Realizacja rozporządzenia w sprawie Krajowych Ram Interoperacyjności – wnioski i dobre praktyki na podstawie przeprowadzonych kontroli w JST

III PODKARPACKI KONWENT INFORMATYKÓW I ADMINISTRACJI

20-21 października 2016, Zamek Dubiecko

Paweł Jaworski
Informatyk Wojewódzki

O czym będzie wystąpienie

- Podzielenie się doświadczeniami zebranymi w czasie przeprowadzanych kontroli w jst
- Nawiązanie do wytycznych MC
- Realizacja KRI i nie tylko na „własnym podwórku”

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.

Ważne w KRI 1/2

§ 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

Ważne w KRI 2/2

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. ….

Czego brakuje w JST?

PBI

Brak wewnętrznych regulacji, które obejmowałyby system zarządzania bezpieczeństwem informacji zgodnie z §20 rozporządzenia KRI, a nie tylko system ochrony danych osobowych (ustanowiony, kompletny, działający)

PBI – główny dokument w SZBI

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.

- Procedury;
- Regulaminy;
- Instrukcje.

PBI c.d.

Kluczowym dokumentem SZBI jest **Polityka Bezpieczeństwa Informacji (PBI)**, która zawiera:

- wyrażoną przez kierownictwo deklarację stosowania zabezpieczeń,
- opisuje organizację i **ustala osoby** odpowiedzialne oraz ich zakresy odpowiedzialności,
- wprowadza klasyfikację informacji i sposób postępowania z poszczególnymi rodzajami informacji.

PBI jest dokumentem nadrzędnym nad innymi politykami i procedurami

PBI c.d.

W ramach SZBI funkcjonują inne polityki, instrukcja, regulaminy i procedury np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.

Inne regulacje wewnętrzne stanowiące dokumenty wykonawcze PBI to przykładowo:

- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;

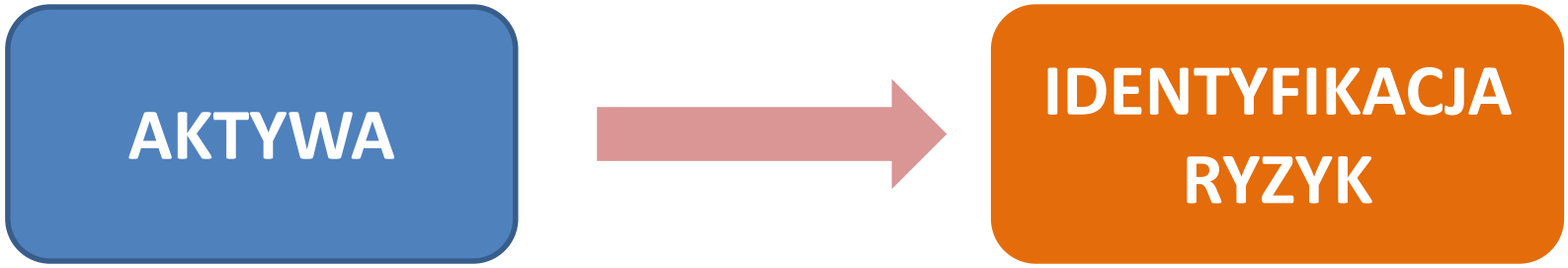
PBI c.d.

- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- **Procedura stosowania środków kryptograficznych;**
- **Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;**
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- **Procedura wykonywania i testowania kopii bezpieczeństwa;**
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych;
- Procedura zachowania ciągłości działania.

PAMIĘTAĆ O CYKLICZNYM SPRAWDZANIU PROCEDUR, INSTRUKCJI, REGULAMINÓW ITP.

Rejestr ryzyk

Badane rejestry ryzyk nie odpowiadały w pełni potrzebom PBI, gdyż zawierały głównie ryzyka dotyczące zadań planowanych na potrzeby kontroli zarządczej. Rejestry często nie uwzględniały szeregu istotnych ryzyk informatycznych związanych z ochroną BI, np. ryzyka pożaru serwerowni, ryzyka włamania do systemu teleinformatycznego itp.



Okresowe audyty PBI - raz do roku

Regulacje wewnętrzne Urzędu **nie określały zasad przeprowadzenia okresowych przeglądów systemu bezpieczeństwa informacji**, w tym wykonywania **corocznych audytów** w zakresie bezpieczeństwa informacji. Również w praktyce najczęściej nie występowały takie sprawdzenia.

Obowiązek wynika z § 20 ust. 2 pkt 14 KRI

Uprawnienia pracowników

Nie zawsze była przestrzegana **zasada minimalnych uprawnień** pozwalających na wykonanie powierzonych zadań. Ponadto w badanych systemach nie były podejmowane niezwłocznie działania wyrejestrowujące użytkownika z systemu informatycznego w takich przypadkach jak: **rozwiązanie umowy, utrata upoważnienia do przetwarzania danych osobowych, zmiana zakresu obowiązków**.

Pamiętać: cykliczne przeglądy uprawnień

Szkolenia pracowników

Należy pamiętać aby **szkolenia** wewnętrzne lub zewnętrzne obejmowały tematykę nie tylko z zakresu ochrony danych osobowych ale również z **zakresu bezpieczeństwa informacji**.

Zapisy w umowach z firmami zewnętrznymi

Service Level Agreement, SLA (pol. **umowa o gwarantowanym poziomie świadczenia usług**) – umowa utrzymania i systematycznego poprawiania ustalonego między klientem a usługodawcą poziomu jakości usług.

Powierzenie przetwarzania danych osobowych firmom zewnętrznym.

Klauzule społeczne – prawo zamówień publicznych

Urządzenia mobilne

Ważne jest opisanie zasad określających sposoby **zabezpieczenia urządzeń mobilnych i danych w nich zawartych** przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także **zasady korzystania z ogólnodostępnych sieci**. W celu podniesienia bezpieczeństwa danych gromadzonych na urządzeniach mobilnych dobrą praktyką jest **szyfrowanie dysków tych urządzeń**.

A co z telefonami komórkowymi?

Inwentaryzacja sprzętu i oprogramowania

Należy wykorzystać oprogramowanie do **automatycznej inwentaryzacji (audytu) sprzętu i oprogramowania**. Nie jest ono tożsame z rejestrem księgowym. W praktyce chodzi o zapewnienie funkcjonowania rejestru zasobów teleinformatycznych, zwanych bazą konfiguracji CMDB. Czyli utrwalenie stanu dla innych osób, tak aby obejmował on bazę licencji, konfiguracji urządzeń sieciowych, historię, aktualizacje.

Zachowanie ciągłości działania

Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego.

To również konfiguracja urządzeń sieciowych. Warto zastanowić się nad wirtualizacją serwerów.

Nie zapominać o testowaniu wykonywanych kopii zapasowych (bezpieczeństwa) i czasie ich odtworzenia.

Przechowywanie kopii w innej lokalizacji.

Zapewnienie rozliczalności

Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, **kto, kiedy i co wykonał w systemie teleinformatycznym**.

Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń, a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych).

Należy również systematycznie przeglądać dzienniki oraz przechowywać je co najmniej 2 lata.

Szkolenia dla kadry IT

Braki specjalistycznych szkoleń dla kadry informatycznej co w konsekwencji skutkowało:

- nie wykorzystaniem pełnych możliwości konfigurowanych urządzeń,
- brakiem wdrożenia nowych rozwiązań (np. AD),
- unikaniem sprawdzeń ustawień skonfigurowanych w przeszłości urządzeń i systemów na zasadzie **„jak działa to nie ruszam”**,
- nadmiernemu ufaniu firmom zewnętrznym bez zadbania o wpisy w umowie chroniące przetwarzane przez nich informacje.

Automatyzacja zadań

- Kamera zamiast rejestru wejść do serwerowni;
- System monitorujący warunki środowiskowe z modułem otwarcia drzwi;
- Systemy do automatycznego audytu sprzętu i oprogramowania;
- W dużych jednostkach zasadnym jest wdrożenie systemu typu Help Desk.

Bezpieczeństwo w systemach teleinformatycznych - § 20 ust. 2 pkt 12 KRI

- dbałości o aktualizację oprogramowania;
- minimalizowaniu ryzyka utraty informacji w wyniku awarii;
- ochronie przed błędami, utratą, nieuprawnioną modyfikacją;
- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa;
- zapewnieniu bezpieczeństwa plików systemowych;

Bezpieczeństwo w systemach teleinformatycznych - § 20 ust. 2 pkt 12 KRI

- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

Organizacja pracy

- Serwerownia to nie „składzik” – tam są najważniejsze dane jednostki;
- W dokumentacji nie należy umieszczać informacji o producencie i modelu zastosowanych urządzeń składowych sieci Urzędu;
- W przypadku administrowania infrastrukturą informatyczną w innych pomieszczeniach niż serwerownia należy pamiętać o podwyższonych zasadach bezpieczeństwa fizycznego i środowiskowego;
- Nie chwalić się serwerownią – tabliczka informacyjna na drzwiach.

Aż tak źle nie jest

Warto zaglądnąć

Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych

http://mc.bip.gov.pl/ -> Kontrole Ministerstwa Cyfryzacji -> Wytyczne

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:

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