroli str. 383)

W okresie od 27 czerwca 2023 r. do 9 sierpnia 2023 r. audytor wewnętrzny wykonał tzw. czynność doradczą w trybie § 22 rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu[36]. Tematem czynności doradczej była m.in. analiza spełnienia na poziomie Starostwa wymogów w zakresie SZBI. Jako cel czynności zdefiniowano wzmocnienie bieżącego monitorowania SZBI oraz identyfikację potencjalnych obszarów ryzyka w zakresie SZBI. W efekcie ww. działań sporządzono Zbiorczą informację w zakresie spełnienia na poziomie Starostwa Powiatowego w Wodzisławiu Śląskim oraz jednostek organizacyjnych powiatu wodzisławskiego wymogów w zakresie SZBI; w zakresie uchybień dokument ten zawierał informację, że Starostwo nie posiadało planów postępowania w odniesieniu do zidentyfikowanego ryzyka.

(akta kontroli str.257-277)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w badanym zakresie. W okresie objętym kontrolą były prowadzone analizy ryzyka w zakresie bezpieczeństwa informacji. Prawidłowo zarządzano incydentami naruszenia bezpieczeństwa informacji. Pracownicy byli przeszkoleni w zakresie ochrony danych osobowych.

IV. Uwagi

Uwagi

Uwzględniając działania Starostwa podjęte w trakcie kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, zwraca uwagę na:

1. Obowiązek dokonywania cyklicznych testów scenariuszy przewidzianych procedurą *Zarządzanie ciągłością działania.*

2. Konieczność ograniczenia kręgu *osób, którym* udostępniane zostają procedury zawierające dane, których ujawnienie może stworzyć zagrożenie bezpieczeństwa informacji podlegających ochronie, wyłącznie do osób uprawnionych.

3. Konieczność odpowiedniego zabezpieczenia pomieszczeń serwerowni (zarówno pod kątem odnotowywania dostępu osób trzecich, jak i rodzaju materiałów w nich przechowywanych).

[36] Dz.U. z 2018 r., poz. 506.

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 Katowicach. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag

Zgodnie z art. 62 ustawy o NIK, należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag 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.

Katowice, dnia 19 września 2024 r.

Kontroler

Jacek Kordanowski

Gł. specjalista kontroli państwowej

Najwyższa Izba Kontroli

Delegatura w Katowicach

.....