WOJEWODA DOLNOŚLĄSKI

KO-KZ.431.2.4.2024.BJ

Pan
Dariusz Smoliński
Dolnośląski Wojewódzki
Inspektor Jakości Handlowej
Artykułów Rolno-Spożywczych

ul. Ofiar Oświęcimskich 12
50-069 Wrocław

SPRAWOZDANIE

Wrocław, dnia 30 grudnia 2024 r.

I. Informacje organizacyjne

Jednostka kontrolowana	Wojewódzki Inspektorat Jakości Handlowej Artykułów Rolno-Spożywczych we Wrocławiu
Kierownik jednostki kontrolowanej	Dariusz Smoliński - Dolnośląski Wojewódzki Inspektor Jakości Handlowej Artykułów Rolno-Spożywczych
Zakres kontroli	Realizacja przez Dolnośląskiego Wojewódzkiego Inspektora Jakości Handlowej Artykułów Rolno-Spożywczych zaleceń sformułowanych w wystąpieniu pokontrolnym z dnia 5 marca 2020 r. (znak: NK-KE.431.44.2019.DD).
Podstawa prawna kontroli	Art. 6 ust. 4 pkt 1 i art. 51 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1], art. 28 ust. 1 pkt 1 i art. 51 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie[2] oraz na podstawie zatwierdzonego w dniu 25 czerwca 2024 r. przez Wojewodę Dolnośląskiego planu kontroli na II półrocze 2024 r. (znak: NK-KSE.430.4.2024.RG)
Data rozpoczęcia i zakończenia czynności kontrolnych	Od 18 do 29 listopada 2024 r.
Kontrolerzy	Bartosz Jędrysiak – inspektor wojewódzki z Wydziału Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, upoważnienie nr 51 z dnia 7 listopada 2024 r. (KO-KZ.0030.51.2024.BJ). (Dowód: akta kontroli str.: 6-7)

[1] tekst jedn. Dz. U. z 2020 r. poz. 224.
[2] tekst jedn. Dz. U. z 2023 r. poz. 190.

II. Ocena kontrolowanej jednostki

Realizację kontrolowanych zadań oceniono **pozytywnie pomimo stwierdzonych nieprawidłowości.**

III. Ustalenia kontroli

1. Wstęp.

W dniach 21 i 26 listopada 2019 r. zespół kontrolny z Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu przeprowadził w Wojewódzkim Inspektoracie Jakości Handlowej Artykułów Rolno-Spożywczych we Wrocławiu[3] kontrolę problemową, której przedmiotem było bezpieczeństwo teleinformatyczne jednostki – działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań administracji rządowej. Realizację powyższego zadania przez WIJHARS oceniono negatywnie. W wystąpieniu pokontrolnym z dnia 5 marca 2020 r. wskazano, mając na uwadze stwierdzone nieprawidłowości, iż w celu ich wyeliminowania należy:

1. Opracować i wdrożyć kompleksową dokumentację z zakresu SZBI.
2. Dokonać ponownego oszacowania ryzyka w zakresie serwerowni z uwzględnieniem ustaleń i wniosków wynikających z niniejszego wystąpienia pokontrolnego.
3. Opracować i wdrożyć procedurę zgłaszania incydentów naruszenia bezpieczeństwa w zakresie naruszeń zabezpieczeń systemów teleinformatycznych.
4. Przynajmniej raz w roku przeprowadzać audyt wewnętrzny w zakresie bezpieczeństwa informacji.
5. Zabezpieczyć serwerownię przed dostępem osób nieuprawnionych, w tym pracowników Inspektoratu.
6. Wyposażyć serwerownię w czujnik dymu.
7. Dokonać analizy możliwości podziału sieci LAN na kilka sieci VLAN, w celu zwiększenia jej bezpieczeństwa.
8. W ramach wprowadzonej polityki haseł stosować minimalną długość hasła, tj. 8 znaków.
9. Wprowadzić atrybut wymuszania złożoności haseł oraz jego cyklicznej zmiany, co 30 dni.
10. Wprowadzić zabezpieczenie w postaci blokady konta użytkownika po trzykrotnym wprowadzeniu błędnego hasła.
11. Ustawić wygaszacze ekranów na komputerach pracowników zgodne z czasem aktywacji wynikającym z przyjętej Instrukcji oraz bez możliwości edycji przez pracowników.
12. Ustalać uprawnienia użytkowników w wykorzystywanych systemach teleinformatycznych oraz na stacjach roboczych stosownie do wykonywanych zadań.
13. W przypadku rozwiązania stosunku pracy z pracownikiem niezwłocznie dezaktywować konto.
14. W porozumieniu z wykonawcą oprogramowania zapewnić atrybut rozliczalności w systemie Symfonia.

---

[3] Dalej jako: WIJHARS, kontrolowana jednostka.

15. W przypadku kopii zapasowych zapewnić retencję danych z okresu co najmniej 2 tygodni.
16. Zapewnić częstsze wykonywanie kopii zapasowej, która jest przechowywana na zewnętrznym nośniku danych.

(Dowód: akta kontroli str.: 8-20)

Jako termin realizacji powyższych zaleceń (lub termin wskazania przyczyn braku ich realizacji) wskazano dzień 3 kwietnia 2020 r. Pismem z dnia 3 kwietnia 2020 r. kontrolowany organ udzielił odpowiedzi w zakresie powyższych zaleceń, wskazując iż:[4]

1. Zleciłem przygotowanie kompleksowej dokumentacji z zakresu SZBI firmie zewnętrznej, która opracowała dla podległej mi jednostki System Zarządzania Bezpieczeństwem Informacji według normy PN-ISO/IEC 27001:2013, którego integralną częścią jest m.in.: Polityka Bezpieczeństwa Informacji według normy PN-ISO/IEC 27001:2013, Polityka Bezpieczeństwa Systemów Informatycznych oraz Polityka Ochrony Danych Osobowych. W chwili obecnej prowadzone są konsultacje, które pozwolą na ostateczne zatwierdzenie opracowanych procedur.
   W załączeniu przekazuję wydruk struktury dokumentów w ramach opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
2. Ustalono, że w chwili obecnej poziom istotności dla ryzyka w zakresie serwerowni jest na poziomie wysokim. Taka sytuacja wymaga podjęcia nowych działań.
   W związku z przyjęciem przez Rząd ustawy o zmianie ustawy o jakości handlowej artykułów rolno-spożywczych, zgodnie z którym, Inspekcja Handlowa Artykułów Rolno-Spożywczych przejmie część kompetencji Inspekcji Handlowej i będzie kontrolować jakość na wszystkich etapach obrotu. Zwiększenie kompetencji w zakresie kontroli jakości handlowej artykułów rolno-spożywczych podległej mi jednostki i przejęcie części pracowników Inspekcji Handlowej spowoduje konieczność modernizacji naszej siedziby.
   W związku z powyższym rozważam w miarę posiadanych środków finansowych przeniesienie lub całkowite wyodrębnienie pomieszczenia dedykowanego tylko dla serwera.
3. Procedura zgłaszania incydentów naruszenia bezpieczeństwa w zakresie naruszeń zabezpieczeń systemów teleinformatycznych stanowić będzie integralną część opracowywanej przez firmę zewnętrzną dokumentacji z zakresu SZBI.
4. Po zatwierdzeniu i wdrożeniu nowej dokumentacji z zakresu SZBI, przewidujemy zlecenie firmie zewnętrznej przeprowadzenie audytu w zakresie bezpieczeństwa informacji.
5. Ograniczono do minimum dostęp pracowników i osób nieuprawnionych do pomieszczenia, w którym znajduje się serwer.
6. W pomieszczeniu serwerowni planowany jest montaż czujnika dymu.
7. Zostanie wykonana analiza aktualnej struktury sieci LAN i ewentualnego podziału na odrębne segmenty (VLAN-y).
8. W chwili obecnej stosowana jest polityka haseł o minimalnej długości hasła od 8 znaków oraz odpowiednim stopniu skomplikowania.

[4] Numery poszczególnych punktów odpowiadają numerom przypisanym poszczególnym zaleceniom.

9. Kontroler Active Directory i konta użytkowników zostały przekonfigurowane do cyklicznego wymuszania zmiany haseł oraz wymogu ich odpowiedniego skomplikowania.
10. Wprowadzona została blokada po 3 błędnych wpisaniach hasła.
11. Wygaszacze ekranu mają ustawiony czas aktywacji nie większy niż przewidziany w obecnie obowiązującej Instrukcji SZBI. Ograniczenie w edycji zostanie wymuszone poprzez zmiany uprawnień użytkowników.
12. Uprawnienia użytkowników na stacjach roboczych zostały ustawione zgodnie z wykonywanymi zadaniami.
13. Przyjęto zasadę niezwłocznego dezaktywowania konta w przypadku rozwiązania stosunku pracy z pracownikiem.
14. W chwili obecnej prowadzona jest analiza możliwości wprowadzenia rozliczalności w systemach Symfonia, kosztów oraz ewentualnych możliwości zmiany na inne programy finansowo-księgowe dostępne na rynku. Wymaga to większego przygotowania ze względu na czasochłonność oraz koszty całej operacji.
15. Na chwilę obecną wprowadzone zostało wykonywanie dodatkowej kopii raz na 7 oraz 14 dni dla zapewnienia retencji. W dalszej perspektywie rozważony zostanie zakup licencjonowanego oprogramowania do wykonywania kopii, które będzie umożliwiało automatyczne wykonywanie kopii z większą retencją.
16. Ustalono wykonywanie kopii zapasowych co 20 dni.

(Dowód: akta kontroli str.: 21-25)

2. <u>Realizacja zalecenia pokontrolnego nr 1.</u>
„Opracować i wdrożyć kompleksową dokumentację z zakresu SZBI"

W wyniku pierwszej kontroli z 2019 r. stwierdzono, iż wówczas obowiązująca w WIJHARS dokumentacja z zakresu Systemu Zarządzania Bezpieczeństwem Informacji[5] nie była kompleksowa, ponieważ nie uwzględniała wszystkich kategorii informacji przetwarzanych w WIJHARS, a odnosiła się głównie do ochrony danych osobowych. SZBI nie uwzględniał także zasad sporządzania analizy ryzyka, wytycznych w zakresie projektowania, konstruowania oraz wdrażania systemów teleinformatycznych, a także kwestii dotyczących cyklicznych szkoleń dla osób zaangażowanych w proces przetwarzania informacji. Ponadto, nie uregulowano kwestii zakresu przedmiotowego audytu wewnętrznego bezpieczeństwa informacji.

Pismem z dnia 18 listopada 2024 r., za pośrednictwem platformy ePUAP, kontrolowany przekazał obecnie obowiązującą w WIJHARS dokumentację z zakresu SZBI, na którą składają się:

- System Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-ISO/IEC 27001:2013;
- Polityka Bezpieczeństwa Informacji według normy PN-ISO/IEC 27001:2013;
- Polityka Ochrony Danych Osobowych;
- Polityka Bezpieczeństwa Systemów Informatycznych;

[5] Dalej jako: SZBI.

- Zarządzenie nr 10/2018 Dolnośląskiego Wojewódzkiego Inspektora Jakości Handlowej Artykułów Rolno-Spożywczych we Wrocławiu z dnia 22 maja 2018 r. w sprawie powołania Inspektora Ochrony Danych w Wojewódzkim Inspektoracie Jakości Handlowej Artykułów Rolno-Spożywczych we Wrocławiu.

Analiza ww. dokumentacji wykazała, iż obecnie obowiązująca w WIJHARS dokumentacja z zakresu SZBI jest zgodna z § 19 ust. 1 rozporządzenia Rady Ministrów z dnia 24 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 r., poz. 773, dalej: r.k.r.i.). Mając na uwadze powyższe wdrożenie zalecenia nr 1 należy ocenić pozytywnie.

(Dowód: akta kontroli str.: 29-157)

3. <u>Realizacja zalecenia pokontrolnego nr 2, 5 i 6.</u>

„Dokonać ponownego oszacowania ryzyka w zakresie serwerowni z uwzględnieniem ustaleń i wniosków wynikających z niniejszego wystąpienia pokontrolnego" (2)

„Zabezpieczyć serwerownię przed dostępem osób nieuprawnionych, w tym pracowników Inspektoratu" (5)

„Wyposażyć serwerownię w czujnik dymu" (6)

W wyniku pierwszej kontroli stwierdzono, iż serwerownia umiejscowiona jest w pokoju przechodnim, do którego dostęp jest nieograniczony z uwagi na umiejscowienie urządzeń służących pracownikom do realizacji bieżących obowiązków (urządzenie wielofunkcyjne Nashuatec DSm620d oraz niszczarka) stanowi naruszenie przepisu § 19 ust. 2 pkt 7 lit. a r.k.r.i.[6], bowiem nie w pełni zapewnia ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji. Jednocześnie stwierdzono brak czujnika dymu w pomieszczeniu serwerowni. Powyższe kwestie nie znalazły pokrycia w analizie ryzyka z dnia 27 grudnia 2018 r. co zostało wskazane w wystąpieniu pokontrolnym z dnia 5 marca 2020 r.

W celu weryfikacji realizacji wskazanych zaleceń pokontrolnych kontrolowany przekazał, pismem z dnia 19 listopada 2024 r. za pośrednictwem platformy ePUAP, arkusz analizy ryzyka w WIJHARS, natomiast kontroler, w obecności Pana A.D. pełniącego funkcję informatyka (administratora systemów informatycznych, dalej: ASI), dokonał w dniu 21 listopada 2024 r. oględzin serwerowni. W wyniku kontroli ustalono, iż przekazana analiza ryzyka w zakresie obszaru „Infrastruktura" odnoszącego się m.in. do serwerowni została oceniona z uwzględnieniem stanu faktycznego stwierdzonego w protokole oględzin. Serwerownia WIJHARS jest obecnie wyodrębnionym pomieszczeniem, do którego dostęp ma tylko ASI. W pomieszczeniu zamontowano też czujnik dymu. W związku z powyższym ustalone w analizie ryzyka w WIJHARS poziomy prawdopodobieństwa, skutki oraz ryzyka wystąpienia poszczególnych incydentów sformułowano prawidłowo. Należy zwrócić jednak uwagę, iż przekazany arkusz analizy ryzyka nie zawiera informacji o dacie jego sporządzenia oraz osobie, która go sporządziła.

---

[6] W ówcześnie obowiązującym rozporządzeniu był to § 19 ust. 2 pkt 7 lit. a r.k.r.i.

Mając na uwadze powyższe należy pozytywnie ocenić wdrożenie zaleceń nr 2, 5 i 6.

(Dowód: akta kontroli str.: 171-175, 176-179)

4. Realizacja zalecenia pokontrolnego nr 3.

„Opracować i wdrożyć procedurę zgłaszania incydentów naruszenia bezpieczeństwa w zakresie naruszeń zabezpieczeń systemów teleinformatycznych"

W wyniku pierwszej kontroli ustalono, iż w WIJHARS nie ustanowiono procedury zgłaszania incydentów dotyczących naruszeń zabezpieczeń systemów teleinformatycznych.

Z przekazanej przez kontrolowanego dokumentacji z zakresu SZBI wynika, iż opracowano dokument o nazwie „Instrukcja Bezpieczeństwa" stanowiący Załącznik nr 2 do Polityki Bezpieczeństwa Informacji według normy PN-ISO/IEC 27001:2013. Punkt 6 Instrukcji Bezpieczeństwa dotyczy postępowania przy stwierdzeniu zdarzeń naruszających bezpieczeństwo informacji, wskazujący:

- przykładowy katalog naruszeń lub podejrzeń naruszeń bezpieczeństwa systemu wraz z koniecznością zgłoszenia ich do ASI,
- czynności, jakie zgłaszający powinien podjąć do czasu przybycia na miejsce ASI,
- czynności, jakie powinien podjąć ASI niezwłocznie po otrzymaniu zawiadomienia oraz po sporządzeniu raportu.

W wyniku kontroli stwierdzono, iż powyższa procedura nie uwzględnia jednak kwestii dotyczących formy zgłoszenia zdarzenia naruszającego bezpieczeństwo informacji, co stanowi uchybienie.

Mając na uwadze powyższe sposób wdrożenia zalecenia nr 3 należy ocenić pozytywnie pomimo stwierdzonych uchybień.

(Dowód: akta kontroli str.: 77-78)

5. Realizacja zalecenia pokontrolnego nr 4.

„Przynajmniej raz w roku przeprowadzać audyt wewnętrzny w zakresie bezpieczeństwa informacji"

W wyniku kontroli z 2019 r. ustalono, iż przeprowadzanie audytu wewnętrznego z zakresu bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 14 r.k.r.i., nie było realizowane.

Pismem z dnia 19 listopada 2024 r. Kontrolowany przekazał cztery dokumenty poaudytowe z zakresu bezpieczeństwa informacji z lat 2021-2023[7]. Z dokumentów poaudytowych wynika, iż czynności audytowe prowadziła komisja składająca się z trzech pracowników WIJHARS, natomiast w roku 2024 r. czynności audytowe zostały przeprowadzone przez certyfikowanego audytora.

---

[7] Protokół z audytu wewnętrznego w zakresie bezpieczeństwa informacji z dnia 17 grudnia 2021 r., protokół z audytu wewnętrznego w zakresie bezpieczeństwa informacji z dnia 23 grudnia 2022 r., protokół z audytu wewnętrznego w zakresie bezpieczeństwa informacji z dnia 16 grudnia 2023 r., sprawozdanie z audytu wewnętrznego z dnia 15 listopada 2024 r.

Mając na uwadze powyższe, pozytywnie należy ocenić realizację zalecenia pokontrolnego nr 4.

(Dowód: akta kontroli str.: 158-170)

6. <u>Realizacja zalecenia pokontrolnego nr 7.</u>
„Dokonać analizy możliwości podziału sieci LAN na kilka sieci VLAN, w celu zwiększenia jej bezpieczeństwa"

W wyniku kontroli z 2019 r. ustalono, iż użytkownicy, przełączniki i serwery są umieszczone w tej samej podsieci LAN, co może rzutować na bezpieczeństwo w sieci.

W toku czynności kontrolnych zweryfikowano, iż sieć LAN została podzielona na dwa VLAN: MGMNT LAN oraz WIJHARS-LAN w celu zwiększenia poziomu bezpieczeństwa w sieci.

Mając na uwadze powyższe, wykonanie zalecenia nr 7 ocenia się pozytywnie.

(Dowód: akta kontroli str.: 180-182, 189)

7. <u>Realizacja zaleceń pokontrolnych nr 8, 9 i 10.</u>
„W ramach wprowadzonej polityki haseł stosować minimalną długość hasła, tj. 8 znaków" (8)
„Wprowadzić atrybut wymuszania złożoności haseł oraz jego cyklicznej zmiany, co 30 dni" (9)
„Wprowadzić zabezpieczenie w postaci blokady konta użytkownika po trzykrotnym wprowadzeniu błędnego hasła" (10)

W wyniku pierwszej kontroli ustalono, iż w WIJHARS obowiązywała Instrukcja zarządzania systemem informatycznym zawierająca politykę haseł jednostki, której jednak nie stosowano w praktyce.

W toku czynności kontrolnych ustalono, że w WIJHARS, przy pomocy usługi Active Directory, ASI ustanowił złożoność hasła na stacjach roboczych wymagającą spełnienia następujących kryteriów:

- długość hasła na minimum 8 znaków,
- zastosowanie przynajmniej 1 wielkiej litery,
- zastosowanie przynajmniej 1 małej litery,
- zastosowanie przynajmniej 1 znaku specjalnego,
- zastosowanie przynajmniej 1 cyfry.

Ponadto, również przy pomocy usługi Active Directory, ustanowiono cykliczność zmiany haseł na stacjach roboczych w cyklach 30-dniowych. Za pośrednictwem przedmiotowej usługi ustanowiono również blokadę konta użytkownika po trzykrotnym wprowadzeniu błędnego hasła. W zaistniałym przypadku do odblokowania konta dochodzi po 15 minutach, a użytkownik zmuszony jest ponownie wprowadzić hasło, mając na to kolejne 3 próby.

Z uwagi na powyższe, wykonanie zaleceń nr 8, 9 i 10 ocenia się pozytywnie.

(Dowód: akta kontroli str.: 180-182, 190, 191)

8. <u>Realizacja zaleceń pokontrolnych nr 11, 12 i 13.</u>

„Ustawić wygaszacze ekranów na komputerach pracowników zgodne z czasem aktywacji wynikającym z przyjętej Instrukcji oraz bez możliwości edycji przez pracowników" (11)
„Ustalać uprawnienia użytkowników w wykorzystywanych systemach teleinformatycznych oraz na stacjach roboczych stosownie do wykonywanych zadań" (12)
„W przypadku rozwiązania stosunku pracy z pracownikiem niezwłocznie dezaktywować konto" (13)

W wystąpieniu pokontrolnym z 2019 r. stwierdzono, iż na komputerach użytkowników zostały ustawione wygaszacze ekranu, niemiej jednak użytkownicy mieli uprawnienia do edycji lub nawet wyłączenia wygaszacza, a na jednej stacji roboczej pracownik posiadał uprawnienia administratora. Ponadto stwierdzono, iż czas aktywacji wygaszacza ustawiony na komputerach dwóch użytkowników był niezgodny z obowiązującą ówcześnie dokumentacją z zakresu SZBI. Stwierdzono również, iż konto byłego pracownika w module Finanse i Księgowość było nadal aktywne po ustaniu zatrudnienia.

W toku czynności kontrolnych ustalono, iż za pośrednictwem usługi Active Directory ustanowiono automatyczne wygaszanie ekranu po 10 minutach bezczynności. Ponadto, przy pomocy wskazanej usługi, ustanowiono uprawnienia „administratora" jedynie dla ASI, natomiast wszystkie pozostałe konta, a także konta nowo zakładane, posiadają automatycznie ustawione uprawnienia „użytkownika". W przypadku rozwiązania stosunku pracy z pracownikiem powiadamiany jest ASI, który niezwłocznie dezaktywuje konta użytkowników.

Powyższe wskazuje na prawidłową realizację zaleceń pokontrolnych nr 11-13, co należy ocenić pozytywnie.

(Dowód: akta kontroli str.: 180-182, 192, 193-194, 195)

9. <u>Realizacja zalecenia pokontrolnego nr 14.</u>

„W porozumieniu z wykonawcą oprogramowania zapewnić atrybut rozliczalności w systemie Symfonia"

W wyniku kontroli z 2019 r. stwierdzono, iż stosowany w WIJHARS system Symfonia nie posiadał modułu rozliczalności.

W toku czynności kontrolnych ASI wyjaśnił, iż: „telefonicznie skontaktowano się z działem wsparcia obsługi programu „Symfonia" odnośnie możliwości wprowadzenia pełnego modułu rozliczalności. Uzyskano informację, iż dla małych podmiotów nie przewiduje się wprowadzenia takiej modyfikacji. Drugi system – R2Płatnik – posiada moduł rozliczalności". Mając na uwadze powyższe należy wskazać, iż zgodnie z § 20 ust. 1 r.k.r.i., rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Brak wskazanego modułu rozliczalności w systemie Symfonia wskazuje, iż korzystanie z tego systemu przez WIJHARS wiąże się z naruszeniem § 20 ust. 1 r.k.r.i. W przypadku braku możliwości modyfikacji systemu przez producenta systemu w zakresie zapewnienia rozliczalności, kontrolowany winien stosować inny system teleinformatyczny, zapewniający atrybuty wskazane w r.k.r.i.

Wobec powyższego stwierdzono, iż kontrolowany nie zrealizował zalecenia pokontrolnego nr 14, co należy ocenić negatywnie.

(Dowód: akta kontroli str.: 180-182, 196)

10. Realizacja zaleceń pokontrolnych nr 15 i 16.

„W przypadku kopii zapasowych zapewnić retencję danych z okresu co najmniej 2 tygodni" (15)

„Zapewnić częstsze wykonywanie kopii zapasowej, która jest przechowywana na zewnętrznym nośniku danych" (16)

W wyniku kontroli ustalono, iż w WIJHARS stosowane jest oprogramowanie Veeam służące do zarządzania sporządzaniem kopii zapasowych zasobów jednostki. Kopie tworzone są w cyklu dwutygodniowym. Oprócz przechowywania ich w postaci cyfrowej, kopie zapasowe przechowywane są również na dysku zewnętrznym i aktualizowane co 14 dni.

Powyższe wskazuje na zrealizowanie zaleceń pokontrolnych nr 15 i 16, co należy ocenić pozytywnie.

(Dowód: akta kontroli str.:180-182, 197)

11. Podsumowanie.

W wyniku kontroli stwierdzono, iż z 16 zaleceń pokontrolnych sformułowanych w wystąpieniu pokontrolnym z dnia 5 marca 2020 r. skutecznie wdrożono 14 z nich, 1 wdrożono w niepełny sposób (zalecenie nr 3), 1 zaś nie wdrożono (zalecenia nr 14).

IV. Pozostałe informacje, zalecenia pokontrolne i pouczenie

Sprawozdanie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach. Jeden egzemplarz przekazano Dolnośląskiemu Wojewódzkiemu Inspektorowi Jakości Handlowej Artykułów Rolno-Spożywczych.

Mając na uwadze art. 52 ust. 4 ustawy o kontroli w administracji rządowej w celu wyeliminowania stwierdzonych nieprawidłowości należy:

1. Zamieszczać informacje o dacie sporządzenia oraz osobie sporządzającej na dokumencie obrazującym przeprowadzenie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji.
2. W treści Instrukcji Bezpieczeństwa, stanowiącej załącznik nr 2 do Polityki Bezpieczeństwa Informacji według normy PN-ISO/IEC 27001:2013 wskazać formę zgłoszenia zdarzenia naruszającego bezpieczeństwo informacji.
3. Korzystać z systemów teleinformatycznych posiadających moduł rozliczalności.

Informację o sposobie wykonania powyższych zaleceń lub przyczynach ich niewykonania należy przesłać do dnia **24 stycznia 2025 r.**

Ponadto zgodnie z art. 52 ust. 5 ustawy o kontroli w administracji rządowej: Kierownik jednostki kontrolowanej w terminie 3 dni roboczych od dnia otrzymania sprawozdania ma prawo przedstawić do niego stanowisko - nie wstrzymuje to realizacji ustaleń kontroli.

Z up. WOJEWODY DOLNOŚLĄSKIEGO
Damian Domusiewicz
DYREKTOR WYDZIAŁU
Wydział Kontroli