Z A T W I E R D Z A M

WOJEWODA OPOLSKI

Adrian Czubak

PN.I.431.1.4.2020.RCh

INFORMACJA O WYNIKACH KONTROLI

w przedmiocie:

Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej w urzędach jednostek samorządu terytorialnego w województwie opolskim

Opole, dnia 17 czerwca 2020 r.

SPIS TREŚCI

WYKAZ POJĘĆ I AKTÓW PRAWNYCH

CSIRT NASK	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy
dostępność	właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym
integralność	właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony
poufność	właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym
rejestr publiczny	rejestr, ewidencja, wykaz, lista, spis albo inna forma ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie przepisów ustawowych
rozliczalność	właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie
rozporządzenie KRI	rozporządzenie 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 (Dz. U. z 2017 r. poz. 2247)
system teleinformatyczny	zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 ze zm.)
System Zarządzania Bezpieczeństwem Informacji (SZBI)	część całościowego systemu zarządzania, oparty na podejściu wynikającym ze zidentyfikowanego ryzyka, odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji
ustawa o informatyzacji	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346 ze zm.)
ustawa o kontroli	ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224)
ustawa o krajowym systemie cyberbezpieczeństwa (ksc)	ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz.1560 ze zm.)

I. WPROWADZENIE

Zapewnienie sprawnego funkcjonowania systemów teleinformatycznych i bezpieczeństwa informacji to dzisiaj jedno z najistotniejszych wyzwań stojących przed administracją publiczną. Oprócz oczywistych aspektów zarządczych realizacji powyższego celu, pozytywną rolę w tym zakresie powinna odegrać nowoczesna kontrola poprzez realizację swej funkcji oceniająco-informacyjnej, która jest nie do przecenienia. Wskazują na to także priorytety kontroli, określane w ostatnich latach przez Szefa Kancelarii Prezesa Rady Ministrów, m.in. dla urzędów wojewódzkich.

W związku z powyższym w latach 2017-2020 służby kontrolne Wojewody Opolskiego przeprowadziły w urzędach jednostek samorządu terytorialnego /województwa opolskiego/ wszystkich szczebli, łącznie 13 kontroli problemowych w przedmiocie: Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej[1]. W tym zrealizowano: 10 kontroli w urzędach gmin / miejskich[2], 2 kontrole w starostwach powiatowych[3], a 1 kontrolę w Urzędzie Marszałkowskim Województwa Opolskiego.

Celem kontroli była ocena urzędów jednostek samorządu terytorialnego[4] w obszarze działania systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej. W przypadku stwierdzenia nieprawidłowości, celem kontroli było również ustalenie ich zakresu, przyczyn i skutków oraz osób za nie odpowiedzialnych, a także sformułowanie zaleceń zmierzających do usunięcia nieprawidłowości. Oprócz powyższego, bardzo ważnym celem kontroli było usprawnienie funkcjonowania jednostek kontrolowanych.

W toku kontroli największy nacisk położono na kwestie związane z funkcjonowaniem Systemów Zarządzania Bezpieczeństwem Informacji. Prawidłowe działanie każdego systemu teleinformatycznego jest bowiem uwarunkowane sprawnie funkcjonującym SZBI. Podstawowym, powszechnie obowiązującym aktem prawnym, który określa wymagania w tym zakresie jest rozporządzenie KRI.

Efektem przeprowadzonych kontroli było sformułowanie łącznie 107 zaleceń / wniosków dotyczących usunięcia nieprawidłowości lub usprawnienia funkcjonowania jednostek kontrolowanych. Z informacji przedłożonych Wojewodzie Opolskiemu przez kierowników tych jednostek wynika, że zostały one zrealizowane, lub podjęto stosowne działania w celu ich realizacji.

---

[1] Podstawę prawną podjęcia niniejszych kontroli stanowi: art. 25 ust. 1 pkt 3 lit. a i ust. 3 ustawy o informatyzacji, oraz art. 6 ust. 4 pkt 3 i art. 2 pkt 1 ustawy o kontroli.

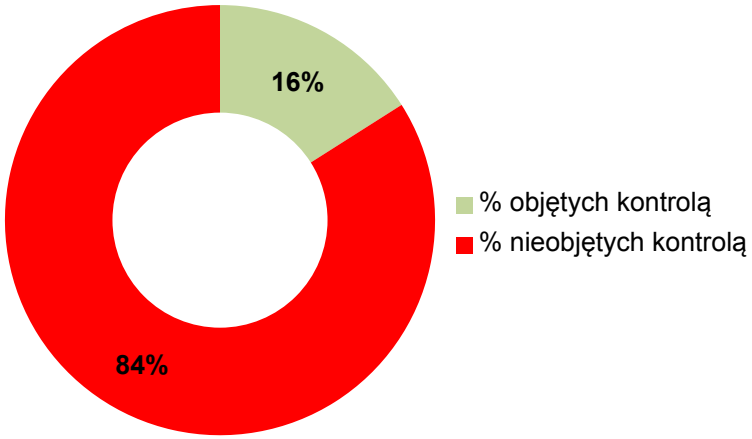
[2] W urzędach gmin w: Popielowie, Pokoju, Murowie i Lasowicach Wielkich; w urzędach miejskich w: Zdzieszowicach, Kluczborku, Grodkowie, Praszce i Lewinie Brzeskim oraz w Urzędzie Gminy i Miasta w Ozimku.

[3] W: Prudniku i Oleśnie.

[4] Do oceny zastosowano kryterium legalności i rzetelności. Średnia długość okresu objętego kontrolą wynosiła 12 miesięcy do dnia rozpoczęcia kontroli (oprócz tego uwzględniano także okres wcześniejszy i późniejszy w zakresie niezbędnym do realizacji celu kontroli).

Celem powstania niniejszego dokumentu[5] jest zagregowanie najistotniejszych ustaleń i wniosków, będących rezultatem przeprowadzonych kontroli w powyższym zakresie oraz przedstawienie ich wszystkim jednostkom samorządu terytorialnego w województwie opolskim. W szczególności zaś tym które dotychczas nie zostały objęte niniejszą kontrolą. Pozwoli to kierownictwu urzędów jednostek samorządu terytorialnego na dokonanie samodzielnego przeglądu pod kątem spełnienia najważniejszych wymagań w swoim obszarze oraz podjęcie stosownych działań celem eliminacji stwierdzonych ewentualnych braków / nieprawidłowości. Jeśli przedmiotowa *Informacja* zostanie w taki sposób wykorzystana, cel jej powstania można będzie uznać za osiągnięty.

Procent jednostek samorządu terytorialnego w województwie opolskim objętych i nieobjętych kontrolą



Cykl funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji[6]

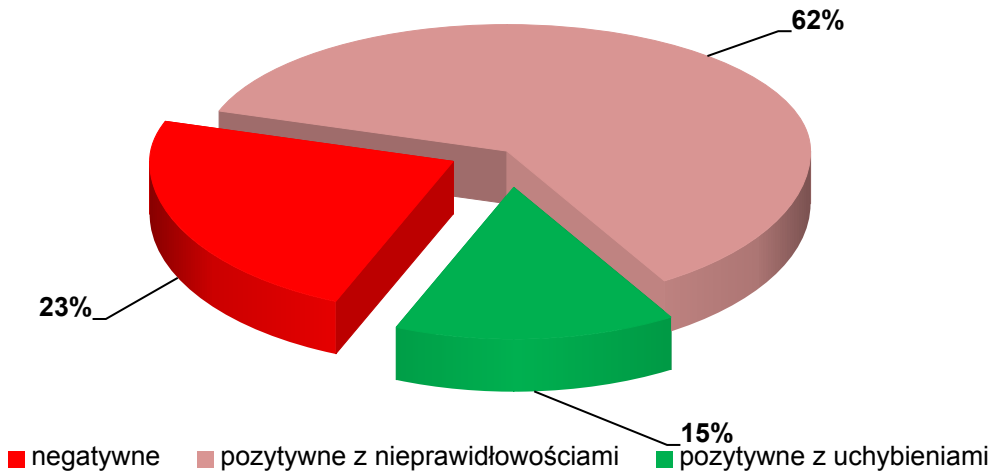
[5] Na podstawie art. 56 ust. 1-3 ustawy o kontroli.

[6] *Informacja o wynikach kontroli. Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego,* Departament Administracji Publicznej NIK, Warszawa 2019, s. 12.

II. OCENA OGÓLNA

Urzędy jednostek samorządu terytorialnego w województwie opolskim, poddane kontroli w obszarze działania systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej, oceniono następująco: negatywnie - 3 (23%), pozytywnie z nieprawidłowościami - 8 (62 %), pozytywnie z uchybieniami - 2 (15%). W ani jednym przypadku nie było podstaw do dokonania tzw. samodzielnej oceny pozytywnej. Pomimo mniejszości – w ogólnej liczbie – ocen negatywnych podkreślić należy, że szczególnie w urzędach ocenionych pozytywnie z nieprawidłowościami, stwierdzono odstępstwa od stanu pożądanego, których w żadnym wypadku nie można bagatelizować. Powyższe wyniki kontroli przemawiają za koniecznością wzmocnienia nadzoru nad przedmiotowym obszarem.

Oceny jednostek kontrolowanych



Wykaz jednostek kontrolowanych i ich ocen

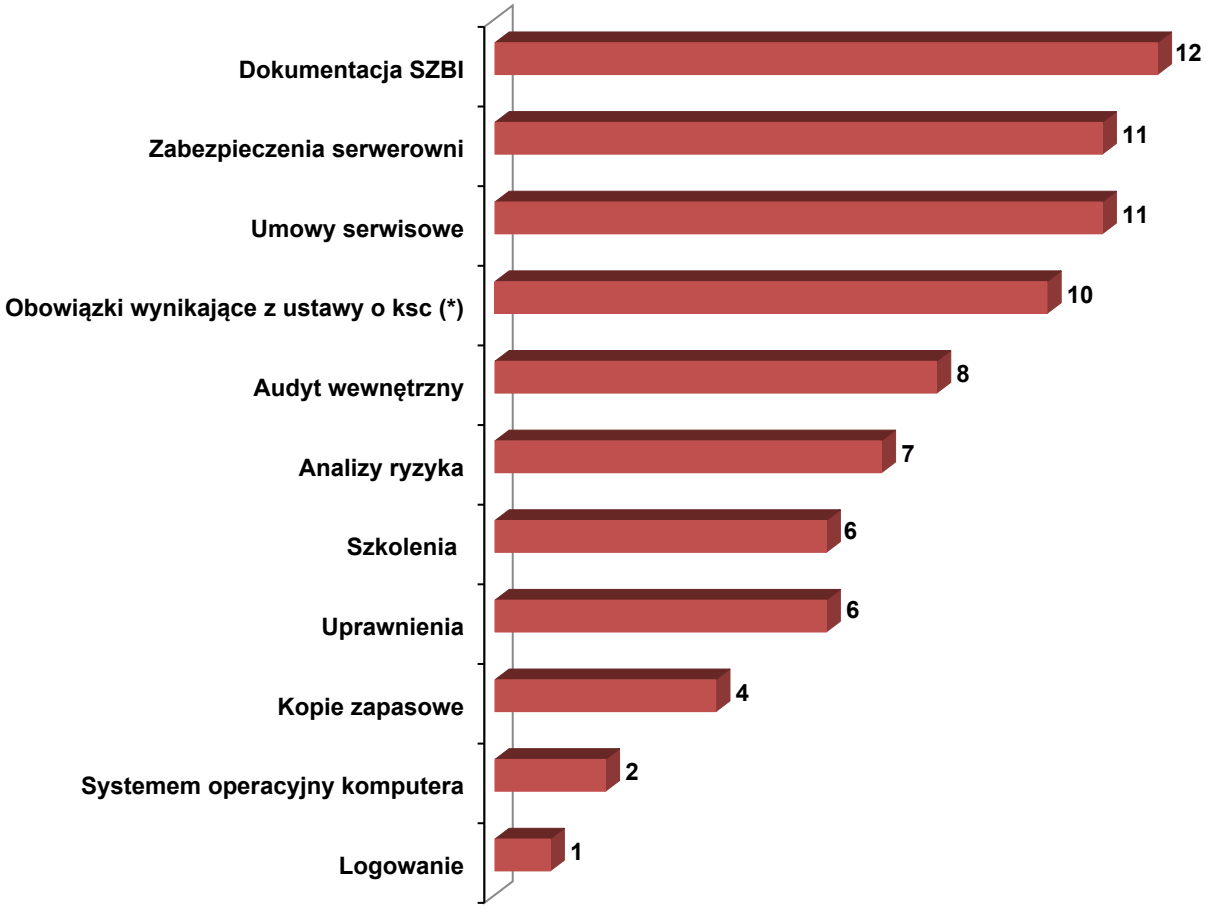
Lp.	Nazwa jednostki kontrolowanej[7]	Ocena kontrolowanej działalności[8]
1.	Urząd Miejski w Zdzieszowicach	Pozytywna z nieprawidłowościami
2.	Urząd Miejski w Kluczborku	Pozytywna z nieprawidłowościami
3.	Urząd Miejski w Grodkowie	Negatywna
4.	Urząd Gminy w Popielowie	Pozytywna z nieprawidłowościami
5.	Urząd Gminy Pokój	Pozytywna z nieprawidłowościami
6.	Urząd Marszałkowski Województwa Opolskiego	Pozytywna z uchybieniami
7.	Starostwo Powiatowe w Prudniku	Negatywna
8.	Urząd Gminy w Murowie	Pozytywna z uchybieniami
9.	Urząd Gminy i Miasta w Ozimku	Pozytywna z nieprawidłowościami
10.	Urząd Miejski w Praszce	Negatywna
11.	Urząd Miejski Lewin Brzeski	Pozytywna z nieprawidłowościami
12.	Urząd Gminy Lasowice Wielkie	Pozytywna z nieprawidłowościami
13.	Starostwo Powiatowe w Oleśnie	Pozytywna z nieprawidłowościami

[7] Wg kolejności realizacji kontroli.

[8] Służby kontrolne Wojewody Opolskiego stosują czterostopniową skalę ocen: pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami i negatywna.

III. USTALENIA KONTROLI WSKAZUJĄCE NA ZAKRES STWIERDZONYCH NIEPRAWIDŁOWOŚCI, ICH PRZYCZYNĘ I SKUTKI

Liczba kontrolowanych urzędów, w których stwierdzono nieprawidłowości, z podziałem na najistotniejsze zagadnienia szczegółowe



(*) Kontroli w tym zakresie poddano tylko 10 urzędów z uwagi na fakt, że przedmiotowa ustawa weszła w życie dopiero w dniu 28 sierpnia 2018 r.

Dokumentacja SZBI

Dokumentacja SZBI w aż 12 urzędach (92%) wymagała poprawy lub uzupełnień, aby spełnić wymóg § 20 ust. 1-2 rozporządzenia KRI. Skala wprowadzanych korekt była zróżnicowana (od niewielkich uzupełnień, do kompleksowego przeredagowania lub opracowania jej od nowa). Najważniejsze i najczęściej identyfikowane w tym zakresie nieprawidłowości to: niezapewnienie kompleksowego opracowania dokumentacji; jej mała funkcjonalność; brak przeglądu i doskonalenia /aktualizacji/ dokumentacji w zakresie dotyczącym zmieniającego się otoczenia; ukierunkowanie jej zapisów na ochronę danych osobowych zamiast na bezpieczeństwo informacji (pojęcie szersze od ochrony danych osobowych); brak określenia w dokumentacji obowiązków wynikających dla jednostki samorządu terytorialnego z ustawy o krajowym systemie cyberbezpieczeństwa.

Zabezpieczenia serwerowni

Kontrole w 11 jednostkach (85%) ujawniły w serwerowniach odstępstwa od stanu pożądanego. Najczęściej stwierdzano: przechowywanie w serwerowni nieużywanego sprzętu komputerowego, dokumentacji archiwalnej, pudeł tekturowych (ryzyko pożaru); niewłaściwe usytuowanie serwerowni (ryzyko zalania wodą np. wskutek możliwości rozszczelnienia przewodu instalacji wodnej, kanalizacyjnej lub centralnego ogrzewania); brak wyposażenia serwerowni w czujnik temperatury i wilgotności, jak również brak innych zabezpieczeń fizycznych. Uwagę kontrolerów zwrócił także przypadek umiejscowienia serwerowni w pokoju informatyka.

Umowy serwisowe

W sumie 11 urzędów (85%) dysponowało umowami serwisowymi – kontrolowanych systemów teleinformatycznych – w których nie zapewniono wystarczającego poziomu bezpieczeństwa informacji (pod względem jej dostępności). Najczęściej identyfikowane odstępstwa od stanu pożądanego w tym zakresie to: brak określenia maksymalnego terminu (lub zbyt długi termin) na usunięcie (przez wykonawcę) awarii / błędów / usterek w systemie; brak określenia kar umownych (lub ich niewielka wysokość) za każdy dzień opóźnienia w usunięciu (przez wykonawcę) awarii / błędów / usterek w systemie.

Obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa

We wszystkich 10 kontrolowanych urzędach (100%)[9] stwierdzono nieprawidłowości dotyczące realizacji obowiązków wynikających dla jednostki samorządu terytorialnego z ustawy o krajowym systemie cyberbezpieczeństwa. Nieprawidłowości te polegały na: niewyznaczeniu – lub stosunkowo późnym wyznaczeniu – osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (obowiązek wynikający z art. 21 ust. 1 ustawy o ksc), oraz opóźnieniach w przekazaniu danych ww. osoby do CSIRT NASK (obowiązek wynikający z art. 22 ust. 1 pkt 5 ustawy o ksc).

Audyt wewnętrzny bezpieczeństwa informacji

W 8 jednostkach (62%) stwierdzono nieprawidłowości w zakresie zapewnienia obowiązkowego audytu wewnętrznego bezpieczeństwa informacji, o którym stanowi

[9] Kontroli w tym zakresie poddano tylko 10 urzędów z uwagi na fakt, że przedmiotowa ustawa weszła w życie dopiero w dniu 28 sierpnia 2018 r.

§ 20 ust. 2 pkt 14 rozporządzenia KRI. Nieprawidłowości te polegały na: nieprzeprowadzaniu corocznie (albo nawet w ogóle) audytu; niezapewnieniu niezależności audytu – jednej z jego podstawowych cech[10].

Analizy ryzyka

W 2 kontrolowanych jednostkach (15%) nie przeprowadzano (udokumentowanych) okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, o których stanowi § 20 ust. 2 pkt 3 rozporządzenia KRI. **Z kolei w 5 urzędach (39%) analizy ryzyka wymagały dopracowania.** Ważną, identyfikowaną w tym zakresie nieprawidłowością było również zawężanie analizy ryzyka tylko do ochrony danych osobowych.

Szkolenia osób zaangażowanych w proces przetwarzania informacji

Kontrole w 6 jednostkach (46%) wykazały niezapewnienie wystarczających szkoleń osób zaangażowanych w proces przetwarzania informacji, o których stanowi § 20 ust. 2 pkt 6 lit. a-c rozporządzenia KRI. Najczęstsze uwagi dotyczyły braku pełnej realizacji zakresu ww. przepisu (niepełny zakres szkoleń)[11], lub ograniczenia szkoleń wyłącznie do ochrony danych osobowych.

Uprawnienia osób zaangażowanych w proces przetwarzania informacji

W 6 kontrolowanych urzędach (46%) stwierdzono przypadki nadmiarowych uprawnień użytkowników komputerów wykorzystywanych do obsługi sprawdzanych systemów teleinformatycznych, co jest niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. Stwierdzone nieprawidłowości dotyczyły pracy ww. użytkowników na koncie z uprawnieniami administratora systemu operacyjnego komputera, zamiast na koncie z uprawnieniami użytkownika standardowego.

[10] Audyt nie może być wykonywany przez osobę odpowiedzialną za działania będące przedmiotem audytu. Por.: norma PN-EN ISO 19011 (Wytyczne dotyczące auditowania systemów zarządzania), pkt 3.1. Zob. także: norma PN-ISO/IEC 27000 (Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia), pkt 2.5.

[11] Przepis § 20 ust. 2 pkt 6 lit. a-c rozporządzenia KRI, stanowi o zapewnieniu szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Kopie zapasowe

W 4 urzędach (31%) stwierdzono nieprawidłowości dotyczące kopii zapasowych danych z kontrolowanych systemów teleinformatycznych. Polegały one przede wszystkim na braku testowania jakości wykonania kopii. Było to niezgodne z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Podkreślić należy, że dla minimalizowania ryzyka utraty informacji w wyniku awarii systemu teleinformatycznego, ważne jest nie tylko regularne wykonywanie (tworzenie) kopii zapasowej i jej odpowiednie przechowywanie (tzn. w innej lokalizacji niż miejsce pracy systemu), ale także regularne testowanie jakości jej wykonania.

Systemem operacyjny komputera

W 2 jednostkach (15%) – do obsługi kontrolowanych systemów teleinformatycznych – wykorzystywano komputery z zainstalowanym systemem operacyjnym nie posiadającym już wsparcia producenta. Było to niezgodne z § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI, w myśl którego należy zapewnić odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych w szczególności poprzez dbałość o aktualizację oprogramowania i redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych.

Logowanie

W 1 urzędzie (8%) ujawniono stosowanie przez pracowników (użytkowników) tego samego loginu i hasła przy logowaniu się do systemu operacyjnego komputera, co naruszało przede wszystkim § 20 ust. 1 rozporządzenia KRI (w zakresie dotyczącym konieczności zapewnienia poufności z uwzględnieniem rozliczalności) oraz § 20 ust. 2 pkt 4, 7 i 9 rozporządzenia KRI.

Przyczyną stwierdzonych nieprawidłowości był przede wszystkim niewystarczający nadzór nad obszarem poddanym kontroli, sprawowany przez kierownictwo jednostek kontrolowanych.

Stwierdzone nieprawidłowości skutkowały przede wszystkim obniżeniem poziomu bezpieczeństwa informacji przetwarzanych w tych jednostkach.

IV. WNIOSKI

W celu zapewnienia właściwego działania systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej – a zarazem odpowiedniego poziomu bezpieczeństwa informacji – w urzędach jednostek samorządu terytorialnego w województwie opolskim, Wojewoda Opolski wnioskuje o:

1) Dokonywanie przeglądów i aktualizacji regulacji wewnętrznych dotyczących bezpieczeństwa informacji, pod kątem realizacji wszystkich wymogów określonych w rozporządzeniu KRI (ze szczególnym uwzględnieniem w nich także obowiązków wynikających – dla jednostki samorządu terytorialnego – z ustawy o krajowym systemie cyberbezpieczeństwa), celem zapewnienia kompleksowego funkcjonowania SZBI;

2) Eliminowanie zagrożeń związanych z usytuowaniem, niedostatecznym wyposażeniem i zabezpieczeniem pomieszczenia serwerowni oraz z jego wykorzystywaniem do celów niezwiązanych z przeznaczeniem;

3) Wprowadzanie w zawieranych umowach serwisowych dotyczących systemów teleinformatycznych, stosownych mechanizmów zapewniających szybkie usunięcie sytuacji nieprawidłowych /awarii, błędów, usterek/ w systemie (tzn. maksymalny /optymalny/ termin na ich usunięcie oraz kary umowne w odpowiedniej wysokości za przekroczenie takiego terminu), celem zapewnienia dostępności informacji, o której stanowi § 20 ust. 1 rozporządzenia KRI;

4) Przestrzeganie obowiązków wynikających dla jednostki samorządu terytorialnego z ustawy o krajowym systemie cyberbezpieczeństwa;

5) Przeprowadzanie – nie rzadziej niż raz na rok – (niezależnego) audytu wewnętrznego w zakresie bezpieczeństwa informacji, stosownie do § 20 ust. 2 pkt 14 rozporządzenia KRI;

6) Przeprowadzanie i rzetelne dokumentowanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI;

7) Przeprowadzanie regularnych szkoleń wszystkich osób (pracowników urzędu) zaangażowanych w proces przetwarzania informacji, wyczerpujących dyspozycję § 20 ust. 2 pkt 6 lit. a-c rozporządzenia KRI;

8) Przyznawanie pracownikom urzędu uprawnień w systemie operacyjnym komputera, w stopniu adekwatnym do realizowanych przez nich zadań, w myśl § 20 ust. 2 pkt 4 rozporządzenia KRI;

9) Regularne wykonywanie (tworzenie) kopii zapasowej (całego środowiska pracy danego systemu), jej odpowiednie przechowywanie (tzn. w innej lokalizacji niż miejsce pracy systemu) oraz regularne testowanie jakości jej wykonania, w celu zminimalizowania ryzyka utraty informacji w wyniku awarii, stosownie do § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI;

10) Zapewnienie funkcjonowania na komputerach wyłącznie systemów operacyjnych, posiadających wsparcie ich producenta, zgodnie z § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI;

11) Bezwzględne eliminowanie (ewentualnych) praktyk stosowania przez pracowników urzędu (użytkowników) tego samego loginu i hasła przy logowaniu się do systemu operacyjnego komputera.

Ponadto Wojewoda Opolski wnioskuje o wzmocnienie nadzoru – we wszystkich urzędach jednostek samorządu terytorialnego w województwie opolskim – nad funkcjonowaniem obszaru będącego przedmiotem niniejszej *Informacji o wynikach kontroli*.

Opracowanie Informacji:
Radosław Chodziński
Starszy Inspektor Wojewódzki
w Oddziale Organizacji, Kontroli i Skarg
w Wydziale Prawnym i Nadzoru OUW

Konsultacje merytoryczne:
Adam Szkudklarski
Główny Specjalista
w Oddziale Informatyki i Rozwoju
w Biurze Obsługi Urzędu OUW

Akceptacja:
Katarzyna Piasecka
Kierownik Oddziału Organizacji, Kontroli i Skarg
w Wydziale Prawnym i Nadzoru OUW

Akceptacja:
Izabela Bryja
Dyrektor Generalny OUW