WOJEWODA DOLNOŚLĄSKI

KO-KZ.431.2.3.2024.TW

Pan
Zdzisław Król
Dolnośląski Wojewódzki Lekarz Weterynarii

ul. Januszowicka 48
53-135 Wrocław

SPRAWOZDANIE

Wrocław, dnia 6 grudnia 2024 r.

I. Informacje organizacyjne

Jednostka kontrolowana	Wojewódzki Inspektorat Weterynarii we Wrocławiu
Kierownik jednostki kontrolowanej	Zdzisław Król - Dolnośląski Wojewódzki Lekarz Weterynarii
Zakres kontroli	Realizacja przez Dolnośląskiego Wojewódzkiego Lekarza Weterynarii zaleceń sformułowanych w wystąpieniu pokontrolnym z dnia 28 listopada 2019 r. (znak: NK-KE.431.39.2019.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 21 do 31 października 2024 r.
Kontrolerzy	Tomasz Woch – Główny Specjalista z Wydziału Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, upoważnienie nr 30 z dnia 18 października 2024 r. (KO-KZ.0030.30.2024.TW).

(dowód: akta kontroli str.: 5 -6)

[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 od 7 do 30 października 2019 r. zespół kontrolny z Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu przeprowadził w Wojewódzkim Inspektoracie Weterynarii 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 WIW oceniono negatywnie. W wystąpieniu pokontrolnym z dnia 28 listopada 2019 r. wskazano, mając na uwadze stwierdzone nieprawidłowości, iż w celu ich wyeliminowania należy[4]:

1. Zapewnić aktualizację dokumentacji z zakresu SZBI w ramach zmieniającego się otoczenia zewnętrznego i wewnętrznego.
2. Opracować i wdrożyć kompleksową dokumentację z zakresu SZBI, w szczególności dotyczącą szacowania ryzyka oraz zasad przeprowadzania okresowych analiz ryzyka.
3. Przeprowadzać okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji.
4. Przynajmniej raz w roku przeprowadzać audyt wewnętrzny w zakresie bezpieczeństwa informacji.
5. Uporządkować pomieszczenie serwerowni nr 1 oraz odpowiednio doposażyć oba pomieszczenia w zakresie brakujących urządzeń wskazanych w ustaleniach z kontroli.
6. W celu zwiększenia bezpieczeństwa sieci LAN podzielić ją na kilka sieci VLAN.
7. Przestrzegać wprowadzonej w Instrukcji polityki haseł w zakresie częstotliwości wymuszania zmiany hasła oraz jego długości.
8. Aktywować ustawienia określające złożoność haseł.
9. Ustalić i aktywować w domenie automatyczne uruchamianie wygaszacza ekranu.
10. W ramach aplikacji PROGMAN nadawać uprawnienia pracownikom stosownie do zakresu obowiązków.
11. Podjąć działania w celu ochrony kopii zapasowych (aplikacji PROGMAN) przed dostępem nieupoważnionych pracowników.
12. Podjąć działania, w porozumieniu z wykonawcą systemu vetLINK, które umożliwią ASI bardziej szczegółowe określanie uprawnień dla poszczególnych użytkowników oraz zapewnią rozliczalność na poziomie aplikacji.
13. Zapewnić narzędzie dla ASI umożliwiające prowadzenie inwentaryzacji zasobów informatycznych.

[3] Dalej jako: WIW, kontrolowana jednostka.
[4] W dalszej części niniejszego dokumentu zwane zaleceniami z przypisanym im numerem od 1 do 13.

Jako termin realizacji powyższych zaleceń (lub termin wskazania przyczyn braku ich realizacji) wskazano dzień 13 grudnia 2019 r. W sporządzonej tego dnia odpowiedzi kontrolowany organ, w zakresie powyższych zaleceń, wskazał co następuje[5]:

1. Polityka ochrony danych została zaktualizowana w dniu 2 grudnia 2019 r.
2. Dokumenty zostaną opracowane oraz wdrożone w pierwszym kwartale 2020 roku.
3. Zakupiono moduł podatności na urządzenia UTM. Trwają poszukiwania odpowiedniego oprogramowania (realizacja zalecenia nastąpi w pierwszym półroczu 2020 roku).
4. Zakupiono moduł podatności na urządzenia UTM. Trwają poszukiwania odpowiedniego oprogramowania (realizacja zalecenia nastąpi w pierwszym półroczu 2020 roku).
5. Do dnia 20 grudnia 2019 r. zostanie usunięty papier z otwartych regałów. Do dnia 30 grudnia 2019 r. zostaną zakupione mierniki temperatury oraz wilgotności. Do dnia 31 stycznia 2020 r. do systemu alarmowego zostanie włączony czujnik dymu.
6. Począwszy od pierwszego kwartału 2020 roku będzie sukcesywnie realizowany podział fizycznej sieci LAN na logiczne sieci LAN.

7 – 9. W dniach 3 i 4 grudnia 2019 r. wdrożono ustawienia dotyczące długości i złożoności haseł oraz wymuszonej częstotliwości ich zmian oraz ustawienia dotyczące wygaszaczy ekranu na stacjach roboczych.

10. W dniu 9 grudnia 2019 r. dostosowano uprawnienia poszczególnych pracowników do zajmowanych przez nich stanowisk.
11. W dniu 12 grudnia 2019 r. wyłączono uprawnienia administracyjne użytkownikom AD.
12. W dniu 9 grudnia 2019 r. skierowano odpowiednie pismo do autora oprogramowania. Kolejne działania będą realizowane w pierwszym kwartale 2020 roku.
13. W pierwszym półroczu 2020 roku zostanie zakupione oraz wdrożone odpowiednie oprogramowanie.

2. Realizacja zalecenia pokontrolnego nr 1.

W wyniku pierwszej kontroli w 2019 roku stwierdzono, iż wówczas obowiązująca w WIW dokumentacja z zakresu Systemu Zarządzania Bezpieczeństwem Informacji[6] nie była aktualna, ponieważ nie uwzględniała wszystkich systemów informatycznych, jakie funkcjonowały w kontrolowanej jednostce[7]. Kontrola wykazała, że obecnie obowiązująca dokumentacja z zakresu SZBI nie zawiera powyższych braków.

Mając na uwadze powyższe należy pozytywnie ocenić wdrożenie zalecenia nr 1.

(dowód: akta kontroli str.: 33 - 55)

3. Realizacja zalecenia pokontrolnego nr 2.

W wyniku pierwszej kontroli stwierdzono, iż dokumentacja z zakresu SZBI obowiązująca w kontrolowanej jednostce była fragmentaryczna, ponieważ nie uwzględniała takich obszarów jak: zasady dostępu do pomieszczeń (w tym serwerowni), zasady prowadzenia rejestru aktywów informatycznych, zasady prowadzenia okresowych analiz ryzyka lub szacowania ryzyka, zagadnień związanych z projektowaniem, budową, wdrażaniem oraz

[5] Numery poszczególnych punktów odpowiadają numerom przypisanym poszczególnym zaleceniom.
[6] Dalej jako: SZBI.
[7] Nie uwzględniała ona systemu vetLINK.

monitorowaniem systemów, procedury wewnętrznego audytu bezpieczeństwa informacji oraz zasad prowadzenia szkoleń dla osób zaangażowanych w przetwarzanie informacji.

W czasie prowadzenia niniejszej kontroli okazano dokumenty pn.: *Polityka Ochrony Danych w Wojewódzkim Inspektoracie Weterynarii we Wrocławiu*[8] oraz *Instrukcja Zarządzania Systemem Informatycznym w Wojewódzkim Inspektoracie Weterynarii we Wrocławiu*[9]. Przedmiotem ich regulacji są m. in. zasady dostępu do pomieszczeń, gdzie przetwarzane są dane[10]. W zakresie pozostałych z ww. obszarów, co do których stwierdzono w 2019 roku, iż nie zostały objęte dokumentacją SZBI, ustalono[11], iż aktualna dokumentacja opracowana dla przedmiotowego obszaru również ich nie obejmuje. W zakresie zasad dostępu do pomieszczenia serwerowni wskazano, iż z uwagi na to, iż dostęp do niej jest limitowany za pomocą kart dostępu, to możliwym jest ustalenie kto i kiedy w niej przebywał. W zakresie cyklicznych szkoleń dla osób zaangażowanych w proces przetwarzania danych wskazano, iż każdy z pracowników WIW przed dopuszczeniem do ww. informacji odbywa stosowne szkolenie. W zakresie projektowania, budowy oraz wdrażania systemów informatycznych wskazano, iż uregulowanie tych kwestii nie jest możliwe z uwagi na różnorodność oprogramowania oraz na to, iż korzystanie z niektórych aplikacji wymuszane jest na WIW przez jednostki nadrzędne. Systemy z jakich korzysta kontrolowana jednostka są na bieżąco monitorowane w czasie ich działalności i w razie konieczności są podejmowane stosowne działania naprawcze.

Powyższych wyjaśnień nie można przyjąć z następujących względów. Z uwagi na kluczowe znaczenie serwerowni dla procesu bezpiecznego przetwarzania danych w WIW dokumentacja z zakresu SZBI powinna regulować zasady przyznawania, odbierania oraz monitorowania uprawnień do dostępu do tego pomieszczenia. Sama możliwość ustalenia kto i kiedy w niej przebywał jest niewystarczająca z uwagi na to, iż jest to działanie wtórne. Tymczasem, aby zapewnić jak najskuteczniejszą ochronę danych należy wdrożyć rozwiązania pozwalające na uniknięcie naruszenia ich bezpieczeństwa, nie zaś jedynie działania pozwalające na ustalenie kręgu osób potencjalnie odpowiedzialnych za jego powstanie.

W kwestii konieczności uregulowania w SZBI zasad przeprowadzania cyklicznych szkoleń dla pracowników zajmujących się przetwarzaniem danych chodzi o to, aby zasady utrzymywania wiedzy i kompetencji pracowników na odpowiednim poziomie były odpowiednio sformalizowane. Dzięki temu obowiązywać będą jednolite zasady ich przeprowadzania oraz odstępy czasowe pomiędzy poszczególnymi z nich, co pozwoli na uniknięcie sytuacji, w której pracownik (lub ich grupa) będzie przez dłuższy czas nieobjęta jakąkolwiek formą podniesienia wiedzy i kompetencji w powyższym zakresie.

W zakresie odnoszącym się do uregulowania w SZBI kwestii projektowania, budowy oraz wdrażania systemów informatycznych oraz monitorowania ich pracy należy zaznaczyć, iż organ kontroli zdaje sobie sprawę z faktu, iż niektóre z narzędzi informatycznych, z jakich korzysta WIW są mu *narzucone* przez organ nadrzędny, w związku z czym zadanie w zakresie ich projektowania i budowy spoczywa na nim, nie zaś na kontrolowanej jednostce. Niemniej jednak dokumentacja z zakresu SZBI powinna w ramowy sposób określać opisane na wstępie niniejszego akapitu kwestie tam, gdzie jest to możliwe do wykonania, mając na względzie to, aby nie naruszać bezpieczeństwa danych przetwarzanych przy ich pomocy.

Podsumowując powyższe należy wskazać, iż zgodnie z § 19 ust. 1 rozporządzenia Rady Ministrów z dnia 24 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych

[8] Dalej jako: *Polityka*.
[9] Dalej jako: *Instrukcja*.
[10] Patrz: pkt 2 zagadnienia pn. *Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych* zawartego w *Instrukcji*.
[11] Patrz: pkt 1 pisma Dolnośląskiego Wojewódzkiego Lekarza Weterynarii we Wrocławiu z dnia 12 listopada 2024 r. (znak: WIWorg.1610.4.2024), dalej jako: wyjaśnienia z dnia 12 listopada 2024 r.

wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[12] podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Oznacza to, iż podmiot kontrolowany ma obowiązek posiadać i stosować (oraz modyfikować, gdy zajdzie taka potrzeba) dokumentację SZBI, która w sformalizowany sposób będzie określała zasady polityki bezpieczeństwa informacji. Tym samym nie jest dopuszczalne pomijanie jakiejkolwiek z ww. zasad.

Ponadto przekazane w toku kontroli dokumenty nie zostały opatrzone datą ani informacją kto je sporządził i zatwierdził. Powyższe nie wypełnia zatem obowiązku *ustanowienia*[13], o którym mowa w § 19 ust. 1 r.k.r.i. Zważyć również należy, że dokumentacja wewnętrzna powstająca w danym podmiocie stanowi system kontroli zarządczej[14].

Mając na uwadze powyższe należy negatywnie ocenić wdrożenie zalecenia nr 2.

(dowód: akta kontroli str.: 33 - 66)

4. Realizacja zaleceń pokontrolnych nr 3 i nr 4.

Zalecenia pokontrolne nr 3 i nr 4 dotyczyły okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz audytów bezpieczeństwa informacji. Z uwagi na podobieństwo powyższych obszarów zostaną one omówione w jednym punkcie.

W toku kontroli ustalono, na podstawie udzielonych przez pracowników WIW wyjaśnień, iż analiza oraz audyt, o jakich mowa w powyższych zaleceniach nie są przeprowadzane cyklicznie, lecz są prowadzone w sposób ciągły. Taki sposób działania uzasadniono tym, iż programy i aplikacje wykorzystywane przez kontrolowaną jednostkę przy wykonywaniu przez nią zadań wymuszają cykliczne aktualizacje oraz przeglądy bezpieczeństwa danych. Ponadto działania w powyższym zakresie są prowadzone przez ASI[15] na podstawie zgłoszeń poszczególnych użytkowników jak i z własnej inicjatywy. Z udzielonych wyjaśnień wynika również to, iż posiadane zasoby (zarówno materialne jak i niematerialne) pozwalają na stałe monitorowanie bezpieczeństwa danych.

W toku kontroli okazano również zbiór zidentyfikowanych ryzyk, jakie mogą wystąpić w związku z działalnością kontrolowanej jednostki wraz z określeniem ich rodzaju, możliwego obszaru oraz prawdopodobieństwa wystąpienia, wpływu na klienta zewnętrznego WIW, opis planowanych do podjęcia działań (w przypadku wystąpienia ryzyka) oraz osób odpowiedzialnych za ich przeprowadzenie. Z uzyskanych wyjaśnień od kierownika kontrolowanej jednostki wynika, iż powyższy zbiór opracowała osoba zatrudniona w WIW na stanowisku głównego informatyka na przełomie lat 2023-2024. Od czasu jego opracowania nie wystąpiły jakiekolwiek wydarzenia mające wpływ na treść powyższych informacji, w tym na istotność oraz prawdopodobieństwo wystąpienia poszczególnych ryzyk. Poziomy wystąpienia poszczególnych ryzyk zostały ustalone na podstawie subiektywnej oceny pracownika opracowującego ww. zbiór. Należy przy tym zaznaczyć, iż nie da się stwierdzić czy w treści powyższego zbioru wprowadzano jakiekolwiek zmiany, albowiem jest

[12] Dz. U. poz. 773, dalej jako: r.k.r.i.

[13] Zgodnie ze Słownikiem Języka Polskiego PWN zwrot ten oznacza *uczynić coś obowiązującym urzędowo, oficjalnie*.

[14] Patrz: pkt 10 Standardów kontroli zarządczej jednostek sektora finansów publicznych, stanowiących załącznik do komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (dostępne na stronie: https://www.gov.pl/web/finanse/standardy-i-wytyczne-kontrola-zarzadcza).

[15] Administrator Systemu Informatycznego.

to wyłącznie dokument wewnętrzny, w którego treść są wprowadzane na bieżąco bez zachowywania poprzednich wersji[16].

Mając na uwadze powyższe należy wskazać co następuje. W wyniku kontroli przeprowadzonej w 2019 roku w WIW stwierdzono, iż w wówczas istniejącej i obowiązującej dokumentacji z zakresu SZBI brak było zapisów dotyczących identyfikacji i przeglądów ryzyk, jak również to, iż nie był przeprowadzany coroczny, wymagany przepisami r.k.r.i. audyt bezpieczeństwa informacji. Z wyjaśnień[17] pozyskanych w czasie obecnej kontroli wynika, co opisano wcześniej, iż stan ten nie uległ zmianie. Pozytywnie należy ocenić fakt opracowania i stosowania przez kontrolowaną jednostkę macierzy ryzyk oraz to, iż jej treść jest na bieżąco analizowana i aktualizowana. Niemniej jednak z uwagi na znaczenie tych narzędzi (tj. audytu w zakresie bezpieczeństwa informacji oraz przeglądów ryzyk) w procesie zapewnienia bezpieczeństwa informacji należy negatywnie ocenić fakt braku przeprowadzania audytów w zakresie bezpieczeństwa informacji oraz sformalizowanych okresowych analiz ryzyka. W szczególności, iż r.k.r.i.[18] wprost nakłada obowiązek ich realizacji. Wprawdzie nie narzucają one żadnej formy w jakich należy ich dokonywać, niemniej jednak prowadzenie ich wyłącznie w *formie ciągłej,* jak wynika z dowodów zebranych w toku kontroli, nie może zostać przyjęte. Jak bowiem ustalono w toku kontroli w wyniku tych działań nie powstaje żaden dokument, który podsumowuje ustalenia, jakie poczyniono poddawanym badaniu okresie. Obowiązujący obecnie w WIW system działania w powyższych obszarach pozwala tym samym jedynie na sprawdzenie, jak kształtuje się aktualny stan bezpieczeństwa teleinformatycznego i jakie są aktualne poziomy wystąpienia poszczególnych ryzyk. Nie pozwala on natomiast (z powodu braku dokumentacji) na sprawdzenie jak kształtowały się poziomy poszczególnych ryzyk w przeszłości oraz jak podejmowane przez kontrolowaną jednostkę działania (np. w wyniku sformalizowanych działań audytowych lub okresowych analiz ryzyka) wpłynęły na ich poziom, a tym samym czy były skuteczne w dłuższej perspektywie czasu, jak również czy przyczyniają się do długookresowego zwiększenia bezpieczeństwa teleinformatycznego jednostki.

Poza powyższym należy również zaznaczyć, iż opisana powyżej forma działania kontrolowanej jednostki w przedmiotowych obszarach skutkuje brakiem danych co do tego jak zmieniał się w czasie poziom danego ryzyka, a co za tym idzie czy w dalszym ciągu jest ono aktualne.

Z opisanych powyżej przyczyn należy negatywnie ocenić sposób wdrożenia zaleceń nr 3 i nr 4.

(dowód: akta kontroli str.: 18, 21 – 22, 29 - 30)

5. Realizacja zalecenia pokontrolnego nr 5.

W toku kontroli przeprowadzono oględziny serwerowni mieszczącej się w budynku głównym siedziby WIW oraz serwerowni mieszczącej się w budynku Zakładu Higieny Weterynaryjnej (obydwa budynki są położone na tej samej nieruchomości).

● W serwerowni mieszczącej się na pierwszym piętrze budynku głównego Wojewódzkiego Inspektoratu Weterynarii, w porównaniu ze stanem ustalonym w 2019 roku stwierdzono:

- usunięcie materiałów papierowych z pomieszczenia serwerowni (znajduje się tam wyłącznie sprzęt informatyczny);
- zamontowano czujnik wilgotności;
- wprowadzono fizyczną kontrolę dostępu do pomieszczenia serwerowni;

[16] Patrz: pkt 2 wyjaśnień z dnia 12 listopada 2024 r.

[17] Patrz: protokół z dnia 21 października 2024 r. zawierający ustne wyjaśnienia złożone przez pracowników WIW oraz pkt 1.b. wyjaśnień z dnia 12 listopada 2024 r.

[18] Parz: § 19 ust. 1 i ust. 2 pkt 14 r.k.r.i.

- zdemontowano wewnętrzną ściankę działową;
- drewniane meble zastąpiono metalowym regałem;
- w pozostałym zakresie pomieszczenie serwerowni nie uległo zmianom od 2019 roku.

● W serwerowni mieszczącej się na parterze budynku Zakładu Higieny Weterynaryjnej Wojewódzkiego Inspektoratu Weterynarii, w porównaniu ze stanem ustalonym w 2019 roku stwierdzono:
- zamontowano czujnik wilgotności, temperatury oraz dymu;
- w pozostałym zakresie pomieszczenie serwerowni nie uległo zmianom od 2019 roku (w tym w zakresie braku zabezpieczeń fizycznych na oknie).
W toku oględzin dokonano utrwalenia stanu faktycznego za pomocą aparatu w telefonie, które stanowią załącznik do protokołu oględzin.

Mając na uwadze stan powyższych pomieszczeń w 2019 roku należy stwierdzić, iż pomieszczenie serwerowni nr 1 uporządkowano poprzez usunięcie z niego materiałów łatwopalnych, jak również doposażono je w czujnik wilgotności oraz fizyczną kontrolę dostępu do pomieszczenia. Pomieszczenie serwerowni nr 2 również doposażono w brakujące w czasie poprzedniej kontroli urządzenia (tj. czujnik wilgotności, dymu oraz urządzenie do mierzenia temperatury). Negatywnie należy natomiast ocenić fakt, iż okno pomieszczenia serwerowni nr 2 (mieszczącej się na parterze budynku) w dalszym ciągu nie posiada jakichkolwiek fizycznych zabezpieczeń.

(dowód: akta kontroli str.: 8 – 17, 32)

6. Realizacja zalecenia pokontrolnego nr 6.

W wyniku kontroli ustalono, iż w okresie od zakończenia kontroli sformalizowanej wystąpieniem z dnia 28 listopada 2019 r. w kontrolowanej jednostce dokonano kompleksowej inwentaryzacji sieci LAN oraz zakupiono urządzenie brzegowe UTM[19]. Działania te umożliwiły efektywny podział dotychczasowej sieci, co wykazano poprzez udostępnienie schematów podziału sieci funkcjonującej w WIW. W toku kontroli wskazano, iż powyższe przedsięwzięcie zostało zrealizowane w siedzibie kontrolowanej jednostki mieszczącej się we Wrocławiu. Prace dotyczące sieci w siedzibie WIW w Legnicy wciąż trwają.

Mając na uwadze powyższe należy pozytywnie ocenić sposób wdrożenia niniejszego zalecenia.

(dowód: akta kontroli str.: 19, 28)

7. Realizacja zaleceń pokontrolnych nr 7 – nr 9.

Zalecenia pokontrolne nr 7 – nr 9 zawarte w wystąpieniu pokontrolnym z dnia 28 listopada 2019 r. odnoszą się do polityki haseł (ich złożoności oraz częstotliwości zmian) oraz do funkcjonowania wygaszaczy ekranu na poszczególnych stacjach roboczych. Z uwagi na to, iż dotyczyły one pokrewnych obszarów zostaną one omówione w jednym punkcie.

W toku kontroli pracownicy WIW odpowiadający za obszar będący przedmiotem niniejszej kontroli wyjaśnili, iż wszystkie komputery w kontrolowanej jednostce są w domenie (brak jest indywidualnych stacji roboczych). Dzięki temu użytkownikom tej domeny można narzucać (bez możliwości obejścia) określone zasady korzystania z niej, w tym dotyczące powyższych kwestii. Z okazanych zasad polityki domeny WIW wynika, iż zalecenia w zakresie

[19] Jest to wielofunkcyjna bramka bezpieczeństwa funkcjonująca na styku sieci z Internetem.

wskazanym w pkt 7 – pkt 9 wystąpienia pokontrolnego z dnia 28 listopada 2019 r. zostały skutecznie wdrożone.

(dowód: akta kontroli str.: 19, 23)

8. Realizacja zaleceń pokontrolnych nr 10 i nr 11.

Zalecenia pokontrolne nr 10 i nr 11 zawarte w wystąpieniu pokontrolnym z dnia 28 listopada 2019 r. dotyczyły zarządzania zakresem uprawnień poszczególnych pracowników WIW oraz dostępu jaki mieli oni do kopii zapasowych. Z tego względu ich wdrożenie zostanie omówione w ramach jednego punktu.

W toku kontroli ustalono, iż zakończenie współpracy z daną osobą nie skutkuje usunięciem jej konta, lecz jego wyłączeniem. Jedynie osoby pełniące funkcję ASI posiadają uprawnienia administratora, pozostali zaś pracownicy jedynie uprawnienia użytkowników, bez dostępu do kopii zapasowych.

W związku z powyższym należy pozytywnie ocenić sposób wdrożenia zaleceń pokontrolnych nr 10 i nr 11.

(dowód: akta kontroli str.:19, 30 - 31)

9. Realizacja zalecenia pokontrolnego nr 12.

W wyniku kontroli stwierdzono, iż ASI ma możliwość szczegółowego nadawania uprawnień poszczególnym użytkownikom aplikacji vetLINK, adekwatnych do pełnionych przez nich funkcji. Ponadto na poziomie powyższego oprogramowania są widoczne działania poszczególnych jego użytkowników, co skutkuje zapewnieniem wymogu rozliczalności.

Mając na uwadze powyższe należy pozytywnie ocenić wdrożenie zalecenia pokontrolnego nr 12.

(dowód: akta kontroli str.: 19 – 20, 24 - 25)

10. Realizacja zalecenia pokontrolnego nr 13.

W wyniku kontroli stwierdzono, na podstawie udzielonych wyjaśnień oraz okazanych zestawień, iż w kontrolowanej jednostce ASI podjął działania, w wyniku których została stworzona lista zasobów informatycznych z przypisanymi do nich użytkownikami, opisem cech oraz zainstalowanego oprogramowania. Urządzenia te podzielone są na grupy, natomiast posiadane narzędzie umożliwia wygenerowanie listy urządzeń (wraz z ich cechami) przypisanych do poszczególnych osób.

Mając na uwadze powyższe należy pozytywnie ocenić wdrożenie zalecenia pokontrolnego nr 13.

(dowód: akta kontroli str.: 20, 26 - 27)

11. Podsumowanie.

W wyniku kontroli stwierdzono, iż z 13 zaleceń pokontrolnych sformułowanych w wystąpieniu pokontrolnym z dnia 28 listopada 2019 r. skutecznie wdrożono 9 z nich, 1 wdrożono w niepełny sposób (zalecenie nr 5), 3 zaś nie wdrożono (zalecenia nr 2 – nr 4).

IV. Pozostałe informacje, zalecenia pokontrolne i pouczenie

Sprawozdanie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach. Jeden egzemplarz przekazano Dolnośląskiemu Wojewódzkiemu Lekarzowi Weterynarii we Wrocławiu.

Mając na uwadze art. 52 ust. 4 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej w celu wyeliminowania stwierdzonych nieprawidłowości należy:

1. Dokończyć opracowywanie dokumentacji SZBI.
2. Poza już prowadzonymi działaniami, przeprowadzać okresowe analizy ryzyka utraty integralności, dostępności oraz poufności informacji oraz co najmniej raz w roku audyt wewnętrzy w zakresie bezpieczeństwa informacji.

Informację o sposobie wykonania powyższych zaleceń lub przyczynach ich niewykonania należy przesłać do dnia **24 grudnia 2024 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