Załącznik do pisma znak: COA.WK.588.1.2019.MF

Informacja o najważniejszych i najczęściej powtarzających się nieprawidłowościach stwierdzonych w wyniku kontroli przeprowadzonych przez KPRM w zakresie *wykorzystania systemów teleinformatycznych do realizacji zadań publicznych*

I. System zarządzania bezpieczeństwem informacji

1. **[Regulacje wewnętrzne w obszarze bezpieczeństwa informacji]** Zgodnie z przepisami[1], podmiot realizujący zadania publiczne powinien opracować i ustanowić, wdrożyć i eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić system zarządzania bezpieczeństwem informacji (dalej: *SZBI*) zapewniający poufność, dostępność i integralność informacji, z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Wymaga to opracowania dokumentacji *SZBI*, w tym szeregu **regulacji wewnętrznych** oraz **zapewnienia ich aktualizacji** w zakresie zmieniającego się otoczenia. Wskazać należy, że *SZBI* dotyczy **wszystkich użytkowników** przetwarzających informacje, nie tylko administratorów systemów, dlatego ważne jest opracowanie **kompleksowej dokumentacji *SZBI***, która wspomoże użytkowników w prawidłowej realizacji zadań z zakresu bezpieczeństwa informacji, a w przypadku ich nierealizowania bądź nienależytego realizowania, zabezpieczy interesy jednostki oraz umożliwi zidentyfikowanie słabych punktów i osób odpowiedzialnych.

Należy podkreślić, że opracowanie dokumentacji we wszystkich obszarach *SZBI*, z uwzględnieniem zadań i odpowiedzialności użytkowników, jest niezbędnym warunkiem skutecznego zarządzania bezpieczeństwem informacji w podmiocie. W powyższym zakresie najczęstszą nieprawidłowością **było wdrożenie w jednostkach *Polityk bezpieczeństwa informacji*, które nie obejmowały większości istotnych zagadnień w zakresie bezpieczeństwa informacji**, m.in.:

- zasad prowadzenia rejestru aktywów informacyjnych;
- przeprowadzania okresowych analiz ryzyka;
- zapewnienia cyklicznych szkoleń dla osób zaangażowanych w proces przetwarzania informacji;
- zasad zarządzania incydentami;
- zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- zagadnień związanych z projektowaniem, budową, wdrażaniem systemów oraz ich monitorowaniem, a także związanych z wewnętrznym audytem bezpieczeństwa informacji oraz rozliczalnością działań w systemach.

Należy zauważyć, że brak części sformalizowanych zasad i procedur w tym obszarze może przyczynić się do nieskutecznej identyfikacji nieprawidłowości, a w konsekwencji do braku podejmowania niezbędnych działań korygujących. Bezpieczeństwo informacji w bardzo dużym stopniu uzależnione jest od samych użytkowników (pracowników), poziomu ich świadomości i wiedzy. Z tego powodu tak ważne jest precyzyjne określenie wymagań w tym zakresie w regulacjach wewnętrznych.

[1] § 20 ust. 1 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 (Dz. U. z 2017 r. poz. 2247 t. j.), dalej: *Rozporządzenie KRI*.

2. **[Przegląd *SZBI*]** Działania w ramach *SZBI* powinny być podejmowane w sposób ciągły i tym samym system powinien być stale doskonalony. W związku z tym konieczne jest jego monitorowanie i poddawanie **cyklicznym przeglądom**, w celu zdiagnozowania obszarów wymagających usprawnienia, co z kolei powinno znaleźć odzwierciedlenie w dokumentacji systemu.

W jednostkach objętych badaniem ww. zakresie stwierdzono nieprawidłowości polegające na:

- nieprowadzeniu regularnych i sformalizowanych przeglądów *SZBI* lub nierealizowaniu ich w zakresie całego *SZBI,* a jedynie w wybranym przedmiocie, np. w odniesieniu do systemu bezpieczeństwa danych osobowych;
- nierzetelnym wykonaniu *Przeglądu SZBI*, tj. dokumenty stanowiące podstawę do jego przeprowadzenia (np. wyniki audytu wewnętrznego, analiza ryzyka oraz rejestr incydentów) nie stanowiły wiarygodnego źródła informacji albo ich nie opracowano. Tym samym *SZBI* nie był doskonalony.

3. **[Audyt wewnętrzny w obszarze bezpieczeństwa informacji]** Kolejnym istotnym narzędziem zarządczym dostarczającym niezbędnej wiedzy o stanie *SZBI* i pozwalającym na **identyfikowanie potencjalnych słabości** lub **zagrożeń** w systemie bezpieczeństwa informacji jest audyt wewnętrzny. Ustalono, że narzędzie to nie było efektywnie wykorzystywane, bowiem w jednostkach:

- nie przeprowadzano corocznego obowiązkowego audytu wewnętrznego bądź ograniczano jego zakres wyłącznie do środków technicznych i organizacyjnych zabezpieczających aktywa informacyjne jednostki;
- zalecenia po realizacji audytu nie były wykonywane albo wykonywano je z dużym opóźnieniem i nie spełniały określonych wymogów;
- regulacje wewnętrzne jednostek nie określały obowiązku corocznego przeprowadzania audytu wewnętrznego oraz zasad jego prowadzenia.

4. **[Aktywa informatyczne]** Skuteczne zarządzanie infrastrukturą informatyczną wymaga posiadania **aktualnej inwentaryzacji sprzętu i oprogramowania**, obejmującego ich rodzaj i konfigurację (bazy konfiguracji CMDB). Posiadanie takich informacji jest niezbędne przy wprowadzaniu wszelkich zmian w środowisku informatycznym. Jednocześnie należy podkreślić, że ww. baza **nie jest tożsama** z zapisami księgi inwentarzowej. Zawiera ona bowiem, w szczególności informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. W większości jednostek stwierdzono, że:

- nie prowadzono aktualnej i kompletnej inwentaryzacji aktywów informatycznych;
- nie zostały opracowane procedury zarządzania sprzętem i oprogramowaniem;
- nie przestrzegano wewnętrznych regulacji ww. zakresie.

Wyjaśnić należy, że brak pełnej, aktualnej informacji o stanie aktywów **uniemożliwia przeprowadzanie rzetelnej analizy ryzyka** i **przygotowanie pełnego planu postępowania z ryzykiem**. W konsekwencji jednostki nie posiadają niezbędnej wiedzy pozwalającej efektywnie zarządzać obszarem bezpieczeństwa informacji.

5. **[Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji]** W celu określenia potrzeb organizacji w odniesieniu do wymagań związanych z bezpieczeństwem informacji oraz utworzenia skutecznego *SZBI* niezbędne jest **systematyczne podejście do zarządzania ryzykiem**. Zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było integralną częścią wszystkich działań związanych z tym obszarem oraz zostało zastosowane zarówno

do wdrożenia, jak i w ciągłej eksploatacji *SZBI*[2]. W szczególności przystępując do procesu szacowania ryzyka należy określić **zakres procesu zarządzania ryzykiem**, tak aby zapewnić, że analiza ryzyka uwzględni wszystkie aktywa. Zgodnie z normą PN-ISO/IEC 27000 aktywem jest wszystko, co ma wartość dla organizacji. Istnieje wiele typów aktywów, w tym: aktywa informacyjne, oprogramowanie, takie jak program komputerowy, fizyczne, takie jak komputer, usługi, personel i jego kwalifikacje, umiejętności i doświadczenie oraz wartości niematerialne, takie jak reputacja i wizerunek. Jednostka powinna także określić ryzyka powstające poza nią w wyniku kontaktów z innymi podmiotami/jednostkami[3] (stronami zainteresowanymi[4]). Zauważyć należy, że szybki postęp technologiczny w środowisku informatycznym i pojawianie się nowych ryzyk dla bezpieczeństwa informacji wskazuje, jak ważnym elementem *SZBI* jest **prowadzenie okresowych analiz ryzyka**. Dlatego też minimalnym wymogiem spełniającym warunek przeprowadzenia okresowej analizy ryzyka, powinna być jej realizacja przed wykonaniem corocznego audytu bezpieczeństwa informacji. Pozwoliłoby to bowiem na objęcie audytem w szczególności tych zagadnień, w których ujawniono najwyższe ryzyka wystąpienia zagrożeń.

W zakresie zarządzania ryzykiem stwierdzono nieprawidłowości polegające na nieprowadzeniu systematycznej, okresowej analizy ryzyka bądź jej przeprowadzeniu w niepełnym zakresie, tj. analizy:

- nie odnosiły się do wszystkich aktywów jednostek;
- nie były prowadzone w zakresie utraty integralności, dostępności lub poufności informacji, a prowadzono je w odniesieniu do wybranych przez jednostki atrybutów, np. związanych z wizerunkiem czy utratą klientów.

Finalnym dokumentem procesu zarządzania ryzykiem jest **plan postępowania z ryzykiem**, na który składa się wyszczególnienie ryzyk, celów stosowania zabezpieczeń oraz wskazanie zabezpieczeń. Plan postępowania z ryzykiem jest podstawowym dokumentem wykonawczym do podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy. Jednocześnie, pomimo tak dużej istotności powyższego dokumentu w bezpieczeństwie informacji, żadna skontrolowana jednostka nie dysponowała aktualnym planem postępowania z ryzykiem.

Powyższe nieprawidłowości narażały jednostki na brak zapewnienia wymaganej ochrony aktywów oraz ograniczały możliwości działania jednostki, ponieważ nie stosowano odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk.

6. **[Zarządzanie uprawnieniami]** Kolejnym ważnym elementem bezpieczeństwa informacji jest zarządzanie uprawnieniami. Proces ten ma zapewnić, że osoby zaangażowane w przetwarzanie informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, a w przypadku zmiany/nierealizowania zadań następuje również zmiana/cofnięcie tych uprawnień. W szczególności należy zwrócić uwagę, czy nie dochodzi do sytuacji nadmiernej koncentracji uprawnień i braku nadzoru, w tym „kontrolowania samego siebie". Dlatego też, konieczne jest jasne **określenie kategorii/ról użytkowników** z podziałem ich obowiązków oraz **unikanie konfliktu interesów**.

---

[2] Norma PN-ISO/IEC 27005 *Zarządzanie ryzykiem w bezpieczeństwie informacji*.

[3] Zgodnie z normą PN-ISO/IEC 27005 zaleca się, aby przy określaniu zakresu i granic zarządzania ryzykiem organizacja brała pod uwagę następujące informacje: strategiczne cele biznesowe, strategie i politykę; procesy biznesowe; strukturę i funkcje organizacji; wymagania prawne, wynikające z regulacji oraz umowne, mające zastosowanie do organizacji; stosowaną w organizacji politykę bezpieczeństwa informacji; całościowe podejście organizacji do zarządzania ryzykiem; aktywa informacyjne; lokalizacje organizacji i ich geograficzną charakterystykę; ograniczenia dotyczące organizacji; oczekiwania uczestników; środowisko społeczno-kulturalne; interfejsy (tzn. wymianę informacji ze środowiskiem). Dodatkowo zaleca się, aby organizacja uzasadniła każde wykluczenie z zakresu.

[4] Zgodnie z normą PN-ISO/IEC 27001 wymagania stron zainteresowanych mogą obejmować wymagania prawne i wymagania regulacyjne oraz zobowiązania wynikające z umów.

W kontrolowanych jednostkach stwierdzano nieprawidłowości w zakresie:

- niewprowadzenia zasad dotyczących zarządzania uprawnieniami, w tym dokumentowania nadawania, zmiany i ich odbierania użytkownikom korzystającym z systemów;
- braku określenia jaki dostęp do systemów mają poszczególne kategorie użytkowników;
- nieposiadania przez osoby zaangażowane w proces przetwarzania informacji stosownych uprawnień i uczestniczenia w procesie w stopniu nieadekwatnym do realizowanych zadań oraz obowiązków, tj. powierzono kluczowe role[5] w bezpieczeństwie informacji osobom, które nie były zatrudnione w jednostce, a wykonywały usługi na podstawie umów cywilnoprawnych;
- nieuwzględnienia w umowach cywilnoprawnych postanowień w zakresie realizacji zadań wynikających z *Polityki Bezpieczeństwa Informacji*, funkcjonującej w jednostce;
- nieposiadania przez osoby nadzorujące pracę użytkowników dostępu do systemu, co mogło prowadzić do ograniczenia skutecznego nadzoru nad przetwarzaniem informacji w tym systemie.

Powyższe nieprawidłowości wpłynęły, zatem na obniżenie poziomu ochrony i bezpieczeństwa informacji.

7. **[Szkolenia użytkowników w zakresie bezpieczeństwa IT]** Podnoszenie świadomości w zakresie: zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji, z uwzględnieniem urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich, jest istotnym elementem *SZBI*. Człowiek, jako **część** każdego systemu zarządczego wymaga **szczególnego podejścia** i **zapewnienia ciągłego rozwoju** poprzez system szkoleń. Ważnym elementem, w szczególności z uwagi na zmieniające się zagrożenia bezpieczeństwa informacji i zmieniające się zabezpieczenia, jest ich cykliczność oraz **dostępność dla wszystkich użytkowników** zaangażowanych w proces przetwarzania informacji, a nie tylko dla administratorów systemów.

W wyniku kontroli w jednostkach stwierdzono w tym zakresie następujące nieprawidłowości:

- nie organizowano cyklicznych szkoleń z obszaru bezpieczeństwa informacji bądź organizowano je wyłącznie dla administratorów i pełnomocników bezpieczeństwa informacji;
- nie określono zasad dotyczących zapewnienia wiedzy pracownikom z ww. obszaru;
- nie dokumentowano zapoznania się przez pracowników z *Politykami bezpieczeństwa informacji* i nie wprowadzano obowiązku złożenia oświadczenia o zobowiązaniu się do przestrzegania zasad dotyczących ochrony i bezpieczeństwa informacji. Wskazać należy, że ww. oświadczenia są istotnym elementem dla skutecznego egzekwowania przez pracodawcę odpowiedzialności za naruszenie obowiązków wynikających z regulacji wewnętrznych;
- w ograniczonym zakresie przekazywano wiedzę o nowych zagrożeniach i skutkach wystąpienia incydentów związanych z bezpieczeństwem informacji.

8. **[Zarządzanie incydentami bezpieczeństwa]** Pomimo sporządzenia analizy ryzyka i opracowania planu postępowania z ryzykiem w jednostce, istnieje ryzyko pozostające po zastosowaniu działań określonych w planie postępowania z ryzykiem (ryzyko szczątkowe[6]). W ramach ryzyka szczątkowego oraz niezidentyfikowanych i nieobjętych analizą ryzyk mogą pojawić się incydenty w zakresie naruszenia bezpieczeństwa informacji. Incydenty te, w szczególności powinny być **bezzwłocznie zgłaszane** w określony i z góry ustalony sposób,

[5] Administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych.
[6] Definicja wnikająca z normy PN-ISO/IEC 27005 *Zarządzanie ryzykiem w bezpieczeństwie informacji.*

a także powinien zostać **opisany sposób reakcji** na te incydenty przez wyznaczone osoby, którym szczegółowo powinno określić się zakres zadań i odpowiedzialności. Powyższe ma na celu szybkie podjęcie działań naprawczych. Ponadto rejestr incydentów powinien być **analizowany**, a wyniki analizy powinny wpłynąć na **doskonalenie *SZBI***, w tym w szczególności na **zastosowane zabezpieczenia** określone w planie postępowania z ryzykiem.

W wyniku przeprowadzonych kontroli stwierdzono, że jednostki **nie posiadały formalnych zasad zarządzania incydentami bądź wprowadzone regulacje nie stanowiły kompletnego systemu**, ponieważ nie obejmowały takich zagadnień, jak np.:

- identyfikacja (w tym definicja incydentu), analiza, nadawanie priorytetów, wyszukiwanie powiązań, podejmowanie działań naprawczych, zasady gromadzenia materiału dowodowego dla użytkowników, informacje o ewentualnym postępowaniu dyscyplinarnym dla pracowników, czy też usuwanie przyczyn incydentów;
- precyzyjne określenie w regulacjach zadań i odpowiedzialności dla istotnych ról wskazanych w procesie zarządzania incydentami.

Należy podkreślić, że ustanowienie i wdrożenie prawidłowej procedury zarządzania incydentami, uwzględniającej podział zadań i odpowiedzialności, przejrzyste zasady postępowania w sytuacjach wystąpienia zagrożeń, pozwalające na szybkie podjęcie działań korygujących, jest istotnym narzędziem wpierającym proces doskonalenia *SZBI*.

9. **[Praca na odległość i mobilne przetwarzanie danych]** W związku z możliwością wykonywania pracy na odległość, z wykorzystaniem takich urządzeń jak np. laptopy, tablety, smartfony, pojawiają się nowe zagrożenia bezpieczeństwa informacji. Dlatego ważne jest **opracowanie zasad** wskazujących sposoby zabezpieczenia urządzeń mobilnych i danych na nich przetwarzanych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasad korzystania z ogólnodostępnych sieci. Jednocześnie jednostki powinny określić zakres zadań, które mogą być realizowane poza ich siedzibą oraz wskazać zasady ich wykonywania, bądź zaznaczyć, że ten rodzaj pracy nie jest możliwy.

W tym obszarze stwierdzano nieprawidłowości w zakresie:

- braku opracowania i wdrożenia zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość bądź wprowadzenia regulacji, które nie określały wymagań w zakresie wykonywania tego rodzaju pracy.

10. **[Umowy z wykonawcami]** W przypadku umów cywilnoprawnych z wykonawcami istotne jest zawarcie w ich treści postanowień zabezpieczających w zakresie **właściwego poziomu ochrony i bezpieczeństwa informacji** przez nich uzyskanych. Dodatkowo w umowach serwisowych powinny zostać wskazane również postanowienia zapewniające **odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii**. Czas ten powinien być precyzyjnie określony z uwzględnieniem istotności systemu. Zarówno umowy serwisowe, jak i dotyczące oprogramowania powinny zawierać postanowienia umożliwiające jednostce **przeprowadzenie kontroli podmiotu zewnętrznego** w zakresie przestrzegania bezpieczeństwa informacji.

W wyniku zrealizowanych kontroli stwierdzono, że:

- w umowach serwisowych podpisanych ze stronami trzecimi nie wskazywano postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji, w szczególności nie zawierano obowiązku przestrzegania *Polityki bezpieczeństwa informacji* oraz zasad ochrony, ograniczając się wyłącznie do ogólnych postanowień w zakresie zachowania poufności; postanowień takich nie stosowano również w zawieranych umowach cywilnoprawnych. Było to konsekwencją niewprowadzenia w jednostkach odpowiednich regulacji wewnętrznych w tym zakresie, w szczególności braku ustanowienia katalogu niezbędnych postanowień dotyczących bezpieczeństwa, ochrony i poufności informacji, jakie powinny zostać wprowadzone we wszystkich

umowach cywilnoprawnych oraz w umowach dotyczących współpracy z podmiotami trzecimi w zakresie serwisu i rozwoju sprzętu oraz oprogramowania informatycznego.

Brak właściwych postanowień w umowach nie zabezpieczał należycie interesów jednostek i pozbawiał je możliwości skutecznego dochodzenia odpowiedzialności usługodawcy w przypadku wystąpienia sytuacji stwarzających zagrożenie dla bezpieczeństwa informacji.

- sposób zawierania umów z podmiotami zewnętrznymi w zakresie budowy nowych wersji systemu nie zabezpieczał interesów jednostki oraz nie zapewniał bezpieczeństwa przetwarzanych informacji. Istotną nieprawidłowością było **pominięcie postanowień dotyczących przekazania autorskich praw majątkowych**, w tym w szczególności w zakresie modyfikacji oraz nowych funkcjonalności oprogramowania. W umowach nie określono również terminu, w jakim wykonawca jest zobowiązany do usunięcia zgłaszanych przez pracowników jednostki niezgodności systemu z umowami, kar umownych za niewykonanie lub nienależyte wykonanie umowy, a także osób odpowiedzialnych za realizację umów.

11. [Zarządzanie kopiami zapasowymi] Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Skuteczne zapobieganie utracie przetwarzanych danych wymaga nie tylko tworzenia i przechowywania, ale również regularnego testowania utworzonych kopii zapasowych dla wszystkich systemów. Testowanie jakości kopii powinno odbywać się zgodnie z przyjętymi **zasadami** poprzez odtworzenie systemu na niezależnym sprzętowo środowisku testowym i powinno stanowić istotny **element systemu zapewnienia ciągłości działania**. Jednocześnie ww. działania powinny być **udokumentowane**. W tym obszarze stwierdzono, że:

- w jednostkach nie wprowadzono formalnych zasad testowania kopii zapasowych;
- testowanie kopii odbywało się wyłącznie w zakresie wybranych systemów bądź tylko w przypadku awarii lub błędów w odtworzeniu systemu z zapisanej kopii;
- częstotliwość tworzenia i testowania kopii była niezgodna z wprowadzonymi regulacjami wewnętrznymi.

12. [Plan ciągłości działania] Ważnym elementem *SZBI* jest opracowanie planu ciągłości działania. W planie tym ujmowane są zazwyczaj zdarzenia o niskim prawdopodobieństwie wystąpienia, ale **katastrofalnych skutkach** (np. pożar, powódź, katastrofa budowlana, terroryzm itp.). Tworzenie kopii zapasowych jest istotnym elementem zapewniającym ciągłość działania, jednak użyteczny i skuteczny plan ciągłości działalności obejmować powinien ponadto **zabezpieczenia o charakterze technicznym** oraz **organizacyjnym**. Jednocześnie plany wymagają **testowania** oraz **okresowych przeglądów**, w celu dostosowania do zmian w organizacji oraz zmieniających się zagrożeń.

Przeprowadzone kontrole wykazały, że:

- w większości skontrolowanych jednostek plany ciągłości działania nie zostały opracowane; brak planu ciągłości działania, który uwzględnia szerokie spektrum ryzyk sprawiał, że jednostki narażone były w szczególności na wysokie ryzyko braku kontynuacji działalności w przypadku wystąpienia zdarzeń nadzwyczajnych;
- wdrażane w jednostkach rozwiązania w obszarze zapewnienia ciągłości działania, w tym wprowadzone dokumenty *SZBI* nie zostały poprzedzone analizą ryzyka, która w przypadku planu zapewnienia ciągłości działania jest szczególnie istotna, ponieważ jest to plan tworzony właśnie na wypadek materializacji różnego rodzaju ryzyk.

13. [Projektowanie, wdrażanie i eksploatacja systemu teleinformatycznego] Bezpieczeństwo systemów teleinformatycznych, a także dostępność, integralność i poufność zgromadzonych w nich danych w dużym stopniu zależy od ich budowy oraz sposobu wdrożenia,

dlatego ważne jest, aby system został **zaprojektowany i zbudowany** zgodnie z **zasadami bezpieczeństwa**, tym samym zapewniał sprawną i efektywną realizację zadań. Zarówno wdrożenie, jak też zmiany systemu, przeprowadzone w sposób zorganizowany, pozwalają na dostarczenie wysokiej jakości, adekwatnych rozwiązań przy minimalizacji kosztów. W tym kontekście ważne jest, aby w procesie projektowania systemu (definiowania potrzeb jednostki) uczestniczyli nie tylko administratorzy systemu, ale również jego użytkownicy, a wyniki analizy ich potrzeb zostały uwzględnione w dokumentacji projektowej.

Przeprowadzone kontrole wskazały, że:

- w jednostkach nie zostały opracowane regulacje wewnętrzne opisujące wymagania w zakresie projektowania, wdrażania, przeprowadzania zmian oraz monitorowania systemów teleinformatycznych;
- w przypadku jednostki nieposiadającej systemu teleinformatycznego[7] nie podejmowano skutecznych działań dotyczących opracowania dokumentacji opisującej wymagania w zakresie jego zaprojektowania oraz wdrożenia.

14. [Zabezpieczenia techniczno-organizacyjne dostępu do informacji oraz systemów] W celu uzyskania odpowiedniego poziomu bezpieczeństwa informacji jednostki stosują szereg zabezpieczeń, których celem jest ochrona informacji np. przed kradzieżą, nieuprawnionym dostępem lub uszkodzeniem. Zabezpieczenia powinny być **adekwatne do poziomu ryzyka** wynikającego z analizy ryzyka bezpieczeństwa informacji i **opisane w planie postępowania z ryzykiem**. W ww. zakresie stwierdzano, że **obowiązujące w jednostkach wewnętrzne regulacje w ograniczonym zakresie przyczyniały się do minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji, środków przetwarzania informacji oraz urządzeń mobilnych**, tj.:

- nie obejmowały wszystkich obszarów (np. zasad dostępu do systemów oraz pomieszczeń biurowych, wymagań dotyczących sprzętu i oprogramowania, obowiązków pracowników w zakresie bezpieczeństwa informacji po zakończeniu zatrudnienia, zasad dotyczących sposobu klasyfikacji i oznaczania informacji z uwzględnieniem wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, zarządzania kluczami kryptograficznymi, zasad użytkowania telefonów służbowych);
- głównie odnosiły się do obszaru ochrony danych osobowych;
- ich przygotowanie nie zostało poprzedzone analizą ryzyka.

Mając powyższe na uwadze wprowadzone regulacje w jednostkach były fragmentaryczne, co sprawia, że nie zapewniały wymaganej minimalizacji potencjalnych zagrożeń. Ponadto w wyniku kontroli stwierdzano również niedostateczne zabezpieczenie dostępu do informacji oraz systemów, gdyż:

- jednostki nie przestrzegały postanowień własnych *Polityk Bezpieczeństwa Fizycznego* w zakresie kontroli dostępu do pomieszczeń biurowych (w szczególności nie była prowadzona ewidencja osób wchodzących i wychodzących bądź ewidencja osób pobierających i zdających klucze), a dodatkowo pomieszczenia nie były zabezpieczone przed dostępem osób trzecich. W ww. sytuacjach nie przeprowadzono pełnej analizy ryzyka i nie opracowano planu postępowania z ryzykiem zawierającego opis zastosowanych zabezpieczeń adekwatnych do poziomu ryzyka. W konsekwencji podejmowane działania nie chroniły informacji, w tym przetwarzanych w systemach.
- w jednostkach były zbierane dane z logowania, jednak nie zostały wprowadzone regulacje wewnętrzne dotyczące zasad prowadzenia, wykorzystania i przechowywania dzienników

[7] Zgodnie z definicją wynikającą z *ustawy o informatyzacji* system teleinformatyczny oznacza zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniających przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954, t. j. ze zm.).

systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. Brak formalnych procedur stwarzał zagrożenia w zakresie rozliczalności, nie zapewniał jednolitości postępowania oraz odpowiedniego poziomu bezpieczeństwa informacji.

- istotnym potencjalnym zagrożeniem dla bezpieczeństwa systemów było umiejscowienie serwerowni obok ogólnodostępnego dla wszystkich zainteresowanych osób pomieszczenia kancelarii, przy jednoczesnym braku skutecznego zabezpieczenia pomieszczenia serwerowni przed nieuprawnionym dostępem. Ponadto zagrożeniem były braki w stanie wyposażenia serwerowni, jak również przechowywanie w ich pomieszczeniach zbędnych opakowań po zakupionym sprzęcie informatycznym, co mogło stać się bezpośrednią przyczyną pożaru.
- kolejnym zagrożeniem dla bezpieczeństwa informacji przetwarzanych w jednostkach było wykorzystywanie na komputerach oprogramowania, dla którego producent nie zapewniał wsparcia w postaci modyfikacji oprogramowania w zakresie bezpieczeństwa.
- zarządzanie dostępem do systemów w wielu obszarach odbywało się w sposób niesformalizowany bądź niezgodny z obowiązującymi *Politykami bezpieczeństwa informacji*. Konta użytkowników tworzone były przez osoby nieuprawnione, brakowało nadzoru nad procesem wprowadzania użytkowników oraz przeglądu aktywności użytkowników. Ponadto, mimo że regulacje wewnętrzne określały sposób tworzenia i zmiany haseł, zasady te nie były stosowane, tj. nie następowała okresowa zmiana hasła. Kontrola przeprowadzana przez jednostki w tym zakresie nie była skuteczna i nie prowadziła do wykrywania przypadków, w których hasła nie były regularnie zmieniane.
- obowiązujące procedury dotyczące ochrony antywirusowej i działań podejmowanych po stwierdzeniu zainfekowania nie wskazywały odpowiedzialnych pracowników bądź osoby sprawującej nadzór nad realizacją działań w tym zakresie.

15. [Rozliczalność działań] Rozliczalność jest właściwością systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie[8], zatem zapewnienie rozliczalności działań polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) **wszystkie działania dostępu** do systemu z uprawnieniami administracyjnymi, **w zakresie konfiguracji systemu i zabezpieczeń**, a także **działania, gdy przetwarzanie danych podlega prawnej ochronie** (np. zgodnie z ustawą o ochronie danych osobowych). Informacje zawarte w dziennikach systemowych powinny być **regularnie przeglądane** w celu wykrycia działań niepożądanych/nieuprawnionego dostępu oraz powinny być **przechowywane w bezpieczny sposób**, co najmniej **2 lata**. W ww. zakresie stwierdzano:

- nieprawidłowość dotyczącą niezapewnienia rozliczalności działań prowadzonych w systemach, w szczególności nie wszystkie systemy zbierały informacje o aktywności użytkowników;
- w przypadku gdy informacje o aktywności użytkowników i obiektów systemowych były gromadzone przez system, w jednostkach nie prowadzono ich analizy bądź analizy były wykonywane wyłącznie doraźnie. Działania te nie były dokumentowane oraz nie określono zasad wykonywania regularnych przeglądów aktywności. Brak systematycznych i udokumentowanych przeglądów aktywności użytkowników nie pozwalał na uzyskanie wiedzy na temat ewentualnych niepożądanych działań.

[8] Definicja wynikająca z *Rozporządzenia KRI*.

Resumując wskazać należy, że *SZBI* to część **całościowego systemu zarządzania**[9], oparta na podejściu wynikającym z **ryzyka biznesowego**, odnosząca się do **ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji**[10]. W związku z powyższym *SZBI* dotyczy **wszystkich ww. obszarów**, a przedstawione powyżej nieprawidłowości w nich występujące, stanowiły uzasadnioną podstawę do sformułowania najistotniejszej, systemowej nieprawidłowości nieposiadania kompleksowego, spójnego *SZBI* gwarantującego poufność, dostępność i integralność przetwarzanych danych, zgodnego z *Rozporządzeniem KRI*.

II. Zapewnienie dostępności informacji zawartych na stronach internetowych

Zgodnie z § 19 *Rozporządzenia KRI* podmioty realizujące zadania publiczne zobowiązane były do dostosowania prezentowanych treści na stronach internetowych do wymagań Web Content Accessibility Guidelines (WCAG 2.0)[11]. W wyniku przeprowadzonych kontroli ustalono, że:

- strony internetowe poszczególnych jednostek nie spełniały większości wymagań ww. standardu;
- spełnienia powyższego wymogu nie uwzględniono przy podpisywaniu umów na projektowanie stron, pomijając w nich postanowienia dotyczące zgodności z *Rozporządzeniem KRI*.

Należy zwrócić uwagę na znaczącą rolę społeczną spełnienia wymagań, bowiem tworzenie a następnie funkcjonowanie serwisów internetowych z pominięciem przedstawionych zasad, może utrudniać albo wręcz uniemożliwić osobom z niepełnosprawnością pełne zapoznanie się z treścią zamieszczonych tam informacji.

III. Wymiana informacji w postaci elektronicznej

1. **[Usługi elektroniczne]** Jednym z podstawowych celów działalności jednostek jest świadczenie usług dla obywateli/klientów w sposób sprawny, szybki i jak najbardziej przyjazny. Realizację ww. celu można uzyskać poprzez świadczenie usług elektronicznych dostępnych przez Internet. Podstawową usługą elektroniczną jest Elektroniczna Skrzynka Podawcza (dalej: ESP) – miejsce do przyjmowania korespondencji elektronicznej. Obowiązek jej posiadania wynika z art. 16 ust. 1a *ustawy o informatyzacji*. Jednakże nie wszystkie poddane kontroli jednostki udostępniały ESP, tym samym nie świadczyły elektronicznej usługi na rzecz obywateli/klientów.

2. **[Centralne repozytorium wzorów dokumentów elektronicznych]** Organy administracji publicznej powinny wykorzystywać wzory dokumentów przechowywanych w centralnym repozytorium wzorów dokumentów elektronicznych (CRWDE), jakie zostały już wcześniej opracowane, a w przypadku uruchomienia usługi, dla której nie ma wzorów jednostka ma obowiązek przekazać do repozytorium procedurę obsługi usługi i wzory dokumentów z nią związanych[12]. W wyniku kontroli stwierdzono, że tylko jedna jednostka poddana kontroli, która świadczyła usługi elektroniczne, przekazała i udostępniła w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych, jednakże nie były one aktualne.

3. **[Model usługowy]** W myśl § 2 pkt 8 *Rozporządzenia KRI* model usługowy to model architektury, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystana z tych funkcji.

---

[9] System do ustanawiania polityki i celów oraz osiągania tych celów.

[10] Zgodnie z normą PN-ISO/IEC 27000.

[11] WCAG jest standardem służącym dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niepełnosprawnych. Rozwiązanie to ma na celu zapewnienie prezentacji treści w sposób ułatwiający osobom niepełnosprawnym zapoznanie się z wiadomościami. Ułatwienie to koncentruje się na sposobie wyświetlania i komunikatach głosowych. Ponadto wskazać należy, że *Rozporządzenie KRI* w części dotyczącej zapewnienia dostępu do zasobów informacji osobom niepełnosprawnym, zostało uchylone przez art. 20 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. poz. 848), która jednocześnie w załączniku określa *Wytyczne dla dostępności treści internetowych 2.1 stosowane dla stron internetowych i aplikacji mobilnych w zakresie dostępności dla osób niepełnosprawnych*.

[12] Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, opracowane przez Ministerstwo Cyfryzacji, Warszawa 15 grudnia 2015 r.

Zarządzanie usługami elektronicznymi wymaga posiadania i stosowania **procedur obsługi usług** oraz **dostarczania ich na deklarowanym poziomie dostępności**. Powyższe oznacza w szczególności możliwość zidentyfikowania właściciela (komórki organizacyjnej) poszczególnych usług, ustalenia odpowiedzialności za utrzymanie usługi od strony technicznej, określenie poziomu świadczenia usług poprzez określenie wskaźników dostępności (np. maksymalny czas niedostępności w danym okresie), monitorowanie poziomu świadczenia usług na zadeklarowanym poziomie, kontroli wskaźników dostępności i reagowania na ich przekroczenie.

W skontrolowanych jednostkach stwierdzono następujące nieprawidłowości:

- nie wdrożono procedur zarządzania usługami;
- poziom dostępności nie został określony dla wszystkich usług bądź został określony w gwarancji do systemu, co ograniczyło zakres jego stosowania;
- monitoring poziomu dostępności prowadzono jedynie dla części usług świadczonych przez systemy teleinformatyczne.

4. **[Obieg dokumentów w podmiocie publicznym]** Wdrożenie elektronicznego obiegu dokumentów wpływa na usprawnienie i przyśpieszenie obiegu dokumentów przy jednoczesnej minimalizacji nakładu pracy. Wykorzystanie w tym celu systemu teleinformatycznego umożliwia przekazywanie dokumentów w postaci elektronicznej, a tym samym obniża koszty wysyłki korespondencji. Mając na uwadze powyższe korzyści, jednostki powinny dążyć do **eliminacji tradycyjnego (papierowego) systemu dokumentowania** przebiegu załatwianych i rozstrzyganych spraw na rzecz elektronicznego systemu zarządzania dokumentacją. Jednakże w większości skontrolowanych jednostek sprawy dokumentowane były w systemie tradycyjnym albo system ten był wykorzystywany we wsparciu z obiegiem elektronicznym. Łączenie obu form powoduje, że część czynności jest powielanych, co niewątpliwie wpływa na obciążenie pracą pracowników. Wskazane zatem jest kontynuowanie działań zapewniających techniczne i organizacyjne warunki do wprowadzenia w jednostkach wyłącznie elektronicznego systemu zarządzania dokumentacją.

Dyrektor
Centrum Obsługi Administracji
Maciej Tomczak