NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.003.02.2020

Pan
Marcin Walentynowicz
Dyrektor Centralnego Ośrodka Informatyki
Aleje Jerozolimskie 132-136
02-305 Warszawa

WYSTĄPIENIE POKONTROLNE

P/20/004 – Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, F +48 22 444 52 52
kap@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne

Jednostka kontrolowana	Centralny Ośrodek Informatyki (dalej: COI) Aleje Jerozolimskie 132-136, 02-305 Warszawa
Kierownik jednostki kontrolowanej	Marcin Walentynowicz, Dyrektor Centralnego Ośrodka Informatyki (dalej: Dyrektor COI) w okresie 1 luty 2018 r. – obecnie. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Marcin Suchar, Dyrektor Centralnego Ośrodka Informatyki w okresie 23 czerwca 2017 r. – 31 stycznia 2018 r. Monika Jakubiak, Dyrektor Centralnego Ośrodka Informatyki w okresie 1 września 2016 r. - 23 czerwca 2017 r. Rafał Leśkiewicz, Dyrektor Centralnego Ośrodka Informatyki w okresie 1 czerwca 2016 r. – 31 sierpnia 2016 r. Adam Sobczak, Dyrektor Centralnego Ośrodka Informatyki w okresie 27 stycznia 2016 r. – 31 maja 2016 r. Nikodem Bończa-Tomaszewski, Dyrektor Centralnego Ośrodka Informatyki w okresie 19 kwietnia 2012 r. - 26 stycznia 2016 r.
Zakres przedmiotowy kontroli	Zapewnienie przez COI funkcjonowania platformy ePUAP[1] oraz Profilu Zaufanego (dalej: PZ).
Okres objęty kontrolą	Od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych, tj. do 30 września 2020 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontrolerzy	1. Piotr Bielecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/45/2020 z 5 czerwca 2020 r. 2. Mariusz Czarnecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/39/2020 z 4 czerwca 2020 r. (akta kontroli str. 1-2)

[1] Elektroniczna Platforma Usług Administracji Publicznej.
[2] Dz. U. z 2020 r. poz. 1200, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W okresie poddanym kontroli COI na zlecenie Ministerstwa Cyfryzacji (dalej: MC) zapewnił utrzymanie i rozwój systemów ePUAP oraz PZ zgodnie z umowami z MC, jednak w realizacji tego zadania stwierdzono kilka nieprawidłowości.

Dla zapewnienia dostępności systemu na określonym poziomie COI zawarł umowy z usługodawcami zewnętrznymi i monitorował ich wykonanie. W razie niezapewnienia dostępności usług zewnętrznych na określonym poziomie COI naliczał kary umowne.

Dostępność systemów ePUAP i PZ utrzymywała się powyżej minimalnych progów określonych w umowach, tj. 98% dla ePUAP oraz 99% dla PZ i według raportów utrzymania przekazywanych w tym okresie przez COI do MC wynosiła 100%. Ustalono jednak, że zasady obliczania dostępności tych systemów określone w umowach na utrzymanie były nierzetelne, ponieważ przyjęto założenie, że dostępność tą zmniejszają jedynie wąsko rozumiane incydenty krytyczne, które powodują niedostępność głównych funkcji systemu, natomiast incydenty o niższym priorytecie, które utrudniają lub uniemożliwiają korzystanie z systemów przez poszczególnych użytkowników, nie miały wpływu na obniżenie raportowanego poziomu dostępności.

COI skutecznie monitorował działanie systemów ePUAP i PZ reagując na pojawiające się awarie. Wsparcie techniczne dla użytkowników tych systemów zostało zorganizowane zgodnie ze współczesną praktyką w tym zakresie. Zaległości w obsłudze zgłoszeń wpływających od użytkowników tych systemów narastały w I połowie 2020 r., co spowodowane było zwiększonym wykorzystaniem tych platform przez obywateli i urzędy w związku ze stanem epidemii COVID-19. W COI podjęto odpowiednie działania zmierzające do poprawy tej sytuacji.

COI na zlecenie Ministerstwa Cyfryzacji rozwijał systemy ePUAP i PZ i podjął w tym zakresie współpracę z interesariuszami tych systemów. Realizowany przez COI proces zarządzania zmianami, od strony proceduralno-zarządczej był zorganizowany prawidłowo w sposób typowy dla tego rodzaju procesów.

W COI podjęto działania w celu wdrożenia wymagań międzynarodowej normy z zakresu bezpieczeństwa informacji ISO/IEC 27001. Ponadto, COI wdrożył procedury i zapewnił możliwość odtworzenia systemu w przypadku wystąpienia katastrofy.

Stwierdzone nieprawidłowości polegały m.in. na:

1. Określeniu w umowach na utrzymanie systemów ePUAP oraz PZ nierzetelnego mechanizmu pomiaru jakości obsługi zgłoszeń problemów przez użytkowników, który nie uwzględniał wielkości przekroczenia wymaganego czasu obsługi, a jedynie sam fakt przekroczenia, w efekcie w marcu 2020 r. odpowiednio 76% incydentów dotyczących PZ i 63% incydentów dotyczących ePUAP nie zostało nawet otwartych, a zaraportowana do MC skuteczność obsługi zgłoszeń dla systemu ePUAP wynosiła 93,6%, natomiast dla systemu PZ 96,2%.
2. Określeniu w umowach na utrzymanie systemów ePUAP i PZ zbyt długich maksymalnych czasów obsługi poszczególnych kategorii incydentów, co może utrudnić korzystanie z tych systemów przez obywateli i urzędy.
3. Niepełnym wdrożeniu (do dnia zakończenia czynności kontrolnych) Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), co było niezgodne z § 20 ust. 1 i 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r.

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

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4] (dalej: rozporządzenie KRI).

4. Przeprowadzeniu przez COI niekompletnych testów bezpieczeństwa systemów ePUAP i PZ, co w ocenie NIK było działaniem nierzetelnym.

III. Opis ustalonego stanu faktycznego

1. Wprowadzenie

Opis stanu faktycznego

COI jest instytucją gospodarki budżetowej, nad którą nadzór w okresie objętym kontrolą sprawował Minister Cyfryzacji. Zgodnie ze statutem COI przedmiotem jego podstawowej działalności jest m.in. odpłatne wykonywanie na rzecz Ministra usług w zakresie utrzymania i rozwoju systemu ePUAP, a także w zakresie obsługi PZ[5].

System ePUAP umożliwia podmiotom publicznym udostępnianie obywatelom e-usług na ogólnopolskiej platformie teleinformatycznej. Dostęp do ePUAP oraz e-usług możliwy jest m.in. z wykorzystaniem PZ, który zapewnia identyfikację elektroniczną użytkownika.

Na podstawie umowy nr 2/U/COI/MC/2016 zawartej 30 marca 2016 r. pomiędzy Ministrem Cyfryzacji oraz Centralnym Ośrodkiem Informatyki, COI jest odpowiedzialny za utrzymanie systemu ePUAP. W dniu 4 kwietnia 2019 r. MC zawarło z COI Aneks nr 4 do ww. umowy, zgodnie z którym okres jej obowiązywania został przedłużony do 4 kwietnia 2022 r. Na podstawie umowy zawartej 29 grudnia 2017 r. pomiędzy Ministrem Cyfryzacji oraz Centralnym Ośrodkiem Informatyki, COI do 30 grudnia 2020 r. jest odpowiedzialny za utrzymanie systemu PZ. W ww. umowach przewidziano także możliwość rozwoju tych systemów przez COI.

(akta kontroli str. płyta DVD 1 poz. 100-151, 476-480, 573-575)

2. Serwis internetowy epuap.gov.pl

Na stronie www.epuap.gov.pl udostępniono dwie podstawowe metody wyszukiwania usługodawców (urzędów) i spraw przez nich świadczonych (e-usług). Zgodnie z instrukcją pn. *ePUAP Jak załatwić sprawę?*[6], pierwsza metoda polega na wyszukiwaniu spraw za pomocą wyszukiwarki zamieszczonej na stronie głównej ePUAP. Według drugiej metody wyszukiwanie urzędów możliwe jest z pomocą wyszukiwarki zamieszczonej w zakładce *Katalog spraw*, w której po odnalezieniu podmiotu właściwego miejscowo i rzeczowo oraz wyborze zakładki *Pokaż sprawy wybranego urzędu,* prezentowane są w sposób hierarchiczny najważniejsze kategorie i podkategorie zdarzeń, do których przyporządkowane zostały nazwy spraw, jakie użytkownik może zrealizować w wybranym przez siebie podmiocie. Inny sposób wyszukiwania urzędów, funkcjonujący w ramach drugiej metody wyszukiwania za pomocą zakładki *Katalog spraw* polega na wyborze opcji: *Inny podział spraw -> Klasyfikacja terytorialna* (dostępne inne opcje: *Alfabetyczna lista spraw oraz Inne klasyfikacje*), której wybór prezentuje usługi dostępne wyłącznie na terenie wybranej jednostki terytorialnej np. konkretnej gminy na terenie Rzeczypospolitej Polskiej. Wybranie jednej z usług świadczonych przez jednostki

---

4 Dz. U. z 2017 r. poz. 2247.

5 Zgodnie z §2 ust. 2 pkt 5 lit. b) oraz §2 ust. 2 pkt 7 statutu COI wprowadzonego zarządzeniem nr 6 Ministra Cyfryzacji z dnia 31 grudnia 2015 r. w sprawie nadania statutu instytucji gospodarki budżetowej pod nazwą *Centralny Ośrodek Informatyki* (Dz. Urz. Ministra Cyfryzacji z 2015 r. poz. 7, ze zm.).

6 Dostępnej na stronie www.epuap.gov.pl w zakładce POMOC -> Załatwianie sprawy.

samorządu terytorialnego pozwala wyszukać urząd i sprawdzić, czy dana usługa jest przez niego realizowana.

W celu weryfikacji działania drugiej metody wyszukiwania spraw wg wybranego urzędu, poddano analizie według ww. instrukcji e-usługi udostępnione na stronie internetowej www.epuap.gov.pl przez 10 urzędów administracji publicznej[7]. Ustalono, że dla każdego z wybranych urzędów katalogi zawierały zarówno usługi świadczone przez te podmioty oraz inne usługi, które nie mogły być do tych urzędów przypisane, a adresatami tych usług były inne podmioty (np. ministerstwa). Szczegółowe sprawdzenie możliwości załatwienia dwóch spraw[8] w sposób elektroniczny za pośrednictwem platformy ePUAP przypisanych do Urzędu Miejskiego w Sochaczewie wykazało, iż przypadku pierwszej sprawy wystąpił błąd formularza uniemożliwiający złożenie pisma, którego adresatem w rzeczywistości było Ministerstwo Cyfryzacji (dalej: MC), a w przypadku drugiej sprawy wprawdzie była możliwość załatwienia sprawy w sposób elektroniczny, ale przez przekazanie informacji do nieistniejącego od ponad czterech i pół roku podmiotu tj. Ministerstwa Spraw Wewnętrznych[9]. Na podstawie analizy listy usług świadczonych przez UM w Sochaczewie na platformie ePUAP ustalono, że nie zostały opublikowane informacje dla części usług w zakresie nazwy organu właściwego do realizacji usługi, tj. wpisana jest informacja *Brak*[10], zostały opublikowane informacje dotyczące nieistniejącego Ministerstwa Spraw Wewnętrznych[11] i Ministra Finansów, Inwestycji i Rozwoju[12] oraz wielokrotnie przy opisie usług występuje różne nazewnictwo organu właściwego do realizacji usługi przez jednostki samorządu terytorialnego, np. *Organ gminy*, w innym przypadku *Organ gminy (wójt, burmistrz, prezydent miasta)* lub *wójt, burmistrz, prezydent miasta*.

(akta kontroli str. 85-109)

Dyrektorzy Pionu Operacji oraz Pionu Rozwoju COI wyjaśnili m.in., że zgodnie z art. 19d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[13], *podmioty udostępniające usługi na ePUAP zapewniają ich zgodność z przepisami stanowiącymi podstawę sporządzenia wzoru dokumentu elektronicznego oraz dokonują aktualizacji tych usług w katalogu usług. Oznacza to, że za informacje zawarte w usłudze oraz ich aktualność i zgodność z przepisami odpowiadają poszczególne podmioty udostępniające usługi. Jeżeli urząd opublikuje np. nieaktualne dane o swoim urzędzie, np. wpisał nazwę urzędu, takie dane będą również wyświetlały się w katalogu usług na ePUAP. W zakresie błędu, który wystąpił w tracie wywołania usługi (…) system ePUAP działał w tym zakresie prawidłowo. Przedmiotowy błąd dotyczył wyłącznie usługi, która została opublikowana w katalogu usług, za której działanie odpowiada podmiot ją umieszczający (…).*

---

7 Na podstawie sprawdzenia kategorii zdarzeń oraz usług świadczonych dla danej kategorii dla Urzędu Miasta (dalej: UM) w Sochaczewie, UM w Piastowie, UM w Hajnówce, UM w Augustowie, UM w Knurowie, UM w Wolsztynie, UM w Oławie, UM w Zgorzelcu, UM w Policach oraz Gminie Knurów i Gminie Koluszki.

8 Pierwszej pn. Przekazanie informacji o udostępnionym przez podmiot publiczny adresie Elektronicznej Skrzynki Podawczej należącej do kategorii Udostępnianie usług -> Udostępnianie przez podmiot publiczny adresu Elektronicznej Skrzynki Podawczej oraz drugiej pn. Udostępnianie danych z rejestru PESEL i rejestru mieszkańców za pomocą urządzeń teletransmisji danych należącej do kategorii Sprawy obywatelskie -> Ogólne sprawy urzędowe.

9 Istniało do dnia 15 listopada 2015 r. Na podstawie rozporządzenia Rady Ministrów z dnia 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji (Dz. U. z 2015 r. poz. 1946), od 16 listopada 2015 r. MSW zostało przekształcone w Ministerstwo Spraw Wewnętrznych i Administracji.

10 Np. usługa Sporządzenie aktu zgonu należąca do kategorii Sprawy obywatelskie ->Zgłaszanie zmian w aktach stanu cywilnego.

11 Np. usługa Udostępnianie danych z Rejestru Dowodów Osobistych w trybie ograniczonej teletransmisji danych należąca do kategorii Sprawy obywatelskie -> Ogólne sprawy urzędowe.

12 Np. usługa Informacja o prognozowanych przychodach firmy audytorskiej dla Komisji Nadzoru Audytowego (KNA-INF) należąca do kategorii Najnowsze usługi -> Najnowsze usługi centralne.

13 Dz.U. z 2020 r. poz. 346 ze zm.

Dyrektor Departamentu Produkcji Oprogramowania COI wyjaśnił, iż weryfikacja listy e-usług świadczonych przez Urzędy nie jest przedmiotem umowy pomiędzy COI, a MC, natomiast COI *mając na uwadze prawidłowe funkcjonowanie systemu realizuje, w ramach wsparcia MC, zadania polegające na manualnej weryfikacji opisów każdej z usług zgłoszonych przez podmioty realizujące zadania publiczne (Urzędy) przed ich publikacją. Weryfikacji podlega kompletność opisu usługi w poszczególnych polach formularza. W przypadku stwierdzenia błędów usługa jest odrzucana przez Centralny Ośrodek Informatyki z powiadomieniem wnioskującego o przyczynie odrzucenia. Następnie proces publikacji opisu usługi rozpoczyna się od początku.*

NIK zauważa, że wprawdzie COI przejął od Centrum Cyfrowej Administracji w 2016 r. do eksploatacji funkcjonujący już system, jednak jako podmiot utrzymujący system powinien informować właściciela systemu (MC) o konieczności dokonania zmian w ramach prac rozwojowych, pozwalających na wyeliminowanie ww. problemów. Zdaniem NIK, COI we współpracy z właścicielem systemu powinien dokonać modyfikacji zastosowanego mechanizmu filtrowania (wyszukiwania) poprzez jego rozbudowanie o możliwość wyboru przez użytkownika usług lokalnych lub centralnych, które mogą być załatwione przez dany podmiot, ujednolicić nazewnictwo adresatów usług za pomocą słowników lub powiązać je ze źródłami danych zewnętrznych, a także wdrożyć rozwiązania nadzorcze w celu niezwłocznego aktualizowania udostępnionych usług przez ich właścicieli. Takie działanie ma na celu zapewnienie prawidłowości wyświetlanych informacji.

(akta kontroli str. 110-131, płyta DVD1 poz. 770, 873, 1030)

3. Zapewnienie sprawnego działania ePUAP oraz PZ

W umowach na utrzymanie systemów ePUAP i PZ dostępność SLA[14] określono na poziomie 98% w odniesieniu do systemu ePUAP oraz 99% w odniesieniu do systemu PZ. Przyjęcie takich wartości powoduje możliwość zaistnienia całkowitej niedostępności każdej z usług przez 7,3 dnia w ciągu roku dla systemu ePUAP oraz przez 3,6 dnia dla systemu PZ.

Zdaniem NIK, systemy ePUAP i PZ, z uwagi na istotne znaczenie dla obywateli i dla funkcjonowania administracji publicznej, powinny mieć gwarantowaną w umowach dostępność o wartości zbliżonej do bankowych systemów informatycznych, tj. 99,9%.

Zgodnie z zawartymi umowami na utrzymanie systemów ePUAP i PZ, COI był zobowiązany do przekazywania MC miesięcznych raportów dotyczących poziomu świadczonych usług utrzymania. Według raportów za okres lipiec 2019 r. – czerwiec 2020 r. dostępność systemów ePUAP oraz PZ w każdym miesiącu tego okresu wynosiła 100%. Dostępność ta była wyznaczana jako iloraz sumy czasów trwania incydentów krytycznych w miesiącu do łącznego czasu wymaganej dostępności systemu w tym czasie.

Analizie poddano zarejestrowane przez COI incydenty krytyczne i pilne od lipca 2019 r. do czerwca 2020 r. oraz incydenty standardowe, które wystąpiły w dniu 22 stycznia 2020 r., kiedy to nastąpiła awaria serwera baz danych w jednym z ośrodków przetwarzania. Ustalono, że w badanym okresie incydentów krytycznych w ogóle w COI nie zarejestrowano (ostatni taki incydent miał miejsce 14 czerwca 2018 r.). W listopadzie i grudniu 2019 r. wystąpiły natomiast dwa incydenty pilne

[14] SLA - umowa o poziomie świadczenia usług informatycznych i ich parametrach (ang. Service Level Agreement).

dotyczące awarii bramek SMS obsługujących system ePUAP[15]. Dla systemu PZ incydentów o priorytecie innym niż standardowy nie odnotowano w COI. Według wyjaśnień Dyrektora Pionu Operacji COI pomimo awarii serwera w dniu 22 stycznia 2020 r. system ePUAP był dostępny, natomiast część użytkowników postrzegała go jako niedostępny.

W opinii NIK incydent sklasyfikowany jako mniej istotny – standardowy lub pilny – może uniemożliwić sprawne korzystanie z systemu przez użytkowników, natomiast zgodnie z umowami utrzymania nie będzie on wpływał na raportowaną dostępność systemów.

Ustalono, że określony w umowach na utrzymanie systemów ePUAP i PZ i stosowany w przekazywanych przez COI do MC raportach sposób obliczania dostępności tych systemów nie uwzględnia ich rzeczywistej dostępności, która dla użytkowników jest niższa niż raportowana dostępność na poziomie 100%. Kontrola wykazała, że zgodnie z umowami na utrzymanie systemów raportowany czas ich dostępności może zmniejszyć jedynie zaistnienie incydentu krytycznego. Przyjęcie w umowach wąskiej definicji incydentu krytycznego powoduje, że awaria uzasadniająca sklasyfikowanie go jako krytyczny (a co za tym idzie obniżenie raportowanego SLA) jest trudna do zaistnienia. Dalszy opis w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 375-465, płyta DVD1 poz. 212-320, 374-377, 476-480, 573-575, 1194-1204)

Sprawne działanie i dostępność systemów ePUAP i PZ na poziomie ustalonym w umowach utrzymaniowych zależy w dużej mierze od jakości 11 usług i dostaw świadczonych na rzecz COI przez usługodawców zewnętrznych, które obejmowały dostawę licencji w zakresie oprogramowania, dostawę sprzętu, a także świadczenie usług dostępu do Internetu, wysyłania krótkich wiadomości tekstowych oraz usług serwisu, wsparcia technicznego sprzętu i oprogramowania. W umowach dotyczących świadczenia usług telekomunikacyjnych określono zarówno maksymalne czasy usunięcia awarii, jak i wymagany poziom dostępności danej usługi, przy czym dostępność tą określono na poziomie 99,5%. W pozostałych umowach z usługodawcami zewnętrznymi określono czas na usunięcie awarii, natomiast nie uregulowano poziomu dostępności.

Umowy, w których określono wymaganą dostępność usług zewnętrznych zawierają zobowiązanie usługodawcy do przekazywania COI miesięcznych raportów o poziomie ich świadczenia. Raporty te były przekazywane do COI przez podmioty dostarczające usługi na rzecz ePUAP oraz PZ. Zawierały one informacje o dokonanych przez COI zgłoszeniach a także osiągniętych w danym miesiącu poziomach dostępności. Ich analizą i rozliczaniem zajmował się Zespół Zarządzania Poziomem Usług w COI. Incydenty, czy awarie dotyczące korzystania z usług dostawców zewnętrznych były rejestrowane w systemie ITSM i zgłaszane usługodawcom, a po ich rozwiązaniu rejestrowany był moment zamknięcia.

Analizie poddano sprawność działania usług świadczonych przez podmioty zewnętrzne w okresie od lipca 2019 r. do czerwca 2020 r. Ustalono, że istotne awarie dotyczyły jedynie usługi wysyłania powiadomień SMS, które w tym okresie miały miejsce jedenastokrotnie, w tym trzykrotnie doprowadziły do przekroczenia określonych w umowach parametrów dostępności SLA. W takim przypadku COI każdorazowo naliczał usługodawcy kary umowne.

(akta kontroli str. 375-465, płyta DVD1 poz. 152-194, 321-358, 1089-1192)

[15] Awaria bramek SMS powoduje brak możliwości dokonania autoryzacji czynności użytkownika.

NIK zauważa, że przyjęty poziom dostępności usług telekomunikacyjnych odbiega od poziomów rynkowych dla branży telekomunikacyjnej, które zazwyczaj wynoszą 99,9%. Ponadto, dla zapewnienia sprawnego działania systemów ePUAP oraz PZ należy dążyć do umownego uregulowania z wykonawcami, zapewnienia parametrów dostępności świadczonych przez nich usług. Należy podkreślić, iż pomimo dotychczasowego sprawnego działania tych usług może zaistnieć sytuacja, w której wprawdzie awarie będą usuwane terminowo, jednak dostępność usług zewnętrznych spadnie poniżej oczekiwanego przez użytkowników poziomu umożliwiającego zapewnienie sprawnego działania ePUAP i PZ.

Infrastruktura teleinformatyczna, w oparciu o którą funkcjonują systemy ePUAP i PZ, znajdowała się w podstawowym i zapasowym ośrodku przetwarzania danych. Serwerownie te są własnością Skarbu Państwa i na podstawie porozumienia pomiędzy Komendantem Głównym Policji i Ministrem Spraw Wewnętrznych z 5 lutego 2014 r. zostały oddane w użyczenie Ministerstwu Spraw Wewnętrznych. Na podstawie umowy użyczenia z 22 lutego 2018 r. pomiędzy Ministerstwem Spraw Wewnętrznych i Administracji, a Ministerstwem Cyfryzacji serwerownie te zostały oddane MC w nieodpłatne używanie na czas nieoznaczony. Umowa ta nie zawierała postanowień dotyczących wymaganego poziomu usług w zakresie zasilania, chłodzenia czy ochrony serwerowni przez użyczającego.

Zdaniem NIK, brak określenia takich parametrów może negatywnie wpływać na zapewnienie sprawnego działania systemów ePUAP i PZ. Należy jednak mieć na względzie, że COI nie było stroną ww. umowy użyczenia i tym samym odpowiada jedynie za infrastrukturę teleinformatyczną znajdującą się w serwerowni oraz za prawidłowe działanie systemów ePUAP i PZ. COI powinno jednak dążyć do umownego określenia parametrów, co pozwoli na zapewnienie dostępności tych systemów na najwyższym możliwym poziomie.

Ustalono, że podstawowa serwerownia systemów ePUAP i PZ posiada wszystkie typowe zabezpieczenia fizyczne i lokalowe, stosowane w tego typu obiektach. Zainstalowano m.in. system kontroli dostępu i włamania, system przeciwpożarowy, system kontroli parametrów środowiskowych serwerowni (wilgotności, temperatury) oraz system monitoringu. W pomieszczeniu tym zainstalowany jest wyłącznie sprzęt teleinformatyczny (szafy, serwery, podłoga techniczna z osprzętem) i nie przebywają tam na stałe pracownicy. Serwerownia ta wyposażona jest w system baterii UPS i agregaty prądotwórcze w celu podtrzymania dostaw energii elektrycznej dla infrastruktury.

(akta kontroli str. 375-471)

4. Wsparcie techniczne dla użytkowników ePUAP i PZ

Wsparcie techniczne dla użytkowników systemów ePUAP i PZ zostało zorganizowane przez COI w ramach tzw. trzech linii wsparcia. Pierwszą linię stanowili pracownicy Zespołu Service Desk Departamentu Eksploatacji Systemów (dalej: DES), do których zadań należała rejestracja i obsługa zgłoszeń napływających od użytkowników, a w razie braku możliwości rozwiązania problemu jego przekazanie do kolejnych linii wsparcia.

Drugą linię wsparcia stanowili pracownicy Zespołu Administrowania Systemami oraz Zespołu Infrastruktury działający w ramach DES oraz Zespołu Bezpieczeństwa Teleinformatycznego z Departamentu Teleinformatycznego i Zespołu Zarządzania Wydaniem i Konfiguracją z Departamentu Standardów i Procedur.

Jeżeli rozwiązanie problemu wymagało dokonania zmian w oprogramowaniu systemów zgłoszenie było przekazywane do trzeciej linii wsparcia, która była obsługiwana przez programistów, testerów i ekspertów Zespołu Rozwoju Usług

Cyfrowych oraz Zespołu Integracji i Testów, funkcjonujących w ramach Departamentu Usług Cyfrowych.

Użytkownicy systemów ePUAP i PZ mogli zgłaszać problemy i pytania poprzez pocztę elektroniczną, formularz kontaktowy na stronie internetowej, a także telefonicznie. Zgodnie z umowami utrzymaniowymi ePUAP i PZ zgłoszenia telefoniczne były przyjmowane od użytkowników w dni robocze w godzinach 8.00-17.00. Zgłoszenia były rozwiązywane przez pierwszą linię wsparcia w godzinach 8.00-16.00. Poza tymi godzinami działanie systemu było na bieżąco, całodobowo monitorowane przez Sekcję COI-Houston działającą w DES.

Potwierdzenie zakończenia obsługi zgłoszenia było realizowane za pomocą poczty elektronicznej. Ocena satysfakcji zgłaszającego ze sposobu rozwiązania problemu, może być dokonana za pomocą tych samych kanałów komunikacji: telefonicznie, mailowo lub poprzez formularz zgłoszeniowy, gdzie jedną z kategorii zgłoszenia jest opinia.

(akta kontroli str. 132-151, 203-240, 375-465, płyta DVD1 poz. 476-480, 573-575,1215)

Na podstawie umów utrzymaniowych, COI sporządzał i przekazywał do MC miesięczne raporty dotyczące utrzymania systemów ePUAP i PZ, które zawierały m.in. informacje na temat liczby wszystkich incydentów (w tym z przekroczonym terminem obsługi), a także wykaz wszystkich zgłoszeń. Ustalono, że na skutek przyjęcia w ww. umowach niewłaściwego mechanizmu pomiaru jakości obsługi zgłoszeń, dane w tym zakresie prezentowane w raportach z utrzymania systemu nie odzwierciedlały rzeczywistości. Na potrzeby wyliczenia liczby zgłoszeń obsłużonych w danym miesiącu w terminie, COI przyjmowało jedynie zgłoszenia zakończone w danym miesiącu, przy czym nie uwzględniano wielkości przekroczenia wymaganego czasu obsługi, a jedynie sam fakt przekroczenia. Dalszy opis w sekcji *Stwierdzone nieprawidłowości*.

Kontrola wykazała, że w I połowie 2020 r. nastąpił gwałtowny wzrost liczby zgłoszeń dla obu systemów, który spowodował, że w każdym miesiącu pozostawały znaczne ilości zgłoszeń nieobsłużonych[16]. I tak, w okresie tym, w odniesieniu do systemu ePUAP, średnia liczba zgłoszeń nieobsłużonych w miesiącu wyniosła 8406[17], natomiast w odniesieniu do systemu PZ - 6895[18]. Stanowi to wzrost średniomiesięcznej liczby nieobsłużonych zgłoszeń w stosunku do drugiej połowy 2019 r. odpowiednio o 557,5% w odniesieniu do systemu ePUAP i 613,6% w odniesieniu do systemu PZ. Dyrektor Pionu Operacji COI wyjaśnił, że stan ten wynikał z rozprzestrzeniania się w pierwszej połowie 2020 r. epidemii COVID-19 i związanym z tym zwiększonym zainteresowaniem obywateli e-usługami oraz zobowiązaniem COI do zaangażowania pracowników na rzecz podmiotów zewnętrznych (np. Głównego Inspektora Sanitarnego, Narodowego Funduszu Zdrowia, czy Sejmu RP).

Analiza treści zgłoszeń wykazała ich niewielką powtarzalność. Najczęściej zgłaszane problemy dotyczyły:

---

[16] W okresie lipiec 2019 r. – czerwiec 2020 r. do Zespołu Service Desk wpłynęło 126 007 zgłoszeń dotyczących systemu ePUAP (od 7 091 w listopadzie 2019 r. do 18 216 w kwietniu 2020 r., średnio 10 501 zgłoszeń miesięcznie) oraz 100 120 zgłoszeń dotyczących systemu PZ (od 4 814 w sierpniu 2019 r. do 15 007 w marcu 2020 r., średnio 8 343 zgłoszeń miesięcznie).

[17] 2 034 nieobsłużone zgłoszenia w styczniu, 2 952 w lutym, 9 046 w marcu, 17 027 w kwietniu, 10 200 w maju oraz 9 175 w czerwcu.

[18] 3 601 nieobsłużonych zgłoszeń w styczniu, 4 472 w lutym, 12 526 w marcu, 8 775 w kwietniu, 4780 w maju oraz 7218 w czerwcu.

- problemów z komponentem kryptograficznym PK Singer instalowanego lokalnie na komputerach i obsługiwanego w różnych przeglądarkach internetowych w całym kraju, (listopad 2019 r. - czerwiec 2020 r.),
- problemów z potwierdzeniem tożsamości za pośrednictwem systemu teleinformatycznego jednego z banków (kwiecień – czerwiec 2020 r.),
- błędów w działaniu systemu, które zwykle dotyczą pojedynczych użytkowników (wynikające np. z krótkotrwałego zawieszenia serwera aplikacyjnego)[19],
- problemów z logowaniem, spowodowanych brakiem danych do logowania (identyfikator i hasło).

Pozostałe, zgłoszenia dotyczyły problemów w użytkowaniu systemów, które wynikały zarówno z ich wadliwego działania, jak i z niewiedzy użytkowników.

Poza rejestrowaniem i obsługą zgłoszeń o powtarzalnym charakterze COI podejmował działania zmierzające do ich trwałego wyeliminowania (np. umieszczenie na stronie internetowej COI instrukcji posługiwania się komponentem PK Singer, usuwanie usterek, zgłaszanie niesprawności bramek SMS, czy publikowanie i aktualizowanie listy najczęściej zadawanych pytań).

Według stanu na dzień 17 czerwca 2020 r. nad utrzymaniem systemów ePUAP i PZ pracowało w COI łącznie 112 osób (w tym: 33 osoby w pierwszej linii wsparcia). Porównanie liczby zgłoszeń wpływających i obsłużonych w danym miesiącu, a także dostępnych w COI zasobów kadrowych zaangażowanych w utrzymanie systemów ePUAP i PZ, w szczególności do obsługi zgłoszeń wskazuje, że były one wystarczające do końca 2019 r.

Narastające od początku 2020 r. zaległości w zakresie obsługi napływających zgłoszeń wymagały podjęcia przez COI działań zmierzających do ich likwidacji. Dyrektor COI wyjaśnił, że od 13 marca 2020 r. wszyscy pracownicy Zespołu Service Desk realizowali na rzecz podmiotów zewnętrznych dodatkowe zadania zlecone przez Ministra Cyfryzacji mające na celu minimalizację skutków pandemii COVID-19. Ponadto wyjaśnił, że COI (…) *podjął niezwłoczne działania, których celem było rozładowanie kolejki zgłoszeń i skrócenia czasu ich obsługi. Do Service Desk zostało przesuniętych 70 pracowników z innych zespołów. Jednocześnie uruchomiony został proces rekrutacji.* (…)

(akta kontroli str. 203-240, 375-465, płyta DVD1 poz. 212-320, 374-377, 476-480, 573-575, 718-756, 1194-1204)

Zdaniem NIK, w umowach na utrzymanie systemów ePUAP i PZ ustalono zbyt długie maksymalne czasy obsługi poszczególnych kategorii zgłoszeń, które w konsekwencji mogą utrudnić korzystanie z tych systemów przez obywateli i urzędy. Obsługa incydentów standardowych trwa, zgodnie z umowami, maksymalnie 20 dni, natomiast pilnych 10 dni w odniesieniu do obu systemów. Do dnia 4 kwietnia 2019 r. incydenty krytyczne dotyczące systemu ePUAP zgodnie z umową powinny być obsługiwane w terminie trzech dni. Dalszy opis w sekcji *Stwierdzone nieprawidłowości*. Na skutek zawarcia aneksu nr 4 do umowy utrzymania systemu ePUAP czas obsługi incydentu krytycznego skrócono do jednego dnia. Obsługa incydentów krytycznych dotyczących systemu PZ przez cały okres jego utrzymania przez COI, powinna trwać maksymalnie 11 godzin.

W COI nie sporządzono procedury reagowania na najczęściej występujące awarie. Funkcjonują w tym zakresie natomiast procedury administrowania systemami, które opisują sposób działania w przypadku zaistnienia problemów lub standardowych

[19] Sygnalizowanych np. jako External server error, Błąd 500.

zdarzeń w działaniu systemów[20]. Procedury te są wykorzystywane przez drugą linię wsparcia.

Na stronach internetowych epuap.gov.pl, pz.gov.pl oraz gov.pl zamieszczono instrukcje korzystania z e-usług, a także listy najczęściej zadawanych pytań z odpowiedziami, które są skierowane do użytkowników systemów ePUAP i PZ.

(akta kontroli str. 375-465, płyta DVD1 poz. 378-400, 476-480, 573-575)

5. Monitorowanie działania systemów

Monitorowaniem działania systemów ePUAP i PZ zajmuje się w COI Zespół COI-Houston funkcjonujący w trybie 24 godziny na dobę, przez siedem dni w tygodniu. Wykorzystuje on w tym celu specjalistyczne narzędzia, takie jak systemy Zabbix, ManageEngine, DynaTrace, Cacti oraz Nagios, które służą do bieżącego monitorowania zajętości infrastruktury systemów ePAUP i PZ. Monitorowaniu tym systemem podlegają parametry obciążenia łącz w centrach danych (zarówno ruchu wchodzącego, jak i wychodzącego), a także użycia procesora, pamięci operacyjnej i dysków do trwałego przechowywania danych dla serwerów aplikacyjnych i bazodanowych. Pomiary parametrów wykonywane są przez ten system punktowo, co 5 minut. Dyrektor Pionu Operacji COI wyjaśnił, że wdrożone zostało również tzw. narzędzie Grafana, do którego zaplanowane jest podłączenie narzędzia do monitorowania ePUAP/PZ. W przypadku wystąpienia awarii zespół COI-Houston podejmował działania mające na celu jej usunięcie.

COI sporządzał i przekazywał do MC miesięczne raporty dotyczące obciążenia infrastruktury. Według raportu za maj 2020 r. stopień wykorzystania przestrzeni dyskowej systemów wynosił 55% w przypadku serwerów aplikacyjnych i 64% w przypadku serwerów bazodanowych.

(akta kontroli str. 375-465, płyta DVD1 poz. 17-24, 708-717, 876-1021, 1059-1060, 1207, 1222)

Zdaniem NIK, takie wartości są typowe dla systemu znajdującego się w fazie produkcyjnej i pozostawiają bezpieczny margines wolnego miejsca, umożliwiający rozszerzenie dostępnych zasobów w razie potrzeby.

6. Rozwój systemów ePUAP i PZ oraz wprowadzanie zmian w oprogramowaniu

Możliwość zmian rozwojowych ePUAP i PZ została przewidziana w umowach utrzymaniowych tych systemów. W ramach określonego w tych umowach budżetu (45 300,0 tys. zł w umowie dotyczącej ePUAP[21] i 6 696,4 tys. zł w umowie dotyczącej PZ[22]) MC mogło udzielać COI zleceń dodatkowych. W okresie obowiązywania tych umów MC udzieliło COI 17 zleceń rozwojowych dotyczących ePUAP oraz 17 zleceń rozwojowych dotyczących PZ. Prace rozwojowe dotyczące systemów były także realizowane w oparciu o umowę dotyczącą budowy Krajowego Węzła Identyfikacji Elektronicznej[23]. W związku z realizacją ww. zleceń

[20] Procedury: Przełączenia Bazy ePUAP, Restartu PK Robota, Restartu serwera APPWEW, Restartu serwera SSF, Restartu Usług Oprogramowania DRACO, Restartu wildfly na serwerach PZ-DT, Weryfikacji Otrzymania Kodu SMS, a także 79 Procedur utrzymaniowych.

[21] Jest to górna granica zobowiązań MC z tytułu realizacji całej umowy, obejmującej również utrzymanie ePUAP, a także SSDIP, Strony Głównej BIP i Publikatora Aktów Prawnych.

[22] Ze środków tych MC mogło zlecać COI również zakup zewnętrznych usług, niezbędnych w procesie utrzymania systemów.

[23] Projekt realizowany przez MC, który ma ułatwić korzystanie z usług elektronicznych poprzez utworzenie jednego uniwersalnego loginu i bezpiecznego zestawu haseł.

rozwojowych, COI poniósł w latach 2017-2020 wydatki głównie na usługi obce[24], w łącznej wysokości:

- 1 805,1 tys. zł w ramach utrzymania ePUAP,
- 1 209,6 tys. zł w ramach prac rozwojowych PZ,
- 14,6 tys. zł w ramach Węzła Krajowego.

Prace rozwojowe systemu ePUAP dotyczyły m.in. wsparcia algorytmu SHA-2, realizacji nowych usług, integracji ePUAP z innymi systemami i rejestrami. Natomiast rozwój PZ dotyczył m.in. prac nad podpisem PZ dla pliku JPK_VAT, stworzenia podpisu eDowodu w systemie PZ oraz automatycznej aktualizacji danych w bazie systemu PZ na podstawie zmian w rejestrze PESEL.

Organizatorem współpracy z kluczowymi interesariuszami[25] w ramach prac nad rozwojem ePUAP oraz PZ w zakresie usług elektronicznych świadczonych za pośrednictwem tych systemów jest MC. COI brał udział w ww. pracach w charakterze wykonawcy oraz doradcy technologicznego MC na podstawie umów zawartych pomiędzy MC i COI. W zakresie zadań realizowanych przez COI w oparciu o ww. umowy dotyczące PZ przedstawiciele interesariuszy brali udział w posiedzeniach Komitetu Sterującego projektu pn. *Budowa Węzła Krajowego*, w pracach merytorycznych, a także w testach integracyjnych. Zadania realizowane przez COI z udziałem interesariuszy w zakresie rozwoju ePUAP dotyczyły głównie zmiany stosowanego w tym systemie algorytmu SHA-1 na SHA-2[26] i polegały na:

- koordynacji akcji kontaktu telefonicznego z wszystkimi potencjalnymi podmiotami na które mogła mieć wpływ zmiana algorytmu SHA-1 na SHA-2 (około 3 tys. interesariuszy),
- prowadzenia warsztatów zorganizowanych przez MC dla dostawców usług i dostawców tożsamości, którzy powinni dostosować własne systemy do algorytmu SHA-2,
- bezpośredniego wsparcia w siedzibie interesariusza (Centrala ZUS) w związku z wdrożeniem nowej aplikacji dla wykonania akcji podpisu kwalifikowanego (PKSigner),
- koordynacji testów integracyjnych wraz z obsługą zgłoszeń interesariuszy dotyczących udziału w testach wraz z wyznaczeniem koordynatorów na wdrożenie produkcyjne.

Interesariuszom na stronie głównej ePUAP[27] udostępniane były bieżące informacje dotyczące ePUAP i PZ, które publikowane są m.in. w sekcji *Aktualności* oraz instrukcje i podręczniki, odpowiedzi na najczęściej zadawane pytania w sekcji *Pomoc* dostępne niezależnie dla obywatela oraz urzędnika.

(akta kontroli str.45-58, 110-131, 193-202, płyta DVD1 poz. 401-681, 769-857, 1030)

Zagadnienia dotyczące dokonywania zmian w wytworzonym oprogramowaniu zostały określone w następujących dokumentach COI:

- *Procedura Zarządzania Wydaniami*, w której uregulowano zarządzanie wydaniami nowych wersji oprogramowania od strony formalnej oraz

[24] Usługi obce w tym Body Leasing, Delegacje pracowników Centralnego Ośrodka Informatyki oraz odsprzedaż sprzętu i licencji. Wydatki nie obejmują kosztów związanych z wynagrodzeniem pracowników COI, pochodnych na ZUS i ZFŚS, kosztów Amortyzacji, oraz kosztów pośrednich w tym m.in. opłat eksploatacyjnych, kosztów lokalizacji, usług pocztowych, użytkowania i eksploatacji części wspólnych itp.

[25] Kluczowi interesariusze w ePUAp i PZ to m.in.: banki jako dostawcy tożsamości, dostawcy usług – podmioty publiczne posiadające uwierzytelnione konto na ePUAP w tym JST, które wykorzystują ePUAP do przygotowywania i udostępniania własnych usług oraz wykorzystują PZ jako środek uwierzytelniający w celu świadczenia usług we własnych systemach, jednostki administracji publicznej korzystające z systemów ePUAP i PZ, które zgłaszają błędy, problemy, wnioski i pytania poprzez Service Desk COI.

[26] Zmiana dotyczyła również systemu PZ.

[27] Pod adresem: www.epuap.gov.pl.

organizacyjnej – w szczególności skład Rady ds. Zmian oraz formę i zawartość Karty Wydania,

– *Procedura Zarządzania Wdrożeniami*, w której zdefiniowano zasady wdrażania zmian o dużym zakresie i uregulowano wytyczne na temat zaplanowania harmonogramu wdrożenia oraz sposobu jego realizacji.

Zgodnie z ww. procedurami, za zarządzanie wydaniami i wdrożeniami odpowiada Rada ds. Zmian, składająca się z Dyrektorów: Pionu Operacji, Pionu Rozwoju, Departamentu Eksploatacji Systemów, Departamentu Cyberbezpieczeństwa, Departamentu Rozwoju Aplikacji oraz Departamentu Usług Cyfrowych. Każda zmiana posiada przypisanego Właściciela Zmiany, tj. osobę inicjującą zmianę, która opracowuje dokument RFC[28]. Dokumentem, który całościowo opisuje dokonaną zmianę jest Karta Wydania. Przed dokonaniem wdrożenia określany jest plan komunikacji z interesariuszami wdrożenia. W przypadku wdrożeń obarczonych dużym ryzykiem niepowodzenia powołuje się specjalny zespół i przygotowuje się plany na wypadek sytuacji kryzysowej. O ostatecznym wyniku działań wdrożeniowych przesądza wydanie decyzji przez osobę koordynującą wdrożenie (zazwyczaj Dyrektora COI) na podstawie rekomendacji zespołu realizującego wdrożenie.

Działania COI w zakresie procesu wytwarzania oprogramowania opisują:

- *Zasady wytwarzania oprogramowania w COI,* definiujące wprowadzenie nowego wprowadzania nowego kodu do wdrożenia*,*
- *Opis narzędzi stosowanych dla zapewnienia ciągłości procesu wytwórczego oprogramowania,* dotyczący narzędzi używanych przez COI, które służą do realizacji tzw. ciągłej integracji,
- *Procedura zapewniania bezpieczeństwa w zarządzaniu zmianą* regulująca proces konsultacji z Departamentem Cyberbezpieczeństwa na etapie przygotowywania, implementacji oraz wdrażania zmian w oprogramowaniu,
- *Opis stosowanej przez COI metodyki testowania oprogramowania .*

Przyjęta przez COI metodyka wytwarzania oprogramowania miała charakter iteracyjno-przyrostowy[29].

Testy oprogramowania przeprowadzane przez COI można podzielić na: testy automatyczne (automatyczna realizacja stworzonych przez programistów testów jednostkowych), testy wydajnościowe, testy funkcjonalno-użytkowe przeprowadzane ręcznie (testy zgodności ze specyfikacją wymagań, testy interfejsu użytkownika, testy WCAG[30], jak również testy integracyjne i akceptacyjne), a także testy bezpieczeństwa.

(akta kontroli str. 375-465, płyta DVD1 poz. 728-729, 759, 1314-1317)

Realizowany przez COI proces zarządzania zmianami, od strony proceduralno-zarządczej był zorganizowany prawidłowo w sposób typowy dla tego rodzaju procesów.

7. Zapewnienie bezpieczeństwa systemów ePUAP i PZ

W COI podjęto działania w celu wdrożenia wymagań międzynarodowej normy z zakresu bezpieczeństwa informacji ISO/IEC 27001. Nie wdrożono natomiast do dnia zakończenia czynności kontrolnych Systemu Zarządzania Bezpieczeństwem

[28] Ang. Request for Comments.

[29] Proces zbierania wymagań, projektowania, budowania oraz testowania systemu zorganizowany w krótsze cykle rozwojowe.

[30] Ang. Web Content Accessibility Guidelines - wytyczne dla dostępności treści internetowych - to zbiór określający, w jaki sposób uczynić treści internetowe bardziej dostępnymi dla osób niepełnosprawnych.

Informacji (dalej: SZBI), co było niezgodne z § 20 ust. 1 i 3 Rozporządzenia KRI. Dalszy opis w sekcji *Stwierdzone nieprawidłowości*.

W ramach prac wdrożeniowych SZBI podjęto m.in. następujące działania:

- wdrożono *Politykę Bezpieczeństwa Informacji*[31] (dalej: PBI), *Politykę Zarządzania Ciągłością Działania*, *Politykę Ochrony Danych Osobowych*,
- przeprowadzono proces analizy ryzyka, a w 2019 r. przeprowadzono zadanie audytowe o charakterze doradczym przez audytorów wewnętrznych COI pn. *Organizacja i zarządzanie bezpieczeństwem informacji wybranych usług w oparciu o normę ISO/IEC 27001* oraz przeprowadzono weryfikację kompletności i adekwatności procesów oraz dokumentacji bezpieczeństwa informacji, z której sporządzono *Raport z przeglądu SZBI*[32],
- przeprowadzono szkolenie z zakresu przyjętej PBI dla członków zespołu COI-HOUSTON,
- 30 września 2020 r. wydano zarządzenie Nr 93/2020 w sprawie w sprawie powołania w Centralnym Ośrodku Informatyki Systemu Zarządzania Bezpieczeństwem Informacji oraz powołania roli Pełnomocnika ds. SZBI, Audytora ds. SZBI i pozostałych ról wspierających SZBI (dalej: zarządzenie ws. powołania SZBI w COI), które zobowiązało Dyrektora Pionu Operacji COI do wdrożenia do dnia 31 listopada 2020 r. procedur administracyjnych SZBI w zakresie audytowania, monitorowania, oceny, przeglądu oraz doskonalenia SZBI.

W COI w 2015 r. wdrożono PBI, jako komplementarną z politykami systemów ustanowionymi przez MC, obejmującą systemy ePUAP i PZ, w ramach której opracowano szereg procedur szczegółowych[33]. PBI uzupełniono w 2018 r. o Politykę monitoringu[34] oraz w 2020 r. o Politykę zapewniania bezpieczeństwa w zarządzaniu zmianą[35], które zostały wdrożone w COI w wyniku implementacji wymaganych przepisów sankcjonujących proces ochrony danych osobowych, w szczególności przepisów *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych)*.

W COI sporządzono formalne i udokumentowane polityki i procedury zarządzania tożsamością i kontrolą dostępu do ePUAP/PZ wchodzące w skład PBI (Polityki Bezpieczeństwa Informacji) w tym procedury PB008 - Zasady nadawania, usuwania i modyfikacji uprawnień oraz procedury nadawania praw dostępu fizycznego w COI oraz wnioskowania o dostęp do obiektów współużytkowanych i MC. Uzupełniające w tym zakresie są instrukcje i podręczniki dla obywateli oraz urzędników opublikowane na stronie www.epuap.gov.pl.

---

31 Na podstawie zarządzenia Dyrektora COI 63/2015 z dnia 26 października 2015 r.

32 Raport z dnia 23 grudnia 2019 r., sporządzony przez pracownika COI posiadającego certyfikat Lead Auditor 27001, niebędącego audytorem wewnętrznym COI.

33 Zgłoszenie i obsługa incydentu bezpieczeństwa PB001, Zabezpieczenia urządzeń przenośnych i ich użytkowanie PB002, Trwałe usuwania danych i niszczenia teleinformatycznych nośników danych PB003, Zarządzanie sprzętem komputerowym PB004, Konfiguracja stacji roboczych urządzeń przenośnych i oprogramowania PB005, Przekazanie nowego systemu do eksploatacji PB006, Zdalne łączenie się w zasobami organizacji Telepraca PB007, Zasady nadawania, usuwania i modyfikacji uprawnień PB008, Metody dostępu do kont uprzywilejowanych PB009, Ochrona antywirusowa PB010, Polityka korzystania z zasobów Internetu PB011, Użytkowanie poczty elektronicznej PB012, Dopuszczenie oprogramowania biurowego do eksploatacji PB013, Zarządzanie nośnikami wymiennymi PB014, Polityka czystego biurka i czystego ekranu PB015.

34 Wdrożona w COI na podstawie zarządzenia Dyrektora COI z 23 maja 2018 r., które weszło w życie 25 maja 2018 r.

35 Wdrożona w COI na podstawie zarządzenia Dyrektora COI z 15 czerwca 2020 r.

(akta kontroli str. 375-465, płyta DVD1 poz. 25-45, 756-764, 1068, 1072, 1051-1064)

W toku kontroli ustalono, iż w COI przeprowadzano półautomatyczne testy bezpieczeństwa[36] m.in. systemów ePUAP i PZ. Z testów tych sporządzano raporty, w których posługiwano się pojęciem *testy penetracyjne*[37]. Zdaniem NIK, tak przeprowadzone testy bezpieczeństwa nie stanowią testów penetracyjnych w rozumieniu powszechnie przyjętych standardów. Dalszy opis w sekcji *Stwierdzone nieprawidłowości*.

Monitorowanie incydentów bezpieczeństwa jest realizowane przez Security Operation Center (dalej: SOC) dla usług świadczonych przez COI na rzecz MC, w tym również na potrzeby monitorowania bezpieczeństwa systemów ePUAP/PZ. Praca SOC odbywa się w trybie ciągłym.

(akta kontroli str. 375-465, płyta DVD1 poz. 46-69, 766)

8. Kopie zapasowe

Polityki tworzenia i testowania kopii zapasowych COI nie zostały opisane w obowiązującej PBI, natomiast zostały zawarte w *Procedurze zarządzania systemem backupowym*, *Procedurze odtworzenia bazy ePUAP* i *Procedurze utrzymaniowej*.

Zdaniem NIK, procedury tworzenia i testowania kopii zapasowych systemów ePUAP oraz PZ wprawdzie zawierają wszystkie wymagane elementy, jednakże dokumenty te mają charakter poradnika administratora, a nie polityk adresowanych do pracowników COI nieznających specjalistycznego systemu do wykonywania kopii zapasowych w sposób zautomatyzowany. W dokumentach tych w zakresie wykonywania i testowania kopii zapasowych zostały opublikowane pliki konfiguracyjne systemu backupowego, ponadto nie wyjaśniono parametrów systemu opisujących częstotliwość tworzenia kopii zapasowych i czasu ich przechowywania. NIK zauważa, że w COI powinna funkcjonować osobna procedura opisująca kompleksowo i zrozumiale politykę tworzenia i przechowywania kopii zapasowych przez COI, a ewentualne szczegółowe rozwiązania dla administratorów wraz z plikami konfiguracyjnymi systemu backupowego mogą stanowić załącznik tego dokumentu.

W trakcie kontroli NIK, COI dokonał aktualizacji obowiązujących procedur zarządzania systemem backupu ePUAP oraz PZ o elementy związane z przygotowaniem i zatwierdzeniem każdorazowo raportu z przebiegu odtworzenia kopii zapasowych przez Dyrektora Departamentu Eksploatacji Systemów COI.

Zgodnie z przyjętymi w COI procedurami, kopie zapasowe są tworzone w sposób niezależny w dwóch serwerowniach w trybie przyrostowym (dla serwerów aplikacyjnych) lub pełnym (baza danych systemu ePUAP) za pomocą systemu automatyzującego ten proces i przechowywane są na urządzeniach dyskowych deduplikatora, a także na taśmach magnetycznych, które znajdują się w tym samych pomieszczeniach, co główne serwery aplikacyjne i bazodanowe. Kopie zapasowe obejmują również tzw. *archive logi*, tj. dziennik zdarzeń obejmujący informacje generowane przez system podczas tworzenia kolejnych kopii zapasowych systemu, co umożliwia podjęcie reakcji na ewentualne błędy pojawiające się w trakcie tego procesu. Kopie bezpieczeństwa przechowywane są w tym samym pomieszczeniu,

---

[36] Polegające na: przygotowaniu listy kontrolnej (tj. listy testów do wykonania), konfiguracja narzędzi, uruchomieniu automatycznych skanerów podatności, manualna weryfikacja wykrytych przez skanery podatności i opracowanie raportu.

[37] Raport z testów: nForms, system ePUAP2, bezpieczeństwa funkcjonalności „Unieważnienie Profilu Zaufanego", „Przedłużenie Profilu Zaufanego" i „Rejestracja Profilu Zaufanego", bezpieczeństwa aplikacji PK Signer.

w którym znajdują się główne serwery aplikacyjne i bazodanowe, co stwarza zagrożenie, że w wypadku katastrofy skutkującej zniszczeniem jednej z serwerowni, zniszczeniu ulegną również kopie zapasowe tam umieszczone. Niezależnie od tego, COI dysponuje zapasowym ośrodkiem danych, posiadającym własne kopie zapasowe, dlatego takie rozwiązanie - zdaniem NIK - należy uznać jako akceptowalne na wypadek wystąpienia awarii.

W toku kontroli ustalono, że kopie zapasowe systemów ePUAP oraz PZ, zgodnie z obowiązującymi procedurami, są regularnie testowane, raz na pół roku. Z testów tych Kierownik Zespołu Administrowania Systemami COI sporządza notatki z odtworzeń ePUAP i PZ.

(akta kontroli str. 188-192, 375-471, płyta DVD1 poz. 359-373, 859-873, 1022-1030)

9. Plany zapewnienia ciągłości działania systemów ePUAP i PZ w sytuacji wystąpienia znaczącej awarii lub katastrofy

COI przygotował oraz wdrożył rozwiązania techniczne i organizacyjne dla ePUAP i PZ w celu zapewnienia ciągłości działania w sytuacji wystąpienia znaczącej awarii lub katastrofy. Ustanowiono Polityki Zarządzania Ciągłością Działania COI oraz Plan Zarzadzania Kryzysowego i Procedury Ciągłości Działania COI-HOUSTON. Dokumenty te, a w szczególności Polityka Zarządzania Ciągłością Działania COI, regulują m.in. zagadnienia dotyczące:

- określenia struktury i planu zarządzania kryzysowego, w tym składu i trybu działania, komunikacji Sztabu Kryzysowego COI, jak również określenia poziomów gotowości alarmowej i zasad wzmożonego monitorowania,
- konieczności utrzymywania Procedur Ciągłości Działania oraz Procedur Odtworzenia dla poszczególnych komórek organizacyjnych COI oraz zasady ich dystrybucji i aktualizacji,
- zasady wykonywania testów Procedur Ciągłości Działania,
- zasady raportowania zagrożeń,
- konieczności wykonywania analizy BIA[38].

(akta kontroli str. 375-465, płyta DVD1 poz. 63-79, 383-399)

W COI wdrożono rozwiązania w zakresie odtworzenia infrastruktury po katastrofie poprzez zastosowanie podwójnej redundancji (nadmiarowości) polegającej na utrzymywaniu dwóch równoległych ośrodków przetwarzania danych oraz zabezpieczono zasoby ludzkie do utrzymania tych systemów w przypadku absencji pracowników przez redundancję osobową. Oba ośrodki zawierają te same bazy danych systemów ePUAP i PZ oraz ten sam zestaw serwerów aplikacyjnych. W obrębie każdego z dwóch ośrodków wykonywane są kopie zapasowe. W razie awarii, bądź zniszczenia ośrodka głównego, jego zadania przejmuje ośrodek zapasowy.

W COI stosowana jest praktyka w zakresie zapewniania środków redundancji, tj. procedura przełączania systemów ePUAP i PZ z ośrodka głównego na zapasowy oraz testów procedury odtwarzania baz danych z kopii zapasowych. W toku kontroli ustalono, iż wykonywane są testy odtwarzania baz danych dwa razy do roku oraz prowadzone są testy przełączania systemów ePUAP i PZ z ośrodka głównego na zapasowy jeden raz do roku. Z testów tych sporządzane są raporty. Z analizy tych

[38] BIA - ang. Business Impact Analysis - analiza wpływu na działalność, jest to proces analizy funkcji biznesowych pozwalający określić, jaki wpływ na działalność organizacji miałoby ich ewentualne poważne zakłócenie lub przerwanie.

dokumentów wynika, iż wszystkie testy przełączeniowe przebiegły pozytywnie, a czas przełączania systemu ePUAP z ośrodka głównego na zapasowy wynosił: 25 minut w kwietniu 2019 r., 37 minut w marcu 2020 r. oraz 2 godziny i 32 minuty w kwietniu 2020 r. Dyrektor Pionu Operacji COI wyjaśnił, iż przełączenie tylko bazy danych jest szybsze niż przełączenie wszystkich serwerów aplikacyjnych, a testy przełączania, obejmowały wyłączenie serwerów aplikacyjnych, co jest czasochłonne i robi się to dla bezpieczeństwa bazy danych.

Zdaniem NIK, przyjęte przez COI rozwiązania techniczne i organizacyjne są właściwe dla zapewnienia ciągłości działania systemów ePUAP i PZ w sytuacji wystąpienia znaczącej awarii lub katastrofy.

(akta kontroli str. 375-471, płyta DVD1, 63-79, 730-755, 859-867)

10. Audyty bezpieczeństwa

W COI przeprowadzono audyt bezpieczeństwa systemu ePUAP przez zewnętrzny podmiot specjalizujący się w wykonywaniu tego rodzaju audytów na podstawie umowy zawartej pomiędzy MC, a tym podmiotem. Przedmiotem audytu było dokonanie oceny poziomu bezpieczeństwa systemu ePUAP. Dyrektor Pionu Operacji COI wyjaśnił, że *wszystkie możliwe do realizacji zalecenia z raportu zostały bezzwłocznie zrealizowane*, *natomiast z uwagi na fakt, iż raport ten nie był przed sporządzeniem konsultowany z COI, część z zaleceń było niemożliwych do wykonania lub generowały ryzyko w obszarach nieznanych audytorom* (…).

Niezależnie od zewnętrznego audytu, w ramach stosowanego w COI procesu wytwórczego oprogramowania prowadzone są testy wdrażanych zmian w oprogramowaniu pod kątem bezpieczeństwa.

(akta kontroli str. 203-240, 375-465, płyta DVD1 poz. 82-88, 1068)

Stwierdzone nieprawidłowości

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

1. W umowach na utrzymanie systemów ePUAP i PZ ustalono maksymalne czasy obsługi poszczególnych kategorii zgłoszeń, które są zbyt długie, gdyż mogą utrudnić korzystanie z tych systemów przez obywateli i urzędy.

   I tak, dla systemu ePUAP maksymalny czas na obsługę incydentu krytycznego w okresie od 30 marca 2016 r. do 4 kwietnia 2019 r. wynosił trzy dni robocze (od tej daty - jeden dzień roboczy). Dla porównania czas obsługi incydentów krytycznych dla systemu PZ wynosił do 11 godzin.

   Natomiast czas obsługi incydentów pilnych zarówno dla systemu ePUAP jak i PZ wynosił 10 dni roboczych, a incydentów standardowych – 20 dni roboczych.

   Dyrektor Pionu Operacji COI wyjaśnił, że *czasy obsługi zgłoszeń zostały ustalone w wyniku uzgodnień pomiędzy stronami umowy na podstawie doświadczeń w utrzymaniu systemów. Należy podkreślić, iż są to graniczne czasy obsługi zgłoszeń, wynikające między innymi ze specyfiki niektórych incydentów, wymagających długotrwałych działań naprawczych. W przypadku incydentów krytycznych Centralny Ośrodek Informatyki podejmuje działania w trybie 24/7 w celu jak najszybszego usunięcia incydentu, aby jak najszybciej zarządzić sytuacją kryzysową.*

   (akta kontroli str. 203-240, 375-465, płyta DVD1 poz. 476-480, 573-575)

2. COI przyjęło nierzetelny mechanizm pomiaru jakości obsługi zgłoszeń.

   Na potrzeby wyliczenia liczby zgłoszeń obsłużonych w danym miesiącu terminowo COI kwalifikowało jedynie zgłoszenia zakończone w danym miesiącu, przy czym nie uwzględniano wielkości przekroczenia wymaganego czasu obsługi, a jedynie sam fakt przekroczenia. W efekcie przyjęcia takich założeń zamykanie przez COI incydentów opóźnionych w kolejnych miesiącach zmniejsza raportowaną skuteczność obsługi zgłoszeń, wobec czego COI nie ma motywacji do ich zamykania po przekroczeniu czasu na ich obsługę.

   W związku z powyższym dane zaprezentowane w raportach utrzymania systemów ePUAP i PZ, dotyczące skuteczności obsługi zgłoszeń przez COI w danym miesiącu nie odzwierciedlały rzeczywistości. Pomimo, iż np. w marcu 2020 r. odpowiednio 76% incydentów dotyczących PZ i 63% incydentów dotyczących ePUAP nie została nawet otwarta, zaraportowana do MC skuteczność obsługi zgłoszeń dla ePUAP wynosiła w marcu 93,6%, a w kwietniu 96,88%, natomiast dla PZ wyniosła odpowiednio 96,2% i 95,88%.

   Ponadto, NIK zauważa, że umowy utrzymaniowe, wbrew praktyce rynkowej nie określają wymaganych czasów reakcji na zgłoszenie, tj. czasu, jaki może upłynąć od zarejestrowania zgłoszenia w systemie do rozpoczęcia jego obsługi.

   Dyrektor Pionu Operacji COI wyjaśnił, że *sposób rozliczania czasu obsługi zgłoszeń i ich raportowania wynika z umów utrzymaniowych na powierzone systemy. Umowy te zostały uzgodnione i podpisane przez Ministerstwo Cyfryzacji i Centralny Ośrodek Informatyki. W raporcie uwzględnia się zgłoszenia, których obsługa została zakończona w danym miesiącu. Raport prezentuje zgłoszenia, z podziałem na zgłoszenia zrealizowane i niezrealizowane zgodnie z SLA. Taki model gwarantuje pełne raportowanie procesu obsługi incydentu. Jeśli dojdzie do przekroczenia SLA incydentu to zostanie ono zaraportowane w miesiącu, w którym zakończy się jego obsługa. W momencie raportowania pracownik nie jest w stanie stwierdzić jak duże przekroczenie zostanie odnotowane na danym incydencie, kiedy faktycznie nastąpi jego realizacja. Model raportowania przyjęty przez COI jest zgodny z aktualnymi trendami rynkowymi. Model ten stawia na pierwszym miejscu percepcję użytkownika końcowego, dla którego kluczowa jest realizacji incydentu w terminie a nie średni czas przekroczenia SLA. Należy podkreślić, że wskazany (…) okres, tj. marzec – czerwiec 2020 r., ze względu na sytuację epidemiczną w kraju jest wybitnie niereprezentatywny. W okresie tym liczba zgłoszeń i połączeń telefonicznych była kilka razy wyższa niż w analogicznym okresie w roku 2019. Jednocześnie Service Desk realizował dodatkowe zadania zlecone przez Ministra Cyfryzacji (…).*

   (akta kontroli str. 203-240, 375-465, płyta DVD1 poz. 212-320, 374-377, 476-480, 573-575, 1194-1204)

3. W umowach na utrzymanie ePUAP i PZ przyjęto niewłaściwy sposób wyliczania dostępności tych systemów.

   Zgodnie z umowami dostępność danej usługi ePUAP i PZ jest ustalana jako udział czasu obsługi incydentów krytycznych w danym miesiącu do całości wymaganego czasu jej dostępności, przy czym incydent krytyczny zdefiniowano jako awarię powodującą całkowity brak możliwości korzystania z głównych funkcji systemu ePUAP lub wszystkich usług wsparcia procesów biznesowych we wszystkich lokalizacjach w zakresie systemu PZ.

   Zdaniem NIK, założenie, że dostępność systemów ePUAP i PZ obniżają jedynie incydenty krytyczne, przy jednoczesnym wąskim zdefiniowaniu tego pojęcia powoduje, że raporty z utrzymania tych systemów w okresie poddanym

kontroli nie odzwierciedlały ich rzeczywistej dostępności. W okresie poddanym kontroli zdarzały się bowiem incydenty o statusie niższym niż krytyczne, które powodowały brak możliwości korzystania z tych systemów przez poszczególnych użytkowników zgodnie z ich przeznaczeniem.

Ponadto, NIK zauważa, że przy wyliczeniach dostępności systemów uwzględnia się jedynie incydenty, których obsługa zakończyła się w danym miesiącu rozliczeniowym, co również ma wpływ na rzetelność określenia dostępności.

Dyrektor Pionu Operacji wyjaśnił, że te kwestie wynikają z umów podpisanych z MC. Ponadto wyjaśnił, że *incydenty krytyczne powodują faktyczną niedostępność systemu lub jego głównych usług. (…) awaria bramki SMS może być zaklasyfikowana jako incydent krytyczny, bądź pilny. Stosowana w systemie ePUAP i PZ bramka SMS wykorzystuje usługi dwóch niezależnych operatorów. Jeśli awaria bramki SMS dotyczy jednego z operatorów nadal zachowana jest ciągłość usługi a incydent uznaje się jako pilny. Incydent krytyczny wystąpi wówczas, gdy dotyczy całkowitej niedostępności bramki SMS u obu operatorów. (…) zgodnie z umową utrzymaniową systemu PZ za incydent krytyczny uznaje się nieprawidłowe działanie systemu w środowisku produkcyjnym powodujący całkowity brak możliwości korzystania z głównych funkcji systemu. Główne funkcje systemu są wyszczególnione i opisane w załączniku numer 8 umowy utrzymaniowej, dzięki czemu strony umowy nie mają wątpliwości co do prawidłowej klasyfikacji danego incydentu. Wszystkie incydenty dotyczące głównych funkcji systemu, powodujące ich całkowitą niedostępność, uznawane są za incydenty krytyczne. (…) przyjęte zapisy służą zapewnieniu rozliczalności danej usługi. W raportach miesięcznych uwzględniane są incydenty, których obsługa została zakończona w danym okresie rozliczeniowym i których parametry obsługi można umieścić w raporcie. Incydenty, których obsługa nie została zakończona i nie znamy na moment końca okresu rozliczeniowego terminu ich zakończenia, są rozliczane w kolejnym okresie. Zamknięcie uniemożliwia ponowne otwarcie danego incydentu co pozwala na uniknięcie ryzyka związanego z powielaniem tych samych incydentów w kolejnych okresach i ich rozliczalność.*

NIK nie kwestionuje, że sposób obliczania dostępności systemów wynika z umów z MC i został tam szczegółowo opisany. Zdaniem NIK, przyjęty w tych umowach sposób obliczania dostępności systemu nie odzwierciedla jednak w pełni rzeczywistości.

(akta kontroli str. 203-240, 375-465, płyta DVD1 poz. 212-320, 374-377, 476-480, 573-575, 1194-1204)

4. COI nie w pełni wdrożył SZBI, co było niezgodne z § 20 ust. 1, w zw. z ust. 3 rozporządzenia KRI, które stanowią, że 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, a wymagania te uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001. Przepisy te obowiązują od 31 maja 2012 r.

   Dyrektor Pionu Operacji COI m.in. poinformował, że SZBI wdrożono w COI *w wyniku wielomiesięcznych prac, zrealizowanych w okresie 2019 – 2020, związanych z oceną stanu dostosowania istniejących regulacji w COI do wymogów normy ISO/IEC 27001 - I-II kwartał 2019 roku oraz z implementacją*

wymogów normy ISO/IEC 27001 do funkcjonujących w organizacji procesów biznesowych, operacyjnych i technicznych - II kwartał 2019 - obecnie. W COI zaplanowano przeprowadzenie certyfikacji SZBI na zgodność z normą ISO/IEC 27001. W tym celu w I kwartale 2020 r. rozpoczęto postępowanie przetargowe, którego celem było wyłonienie firmy certyfikacyjnej, które w II kwartale 2020 r. *zostało wstrzymane ze względu na ograniczenia wprowadzone z powodu pandemii*. (…) *Postępowanie zostanie wznowione w I kwartale 2021 r., chyba że okoliczności zw. z pandemią COVID 19 (wzrastająca liczba zachorowań) przesuną termin realizacji.* Ponadto wyjaśnił, iż *(…) dalsze prace wdrożeniowe będą kontynuowane zgodnie z treścią par. 3 Zarządzenia nr 93/2020, tj.: do 30.11.2020 roku zostaną wdrożone procedury administracyjne SZBI w zakresie auditowania, monitorowania, oceny, przeglądu oraz doskonalenia SZBI. Po zakończeniu pełnego wdrożenia SZBI zostanie przeprowadzony przegląd SZBI w ramach prac Audytora SZBI, na podstawie Procedury audytowania SZBI.*

NIK nie kwestionuje podjęcia przez COI działań w celu wdrożenia SZBI zgodnie z wymaganiami normy ISO/IEC 27001. NIK zauważa jednak, że proces ten trwa w COI już ponad cztery lata i nie został do dnia zakończenia czynności kontrolnych zakończony. W toku kontroli NIK przeprowadzonej w 2016 r. w COI *pt. System Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność* ówczesny Dyrektor COI Pan Rafał Leśkiewicz wyjaśnił, iż trwały wówczas prace przygotowawcze związane z wdrożeniem ww. normy.

Dyrektor COI dopiero 30 września 2020 r., tj. ostatniego dnia prowadzonych przez kontrolerów NIK czynności kontrolnych, podpisał zarządzenie ws. powołania SZBI w COI (wraz ze strukturą zarządczą) oraz zobowiązał Dyrektora Pionu Operacji COI do wdrożenia do dnia 31 listopada 2020 r. procedur administracyjnych SZBI w zakresie audytowania, monitorowania, oceny, przeglądu oraz doskonalenia SZBI. Zatem sam proces wdrożenia będzie ukończony dopiero po wdrożeniu ww. procedur administracyjnych.

(akta kontroli str. 203-240, 361-364, 375-465, płyta DVD 1 poz. 756-764, 1068)

5. COI nie przeprowadził właściwych testów penetracyjnych systemów ePUAP i PZ, co było działaniem nierzetelnym. W ocenie NIK przeprowadzenie pełnych testów jest niezbędne dla uzyskania potwierdzenia, że systemy ePUAP i PZ, które są użytkowane przez obywateli oraz urzędy, są bezpieczne.

   Przeprowadzane przez COI testy półautomatyczne bezpieczeństwa nie stanowią testów penetracyjnych w rozumieniu powszechnie przyjętych standardów[39]. Testy bezpieczeństwa przeprowadzone przez COI zakończyły się na czwartej fazie, tj. identyfikacji obecnych w systemie podatności, podczas gdy prawidłowo przeprowadzony test penetracyjny np. w standardzie PTES (Penetration Testing Metodologies and Standard)[40] składa się z ośmiu faz dla kompletnego ataku na system informatyczny. Pominięcie kluczowych faz właściwego ataku sprawia, że przeprowadzane przez COI testy nie są testami penetracyjnymi, a jedynie skanowaniem podatności.

   Dyrektor Pionu Operacji wyjaśnił, *że przyjęta metodyka prowadzenia testów bezpieczeństwa ePUAP/PZ została wypracowana w oparciu o doświadczenia zebrane w trakcie testów bezpieczeństwa prowadzonych w ciągu ostatnich kilku lat. Wspomniana metodyka została dostosowana do procesu wytwórczego*

[39] Test penetracyjny, zgodnie z definicją brytyjskiej agencji badawczej NCSC (National Cyber Security Center), jest metodą uzyskiwania pewności co do bezpieczeństwa systemu informatycznego poprzez próbę złamania bezpieczeństwa tego systemu, w całości lub w części, przy użyciu tych samych narzędzi i technik, jakie mógłby zastosować atakujący.

[40] http://www.pentest-standard.org/index.php/Main_Page.

oprogramowania, którego istotnym elementem są testy bezpieczeństwa. W przytoczonych przykładach (…) testy bezpieczeństwa obejmowały jedynie zakres wprowadzonych zmian, co było wskazane w poszczególnych raportach z testów. Wskazując wprost w przypadku wprowadzania niewielkich zmian w systemach, przeprowadzane są wyłącznie testy punktowe, natomiast w przypadku dużej ilości zmian lub zmian w kluczowych komponentach, przeprowadzane są testy bezpieczeństwa całego rozwiązania. Decyzja o tym czy przeprowadzane są testy punktowe czy całościowe podejmowana jest w trakcie planowania harmonogramu projektu zmian w systemie, gdzie odbywają się konsultacje przedstawiciela zespołu bezpieczeństwa z analitykami i architektami zaangażowanymi w projekt. Istotnym elementem oceny zmiany jest szacowanie wpływu zmian na atrybuty bezpieczeństwa systemu. Przed rozpoczęciem testów bezpieczeństwa dokonywana jest weryfikacja ostatecznie wprowadzonych zmian, czy zgodne są z pierwotnymi założeniami i czy przyjęty zakres testów jest prawidłowy. Przyjęta przez Centralny Ośrodek Informatyki metodyka prowadzenia testów bezpieczeństwa w ramach procesu wytwórczego oparta jest o elementy standardu PTES oraz OWASP Testing Guide i zawiera między innymi takie działania jak: Planowanie testów bezpieczeństwa; Określenie i weryfikacja zakresu testów bezpieczeństwa; Zapoznanie się z dokumentacją systemu, wywiad z zespołem wytwórczym; Analiza powierzchni ataku; Przeprowadzenie rekonesansu; Automatyczna identyfikacja znanych podatności; Analiza zidentyfikowanych słabości systemu; Przeprowadzenie działań aktywnych (próba ataku, wykorzystania zidentyfikowanych słabości); Potwierdzenie zidentyfikowanych podatności; Ocena skutków oraz ryzyka dla zidentyfikowanych podatności; Opracowanie rekomendacji odnośnie metod usunięcia podatności, minimalizacji ryzyka; Raportowanie. (…)

(akta kontroli str. 203-240, 375-465, płyta DVD1 poz. 46-69, 766)

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Dokonanie we współpracy z właścicielem systemów ePUAP i PZ zmiany sposobu obliczania ich dostępności poprzez uwzględnienie czasu trwania incydentów, które wpływają na faktyczny brak możliwości korzystania z tych systemów zgodnie z ich przeznaczeniem, bez względu na ich sklasyfikowanie jako standardowe, pilne, czy krytyczne.
2. Dokonanie we współpracy z właścicielem systemów ePUAP i PZ zmiany definicji incydentu krytycznego w ten sposób, aby uwzględniała ona brak możliwości lub istotne ograniczenie w korzystaniu z którejkolwiek z głównych funkcji tych systemów.
3. Uwzględnienie w obliczanej dostępności systemów ePUAP i PZ także incydentów niezamkniętych w danym miesiącu.
4. Skrócenie we współpracy z właścicielem systemów ePUAP i PZ gwarantowanych czasów obsługi incydentów pilnych i standardowych dotyczących ePUAP oraz PZ.
5. Określenie we współpracy z właścicielem systemów ePUAP i PZ czasu reakcji na zgłoszenie, tj. czasu, jaki może upłynąć od zarejestrowania zgłoszenia w systemie do rozpoczęcia jego obsługi.
6. Wprowadzenie we współpracy z właścicielem systemów ePUAP i PZ zmiany w zakresie sposobu raportowania o obsłudze zgłoszeń od użytkowników

w sposób, który będzie uwzględniał nie tylko sam fakt przekroczenia terminu na obsługę zgłoszeń, ale również długość okresu tej obsługi.

7. Przeprowadzenie właściwych testów penetracyjnych systemów ePUAP i PZ, zawierających komponent eskalacji ataku.

Ze względu na podjęcie przez COI czynności zmierzających do wdrożenia SZBI, a także ze względu na skrócenie, we współpracy z MC, terminu na obsługę incydentu krytycznego w aneksie nr 4 do umowy na utrzymanie systemu ePUAP z 4 kwietnia 2019 r. z trzech do jednego dnia, NIK odstępuje od formułowania wniosków pokontrolnych w tym zakresie.

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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli. 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 i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, listopada 2020 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Dyrektor
Bogdan Skwarka

.....
podpis

Kontrolerzy
Piotr Bielecki
Główny specjalista kp.

.....
podpis

Mariusz Czarnecki
Główny specjalista kp.

.....
podpis