Realizacja wymagań, które stawia przed JST rozporządzenie w sprawie Krajowych Ram Interoperacyjności

II PODKARPACKI KONWENT INFORMATYKÓW I ADMINISTRACJI

15-16 października 2015, Zamek Dubiecko

Paweł Jaworski
Informatyk Wojewódzki

O czym będzie wystąpienie

Krajowe Ramy Interoperacyjności – KRI

stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą (definicja określona przez NIK)

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 2012 r., poz.526)

Wystąpienie oparte na III filarach

I. Wyniki kontroli NIK w zakresie między innymi KRI.
II. Doświadczenia zbierane w ramach audytu wewnętrznego przeprowadzanego corocznie w PUW.
III. Dobre praktyki wynikające z kontroli realizowanych w JST (wynikające z ustawy o Informatyzacji).

KRI 1/6

Należy zaznaczyć, że ww. rozporządzenie określa między innymi:

§ 1. Rozporządzenie określa:

3) minimalne wymagania dla systemów teleinformatycznych, w tym:

…

b) sposoby zapewnienia bezpieczeństwa przy wymianie informacji,

…

d) sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych.

KRI 2/6

Rozdział IV - Minimalne wymagania dla systemów teleinformatycznych

§ 15. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich **funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności**, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o **udokumentowane procedury**.

KRI 3/6

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli **projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą** podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

To są fazy cyklu życia usług

KRI 4/6

§ 19. W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (**WCAG 2.0**), z uwzględnieniem poziomu **AA**, **określonych w załączniku nr 4 do rozporządzenia.**

Wytyczne do BIP

KRI 5/6

§ 20. 1. 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**.

2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

14 punktów

KRI 6/6

3. **Wymagania określone w ust. 1 i 2 uznaje się za spełnione**, jeżeli system zarządzania bezpieczeństwem informacji został opracowany **na podstawie** Polskiej Normy **PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

4. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

§ 21. ….

Wyniki kontroli NIK

Temat i numer kontroli

Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu (P/14/004)

Krótki film z NIK

Wypowiedź dyrektora Departamentu Administracji Publicznej Bogdana Skwarki - materiał emisyjny

https://www.nik.gov.pl/aktualnosci/nik-o-wdrazaniu-systemow-teleinformatycznych-w-miastach-i-gminach.html

Wprowadzenie oraz uzasadnienie podjęcia kontroli 1/2

Podstawowe wymagania w zakresie systemu zarządzania bezpieczeństwem informacji reguluje § 20 rozporządzenia KRI.

§ 20. 1. 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**.

Wprowadzenie oraz uzasadnienie podjęcia kontroli 2/2

W kontekście **dostępności informacji** dla wszystkich obywateli istotne jest wprowadzanie rozwiązań technicznych umożliwiających korzystanie z nich **przez osoby niepełnosprawne**. Stąd informacje **udostępniane na stronach internetowych urzędów** powinny charakteryzować się także pełną czytelnością dla osób niepełnosprawnych.

Kontrolą objęto okres od dnia wejścia w życie rozporządzenia KRI, tj. **od 31 maja 2012 r.** do dnia zakończenia czynności kontrolnych w 2014 r. Czynności kontrolne przeprowadzono w okresie od 8 czerwca do **24 października 2014 r.**

Ocena kontrolowanej działalności 1/3

Najwyższa Izba Kontroli, **pozytywnie** ocenia działania podjęte przez burmistrzów i prezydentów miast w celu dostosowania objętych kontrolą systemów teleinformatycznych do współpracy z innymi systemami/rejestrami, jednakże NIK sformułowała wiele uwag w tym zakresie

- tylko dwanaście (**16,7%**) systemów współpracowało z innymi systemami urzędu w sposób w pełni zautomatyzowany, tj. **na poziomie najbardziej pożądanym**,
- pięć systemów (**6,9%**) **bezpośrednio korzystało z danych gromadzonych w zewnętrznych systemach/rejestrach** publicznych (zasada referencji), takich jak np. rejestr centralny PESEL czy też System Informacji Przestrzennej.

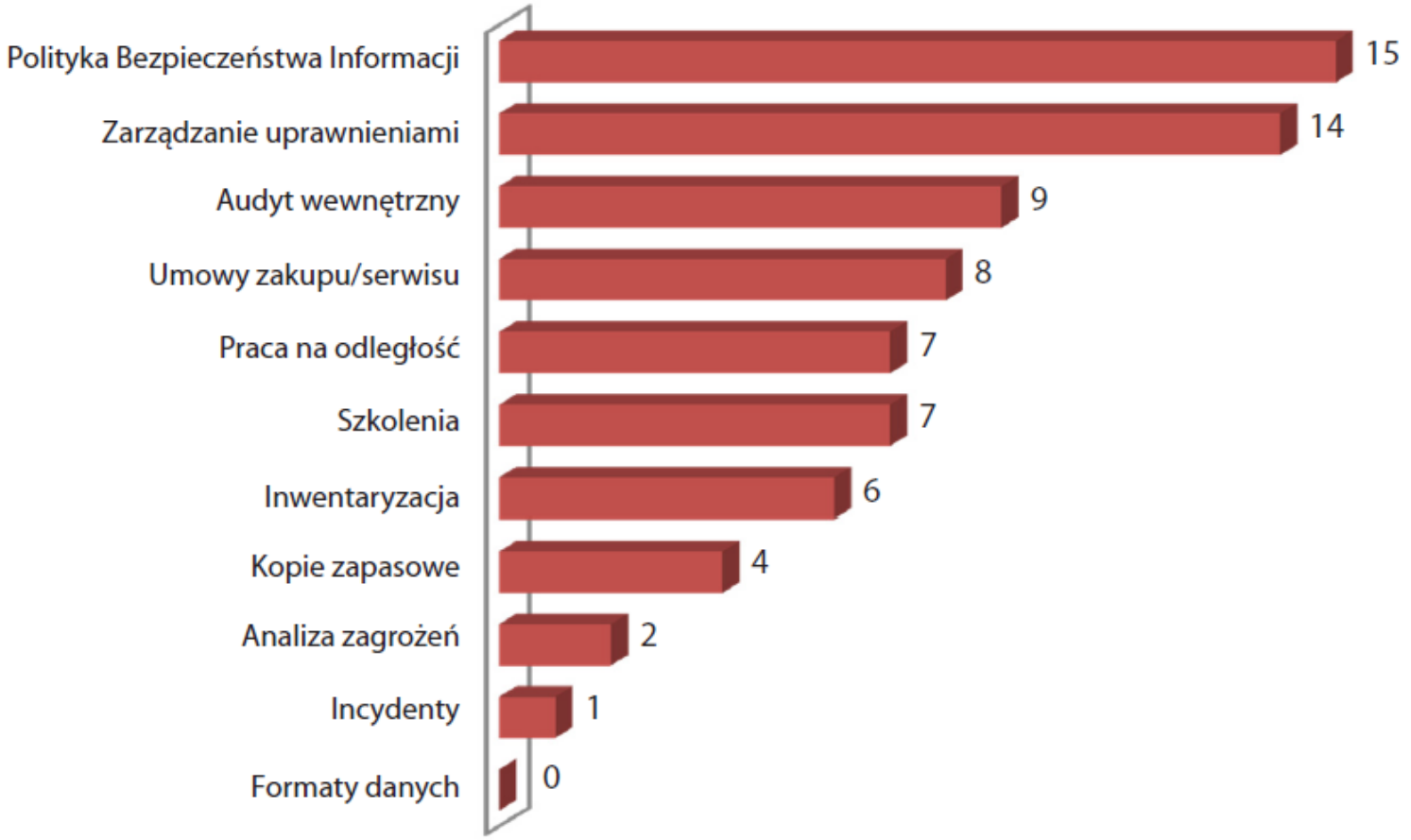
Ocena kontrolowanej działalności 2/3

NIK, ze względu na liczne nieprawidłowości, ogólnie **negatywnie** ocenia działania burmistrzów i prezydentów miast w zakresie zarządzania bezpieczeństwem informacji w urzędach, o którym mowa w § 20 rozporządzenia KRI. NIK stwierdziła nieprawidłowości w tym obszarze w 21 z 24 (**87,5%**) skontrolowanych urzędów miast, z których sześć oceniła negatywnie.

Zdaniem NIK, stwierdzone nieprawidłowości **mogą skutkować utratą dostępności**, **integralności** i **poufności** informacji przetwarzanych w systemach informatycznych urzędów wykorzystywanych do elektronicznej komunikacji i świadczenia usług.

Ocena kontrolowanej działalności 3/3

Liczba kontrolowanych urzędów, w których stwierdzono nieprawidłowości przy realizacji poszczególnych zadań w obszarze zarządzania bezpieczeństwem informacji



Źródło: Wyniki kontroli.

Dokumenty z zakresu Polityki Bezpieczeństwa Informacji

W 15 urzędach, tj. 62,5% objętych kontrolą nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji (dalej PBI), która jest elementem systemu zarządzania bezpieczeństwem informacji (zgodnie z § 20 ust. 2 pkt 1),

- opracowane regulacje dotyczyły głównie danych osobowych, brak szczegółowych instrukcji,
- Polityki Bezpieczeństwa Informacji przygotowane przez firmy zewnętrzne często „mijają” się z rzeczywistością,

Analiza zagrożeń

W zdecydowanej większości jednostek (22 z 24, tj. 91,7%) przeprowadzano okresowe analizy utraty integralności, poufności lub dostępności informacji (zgodnie z § 20 ust. 2 pkt 3)

- cyklicznie aktualizować ryzyka i analizować ich wpływ na ciągłość działania kluczowych systemów – w PUW realizowane jest to raz do roku i w ramach Zespołu Bezpieczeństwa Informacji,
- rejestr incydentów (na jego podstawie można zidentyfikować ryzyka),
- posiadać plan zachowania ciągłości działania - procedury zastępcze na wypadek awarii – łączy się to z kosztami,

Inwentaryzacja zasobów informatycznych

W czterech urzędach z 23 urzędów (tj. 17,4%) nie prowadzono inwentaryzacji zasobów informatycznych (zgodnie z § 20 ust. 2 pkt 2 - utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację),

- mimo posiadania inwentaryzacji nie była aktualizowana,
- są dostępne bezpłatne oprogramowania do przeprowadzania inwentaryzacji np. WinAudit, AIDA32

Zarządzanie uprawnieniami użytkowników

Nie opracowano pisemnych procedur zarządzania uprawnieniami użytkowników do pracy w systemach informatycznych w jednym urzędzie, a w 13 innych urzędach (54,2%) stwierdzono nieprawidłowości polegające na niedochowaniu wymogów określonych w § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI,

- należy cyklicznie aktualizować uprawnienia, czy mają je odpowiednie osoby i w odpowiednim zakresie – dostępność do danych,
- problem z odchodzącymi pracownikami i zmieniającymi stanowiska,

Szkolenia dotyczące bezpieczeństwa informacji

W 17 urzędach (70,8%) zorganizowano dla pracowników szkolenia dotyczące bezpieczeństwa informacji (zgodnie z § 20 ust. 2 pkt 6)

- pracownicy zaangażowani w proces przetwarzania informacji powinni zostać przeszkoleni oraz powinni regularnie być powiadamiani o zagrożeniach w obszarze bezpieczeństwa informacji,

Komputery przenośne

Zasady bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych zgodne z wymogami określonymi w § 20 ust. 2 pkt 8 rozporządzenia KRI ustanowiono tylko w 11 urzędach (45,8%),

- szyfrowanie dysków,
- VPN w celu połączenia z siecią jednostki,
- bezpieczeństwo danych przechowywanych w służbowych telefonach komórkowych,

Odpowiednie zapisy w umowach

W ośmiu skontrolowanych urzędach (33,3%) w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania dotyczących badanych systemów informatycznych, brak było zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z przepisem § 20 ust. 2 pkt 10 rozporządzenia KRI,

Przykładowy zapis w OPZ:

W warunkach Gwarancji: gwarancja świadczona na miejscu u Zamawiającego … w przypadku wymiany dysku twardego uszkodzony dysk pozostaje u Zamawiającego – wykonawca przedstawi oświadczenie producenta potwierdzające spełnienie tego warunku

Audyty wewnętrzne

W dziewięciu urzędach (tj. 37,5%) w okresie objętym kontrolą nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI

Obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok

Kopie zapasowe

W 20 kontrolowanych urzędach (83,3%) kopie zapasowe danych były właściwie tworzone, przechowywane oraz testowane. Jednakże w czterech urzędach stwierdzono nieprawidłowości w tym zakresie, stanowiące naruszenie § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI

- Należy dostosować zapisy w PBI do faktycznie wykonywanych czynności

Dostępność dla osób niepełnosprawnych

W kontekście dostępności informacji dla wszystkich obywateli istotne jest wprowadzanie rozwiązań technicznych umożliwiających korzystanie z nich przez osoby niepełnosprawne. Stąd informacje udostępniane na stronach internetowych urzędów powinny charakteryzować się także pełną czytelnością dla osób niepełnosprawnych.

- BIP
- portale świadczące usługi

Przeprowadzanie kontroli w JST

Podstawa prawna

art. 25 ust. 1 pkt 3 lit. a w zw. z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity z 2014 r., Dz. U. poz. 1114).

Przedmiot kontroli

Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.

Kwestionariusz przed przystąpieniem do kontroli JST przez Wojewodę

Załącznik do prezentacji

Kwestionariusz_v20151006.pdf

Dziękuję za uwagę

Paweł Jaworski

Informatyk Wojewódzki

Wydział Organizacyjno - Administracyjny

Podkarpacki Urząd Wojewódzki w Rzeszowie

ul. Grunwaldzka 15

35-959 Rzeszów

tel. (17) 867 19 25 fax (17) 867 19 66

informatyk@rzeszow.uw.gov.pl

Źródło:

- Źródło: https://www.nik.gov.pl/kontrole/P/14/004/
- materiały PUW w Rzeszowie