Wiadomości Statystyczne. The Polish Statistician, 2022, vol. 67, 6, 65–68
Dyskusje. Recenzje. Informacje / Discussions. Reviews. Information

Projekt „Wdrożenie Kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji – KSZBI dla statystyki publicznej"

Project 'Implementation of a Comprehensive Information Security Management System'

Jedni mówią, że dane są niczym paliwo, inni, że są złotem XXI wieku – surowcem, na którym w coraz większym stopniu budowane są nasze gospodarki, społeczeństwa i demokracje.

Joe Kaeser (2022)

Dostęp do informacji i możliwość wykorzystywania uzyskanych danych przez sektory publiczny i prywatny, placówki naukowe i badawcze oraz instytucje krajowe i międzynarodowe jest kluczowy dla ich funkcjonowania i rozwoju. Zapewnienie dostępu do informacji należy do priorytetowych zadań służb statystyki publicznej, które zbierają, gromadzą, przechowują, opracowują, łączą i wtórnie wykorzystują dane pochodzące od podmiotów gospodarki narodowej i dotyczące tych podmiotów, w tym ich działalności, a także dane od osób fizycznych i dotyczące tych osób, ich życia i sytuacji, oraz dane na temat zjawisk, zdarzeń i obiektów (zgodnie z art. 5 ust. 1 Ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej). Wyniki badań prowadzonych przez pracowników służb statystyki publicznej dostarczają rzetelnych i obiektywnych informacji o sytuacji ekonomicznej, demograficznej i społecznej oraz o środowisku naturalnym. Wynikowe dane statystyczne są uwzględniane przy podejmowaniu strategicznych decyzji na różnych szczeblach administracji rządowej i samorządowej oraz w biznesie, a także służą obywatelom aktywnie uczestniczącym w życiu społeczno-gospodarczym kraju, dlatego ich jakość i dostępność są bardzo ważne.

Należy zauważyć, że „informacja jest narażona na utratę dostępności, integralności i poufności w wyniku oddziaływań pochodzących z różnych źródeł, w tym działań zamierzonych, polegających na dystrybucji szkodliwego oprogramowania, włamaniach do systemów teleinformatycznych i blokowaniu możliwości świadczenia usług" (*Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, s. 4). Dlatego proces realizacji badań statystycznych podlega bardzo rygorystycznym zasadom wypracowanym na poziomie krajowym i międzynarodowym, które pozwalają zapewnić wysoką jakość i wiarygodność danych oraz ich bezpieczeństwo w całym procesie ich przetwarzania. Statystyka publiczna przywiązuje

szczególną wagę do kwestii poufności danych oraz bezpieczeństwa systemów, w których dane te są przetwarzane. Borowiecki i Kwieciński (2003, s. 46) zwracają przy tym uwagę, że „bezpieczeństwa systemów informacyjnych nie należy traktować jako jednorazowego przedsięwzięcia, ale jako proces, który powinien być modyfikowany wraz z pojawiającymi się zmianami w otoczeniu wewnętrznym i zewnętrznym organizacji". Kwestie dotyczące bezpieczeństwa są więc bezwzględnym wymogiem funkcjonowania statystyki publicznej. Podstawowe znaczenie ma w tym zakresie Europejski kodeks praktyk statystycznych (European Statistics Code of Practice), który zawiera 16 zasad dotyczących środowiska instytucjonalnego, procesów statystycznych i wyników badań. W przypadku zasady odnoszącej się do poufności statystyk i ochrony danych wskazano, że „bezwzględnie gwarantuje się prywatność dostawców danych, poufność informacji przez nich przekazywanych, wykorzystanie tych informacji wyłącznie do celów statystycznych, a także bezpieczeństwo danych". Bezpieczeństwo w statystyce publicznej jest rozumiane szeroko, ponieważ dotyczy zapewnienia zarówno poufności przetwarzanych informacji, jak i ich dostępności oraz integralności.

Procesy gromadzenia, przetwarzania i analizy danych oraz udostępniania informacji wynikowych wymagają innowacyjnych, niestandardowych działań ze względu na zmieniającą się rzeczywistość i oczekiwania użytkowników. Statystyka publiczna wdraża usprawnienia, nowe technologie i rozwiązania, które pozwalają wykonywać zadania szybciej, efektywniej i przede wszystkim bezpieczniej.

Odpowiedzią na zachodzące zmiany oraz potrzeby dotyczące zwiększenia poziomu dostępności i efektywności bezpiecznych usług świadczonych przez statystykę publiczną na rzecz obywateli i podmiotów gospodarki narodowej oraz administracji publicznej był realizowany w Głównym Urzędzie Statystycznym projekt „Wdrożenie Kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji – KSZBI dla statystyki publicznej" (dalej jako projekt KSZBI), współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014–2020, Oś Priorytetowa nr II „E-administracja i otwarty rząd", Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej". Miał on na celu zapewnienie wzrostu efektywności pracy służb statystyki publicznej w zakresie bezpieczeństwa informacji, wdrożenie i rozwój procesów biznesowych organizacji oraz wyposażenie służb statystyki publicznej w narzędzia i mechanizmy pozwalające nie tylko na poprawę współpracy z respondentami i właścicielami rejestrów administracyjnych i pozaadministracyjnych, lecz także na zwiększenie bezpieczeństwa informacji. Tego typu działania pozytywnie wpływają na wizerunek statystyki publicznej na arenie krajowej i międzynarodowej.

Efektem projektu KSZBI jest większy poziom bezpieczeństwa użytkowanych urządzeń, systemów i oprogramowań. Systemy i urządzenia zapewniające bezpie-

czeństwo zostały rozbudowane i uzupełnione o nowe komponenty techniczne i organizacyjne, które zapewniają zaawansowaną ochronę przed złośliwym oprogramowaniem i pozwalają analizować aktywność użytkowników w kluczowych aplikacjach internetowych, a dzięki temu chronić te aplikacje i dane przed cyberatakami, oraz umożliwiają bezpieczne unieszkodliwienie potencjalnie szkodliwego kodu i przeprowadzanie kontrolowanej analizy zagrożeń w obszarze odseparowanym od środowisk produkcyjnych. Wdrożone rozwiązania zapewniają także zaawansowaną ochronę stacji roboczych, umożliwiając szybsze wykrywanie ataków, identyfikację zagrożeń, priorytetyzację alertów o systemach wymagających pilnej reakcji oraz przywracanie sprawności i usuwanie skutków ataku. Wprowadzone mechanizmy pozwalają na analizę alarmów generowanych przez sprzęt sieciowy, systemy i aplikacje w czasie rzeczywistym oraz monitorowanie infrastruktury teleinformatycznej, analizę zdarzeń, detekcję zagrożeń bezpieczeństwa i reagowanie na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne za pomocą analizy logo z urządzeń, systemów IT oraz aplikacj. Umożliwiają też korelację zdarzeń i detekcję zagrożeń oraz odpowiednią reakcję na incydenty.

W ramach działań projektowych dokonano przeglądów i audytów systemów zarządzania bezpieczeństwem informacji (SZBI) funkcjonujących w jednostkach służb statystyki publicznej, a także opracowano dokumenty SZBI, dotyczące procesów, procedur, instrukcji i wytycznych oraz rekomendacji. Dokumentacja SZBI spełnia wymagania wynikające z Rozporządzenia 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 i normy PN-ISO/IEC 27001 oraz uwzględnia zapisy norm PN-ISO/IEC 27002, PN-ISO/IEC 27017, PN-ISO/IEC 22301 i PN-ISO/IEC 27005. Po audycie SZBI, przeprowadzonym przez firmę zewnętrzną, dokumentacja została zaktualizowana.

Projekt KSZBI – poza rozbudową systemów teleinformatycznych oraz opracowaniem dokumentów tworzących SZBI – obejmował również działania edukacyjno-informacyjne, służące poszerzeniu kompetencji zarówno kadry zajmującej się bezpieczeństwem teleinformatycznym, jak i pozostałych pracowników służb statystyki publicznej, co przekłada się na poprawę skuteczności procesów ochrony i bezpieczeństwa informacji. Działania edukacyjno-informacyjne skierowane są także do obywateli, przedsiębiorców i pracowników instytucji publicznych, którzy mają dostęp do materiałów informacyjnych dotyczących bezpieczeństwa informacji w statystyce publicznej, w tym ochrony danych osobowych.

Odpowiednio chronione zasoby, doświadczona i zaangażowana kadra pracowników, ustalone metodologie badawcze i właściwe relacje z interesariuszami zewnętrznymi przyczyniają się do zwiększania bezpieczeństwa i dbałości o to, aby informacje

powierzone statystyce publicznej były należycie chronione. Dzięki temu buduje ona swoją wiarygodność.

Bibliografia

Borowiecki, R., Kwieciński, M. (red.). (2003). *Monitorowanie otoczenia. Przepływ i bezpieczeństwo informacji. W stronę inteligencji przedsiębiorstwa*. Kantor Wydawniczy Zakamycze.

Europejski kodeks praktyk statystycznych dla krajowych organów statystycznych i Eurostatu (organu statystycznego UE) przyjęty przez Komitet ds. Europejskiego Systemu Statystycznego 16 listopada 2017 r.

Kaeser, J. (2022, 9 maja). *Data is the 21st century's oil, says Siemens CEO Joe Kaeser*. https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms?msclkid=567422decfa811ec8f6da4afd26cf36f.

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. 2012 poz. 526).

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz.U. 1995 nr 88, poz. 439).

Anna Długosz, Mariola Wiatrowska, Joanna Gajowska
Główny Urząd Statystyczny, Departament Systemów Teleinformatycznych, Geostatystyki i Spisów / Statistics Poland, ICT Systems, Geostatistics and Census Department

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
GUS
Unia Europejska Europejski Fundusz Rozwoju Regionalnego