Opracowanie z cyklu „Polskie przepisy a COBIT®”

Podstawowe pytania o bezpieczeństwo informacji i cyberbezpieczeństwo w jednostkach sektora finansów publicznych

Czerwiec 2016

Opracowali:
Joanna Karczewska
Małgorzata Michniewicz
Adam Mizerski
Adam Rafajeński
Łukasz Wilkosz

„Bezpieczeństwo informacji ma na celu ochronę interesów osób, które polegają na tych informacjach oraz systemów i środków komunikacji dostarczających te informacje przed brakiem dostępności oraz naruszeniem ich poufności i integralności."
COBIT® Security Baseline

WPROWADZENIE

Niniejsze opracowanie zostało przygotowane przez członków stowarzyszenia ISACA[1] w składzie: Joanna Karczewska, Małgorzata Michniewicz, Adam Mizerski, Adam Rafajeński i Łukasz Wilkosz.

Opracowanie zawiera listę podstawowych pytań, które kierownictwo powinno regularnie zadawać, by uzyskać informacje o stanie bezpieczeństwa teleinformatycznego w swojej jednostce i spełnianiu minimalnych wymagań dla systemów teleinformatycznych wymienionych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r., poz. 526).

Opracowanie jest przeznaczone przede wszystkim dla kierowników jednostek administracji rządowej, organów władzy ustawodawczej, władzy sądowniczej i samorządu terytorialnego.

Z opracowania mogą także korzystać:
- osoby odpowiedzialne w jednostkach za bezpieczeństwo informacji i cyberbezpieczeństwo,
- administratorzy odpowiadający za poszczególne systemy teleinformatyczne wdrożone w jednostkach,
- użytkownicy wewnętrzni i zewnętrzni systemów teleinformatycznych wdrożonych w jednostkach,
- audytorzy wewnętrzni jednostek.

PYTANIA, KTÓRE KIEROWNICTWO POWINNO ZADAWAĆ

Oceniając stopień zapewnienia bezpieczeństwa teleinformatycznego w jednostce, kierownik jednostki powinien **regularnie** zadawać konkretne pytania osobom odpowiedzialnym za poszczególne obszary bezpieczeństwa informacji. Uzyskane odpowiedzi pomogą ustalić, czy:
- są znane i stosowane wymagania zawarte w stosownych przepisach prawa;
- są osiągane i przestrzegane przyjęte przez jednostkę założenia dotyczące bezpieczeństwa informacji,
- ryzyko związane ze stosowaniem technologii informatycznych pozostaje na akceptowalnym poziomie.

Mogą także stanowić podstawę do wypracowania jednakowego rozumienia oczekiwanych korzyści oraz alokacji zasobów i optymalizacji działań.

Niniejsza tabela zawiera podstawowy zestaw pytań, które kierownik jednostki może zadać **– każda negatywna lub niepełna odpowiedź powinna wzbudzić zaniepokojenie.**

[1] Międzynarodowe stowarzyszenie ISACA liczy ponad 140 000 członków i sympatyków, którzy mieszkają i pracują w ponad 180 krajach. Opublikowało uznaną na całym świecie metodykę COBIT nadzoru nad technologiami informatycznymi i ich zarządzania. Zajmuje się certyfikacją CISA, CISM, CGEIT, CRISC. W Polsce są dwa afiliowane oddziały ISACA: ISACA Warszawa i ISACA Katowice.

Pytanie zasadnicze	Pytania uzupełniające
System zarządzania bezpieczeństwem informacji (SZBI)	
1. Czy nasza jednostka podjęła kroki w celu zapewnienia bezpieczeństwa informacji ?	Jeżeli tak, to: - czy konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji naszej jednostki (jeżeli taka strategia została przyjęta) ? - czy zidentyfikowano cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich realizację ? - jakie działania w zakresie bezpieczeństwa informacji podjęto w roku bieżącym ?
2. Czy wiadomo, jakie przepisy prawa dotyczące bezpieczeństwa informacji mają zastosowanie w naszej jednostce (nie tylko Ustawa o ochronie danych osobowych) ?	Jeżeli tak, to: - kto odpowiada za monitorowanie zmian przepisów i informowanie o tych zmianach ?
3. Czy nasza jednostka opracowała i przyjęła kompleksową Politykę bezpieczeństwa informacji (PBI) ?	Jeżeli tak, to: - czy została opracowana w oparciu o właściwe standardy i dobre praktyki ? - kiedy przeprowadzono ostatni przegląd PBI naszej jednostki ? <u>Komentarz</u>: Standardy i dobre praktyki powinny obejmować m.in.: - normy wymienione w Rozporządzeniu w sprawie KRI, - dobre praktyki z zakresu bezpieczeństwa portali internetowych, przygotowane przez Zespół zadaniowy do spraw ochrony portali rządowych we współpracy z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL, - dobre praktyki zarządcze nadzoru nad technologiami informatycznymi podmiotu i zarządzania nimi zawarte w metodyce COBIT. Przeglądy PBI powinny być przeprowadzane nie rzadziej niż raz do roku w celu weryfikacji jej zawartości i aktualności.
Identyfikacja aktywów	
4. Czy zidentyfikowano **kluczowe** aktywa informacyjne (zbiory danych / systemy / usługi) naszej jednostki, które należy chronić ?	Jeżeli tak, to: - jakie są to aktywa ? - czy te aktywa zostały uwzględnione w rejestrze ryzyk jednostki ? <u>Komentarz</u>: Proces identyfikacji aktywów należy

Pytanie zasadnicze	Pytania uzupełniające
	powtarzać co najmniej raz do roku w celu weryfikacji ich aktualności.
Szacowanie ryzyka	
5. Czy dokonuje się szacowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji w naszej jednostce?	Jeżeli tak, to: - czy analiza ryzyka zawiera: · opisy ryzyk, zagrożeń i słabych punktów zdiagnozowanych dla poszczególnych systemów teleinformatycznych wdrożonych w jednostce ? · jakie działania podjęto w zakresie postępowania z ryzykiem w celu jego obniżenia do akceptowalnego poziomu ? - czy analiza ryzyka obejmuje także projekty oraz istotne zmiany informatyczne przygotowywane do wdrożenia ? Komentarz: Do analizy ryzyka należy wykorzystywać uznane standardy, np.: PN-ISO/IEC 27005:2014-01, PN-ISO/IEC 31000:2012, Risk IT Framework for Management of IT Related Business Risks, M_o_R® (Management of Risk), COBIT® 5 for Risk oraz „Katalog zagrożeń CERT.GOV.PL” dotyczący cyberprzestrzeni.
Testowanie i monitorowanie bezpieczeństwa	
6. Czy prowadzone jest jakiekolwiek monitorowanie bezpieczeństwa teleinformatycznego naszej jednostki ?	Jeżeli tak, to: - w jaki sposób jest ono prowadzone ? - czy monitorowanie jest ciągłe, czyli przez 24 godziny przez 7 dni w tygodniu i 365 dni w roku ? - czy komórki bezpieczeństwa otrzymują i analizują raporty bezpieczeństwa, z jaką częstotliwością ? - czy wyniki monitoringu bezpieczeństwa są regularnie (np. kwartalnie) przekazywane do osób zarządzających jednostką ?
7. Czy w naszej jednostce są przeprowadzane audyty bezpieczeństwa informacji ?	Jeżeli tak, to: - kiedy został przeprowadzony ostatni audyt bezpieczeństwa informacji ? - czy przy opracowywaniu planów audytu brane są pod uwagę wyniki analizy ryzyka oraz wnioski z poprzednich audytów ? Komentarz: Audyty powinny być przeprowadzane nie rzadziej niż raz do roku.
Zarządzanie incydentami	
8. Czy jest opracowana procedura	Jeżeli tak, to:

Pytanie zasadnicze	Pytania uzupełniające
zgłaszania incydentów ?	- w jaki sposób można zgłaszać incydenty ? <u>Komentarz</u>: Procedura powinna być ogólnie dostępna i określać różne sposoby zgłaszania incydentów (poczta elektroniczna, telefon, inne) przez wewnętrznych i zewnętrznych użytkowników systemów teleinformatycznych jednostki.
9. Czy jest prowadzony <u>jeden</u> rejestr <u>wszystkich</u> zgłaszanych incydentów ?	Jeżeli tak, to: - czy rejestr zawiera informacje m.in. o rodzaju i klasyfikacji incydentów oraz sposobie obsługi ? <u>Komentarz</u>: Klasyfikacja incydentów powinna określać: - które incydenty są najbardziej znaczące – należy się nimi zająć w pierwszej kolejności, - o których incydentach kierownictwo powinno być natychmiast informowane. Rejestr należy wykorzystać do analizy przyczyn wystąpienia incydentów i proponowania ulepszeń w zapewnieniu bezpieczeństwa informacji. Za wysoce niepokojący należy uznać fakt braku odnotowania w rejestrze jakiegokolwiek incydentu bezpieczeństwa w okresie ostatnich 3 miesięcy, ponieważ: „Incydent bezpieczeństwa jest rzeczą pewną. Prawdopodobieństwo dotyczy tego, kiedy nastąpi …”
Testowanie ciągłości działania	
10. Czy dla zidentyfikowanych kluczowych aktywów przygotowane zostały plany funkcjonowania / scenariusze postępowania naszej jednostki w przypadku niedostępności tych aktywów ?	Jeżeli tak, to: - czy plany są regularnie testowane ? <u>Komentarz</u>: Testy planów powinny być przeprowadzane przynajmniej raz do roku w celu weryfikacji ich zawartości i aktualności. W testy powinni być zaangażowani także dostawcy zewnętrzni, którzy obsługują kluczowe zasoby / usługi.
Szkolenia i uświadamianie	
11. Czy w naszej jednostce są prowadzone szkolenia lub działania uświadamiające dla pracowników dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa ?	Jeżeli tak, to: - kiedy odbyło się ostatnie szkolenie ? - czy szkolenia odbywają się regularnie ? - czy wszyscy pracownicy oraz dostawcy zostali przeszkoleni? - jakie podjęto inne działania uświadamiające (biuletyny, ogłoszenia ..) ?

Pytanie zasadnicze	Pytania uzupełniające
	Komentarz: Kierownictwo także powinno uczestniczyć w tych szkoleniach.
Współpraca z dostawcami	
12. Czy nasza jednostka korzysta z dostawców usług i systemów informatycznych ?	Jeżeli tak, to: - jakie są zapisy w umowach, by zostały spełnione wymagania prawne i formalne w zakresie bezpieczeństwa informacji i ciągłości działania ? Komentarz: W umowach należy zastrzec – dla osób upoważnionych przez jednostkę: - prawo dostępu (czyli do wizyty w siedzibie dostawcy lub innym miejscu, gdzie są serwery i inne zasoby teleinformatyczne obsługujące naszą jednostkę), - prawo do audytu.

ROLE I ODPOWIEDZIALNOŚCI W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

Zaleca się opracowanie tabeli przedstawiającej cele i zadania związane z zapewnieniem bezpieczeństwa informacji i cyberbezpieczeństwa w jednostce wraz ze wskazaniem stopnia odpowiedzialności:

R – **Odpowiedzialna** [Responsible] - osoba, która wykonuje dane zadanie;

A – **Rozliczana** [Accountable] – osoba decyzyjna, która ma uprawnienia do zatwierdzenia lub akceptacji wykonania danego zadania;

C – **Konsultowana** [Consulted] - osoba, u której zasięga się opinii w sprawie danego zadania (komunikacja w obie strony);

I – **Informowana** [Informed] - osoba, którą się informuje o postępie danego zadania (komunikacja w jedną stronę).

Dla każdego zadania należy wyznaczyć osobę rozliczaną (**A**) za zatwierdzenie lub akceptację wykonania tego zadania.

Jednostka powinna opracować własną tabelę ról (stanowisk) i odpowiedzialności zgodną ze strukturą organizacyjną, regulaminem pracy, zakresami obowiązków pracowników, wewnętrznymi politykami i procedurami oraz umowami podpisanymi z dostawcami. Wyznaczone role i odpowiedzialności powinny odpowiadać zapisom Polityki bezpieczeństwa informacji jednostki.

Rola (Stanowisko) **Cel i zadanie**	Kierownik jednostki	Kierownik działu merytorycznego	Kierownik Wydziału Informatycznego	Administrator systemu teleinformatycznego	Audytor	Użytkownik wewnętrzny	Użytkownik zewnętrzny	Dostawca usługi informatycznej	Dostawca systemu teleinformatycznego	Dostawca usług telekomunikacyjnych
1. Stworzenie i stosowanie systemu zarządzania bezpieczeństwem informacji										
2. Identyfikacja aktywów, podsystemów, funkcji i zależności od innych systemów istotnych z punktu widzenia funkcjonowania jednostki										
3. Szacowanie ryzyka związanego z bezpieczeństwem informacji										
4. Testowanie i monitorowanie bezpieczeństwa informacji i cyberbezpieczeństwa										
5. Wdrożenie mechanizmów służących właściwemu postępowaniu w przypadku wystąpienia incydentu										
6. Testowanie ciągłości działania										
7. Kształcenie, szkolenia i uświadamianie w kwestiach dotyczących bezpieczeństwa informacji										
8. Współpraca z dostawcami usług i systemów teleinformatycznych										

LITERATURA

W trakcie pracy nad dokumentem autorzy korzystali z następujących zbiorów dobrych praktyk:

Publikacje ISACA w języku angielskim

- COBIT® 5 - A Business Framework for the Governance and Management of Enterprise IT
- COBIT® 5: Enabling Processes
- COBIT® 5: Enabling Information
- COBIT® 5 Implementation
- COBIT® 5 for Assurance
- COBIT® 5 for Risk
- COBIT® 5 for Information Security

Publikacje ISACA w języku polskim

- COBIT 5 Polski (Polish)
- COBIT 5 Enabling Information Polski (Polish)
- COBIT 5 for Risk Polski (Polish)
- COBIT 5 Information Security Polski (Polish)

dostępne na stronie www.isaca.org

Publikacje Polskiego Komitetu Normalizacyjnego

- PN-ISO/IEC 27001:2014-12 - "Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania"
- PN-ISO/IEC 17799:2007 - "Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zarządzania bezpieczeństwem informacji"
- PN-ISO/IEC 27005:2014-01 - "Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji"
- PN-ISO/IEC 24762:2010 - "Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie"