`

Kancelaria Prezesa
Rady Ministrów

Departament Tożsamości Cyfrowej
Zastępca Dyrektora
Michał Kalinowski

DTC.WTC.7202.198.2023
Warszawa, 20 kwietnia 2023 r.

Podmioty przyłączone do węzła krajowego

Szanowni Państwo,

w związku z przyłączeniem Państwa systemu/systemów teleinformatycznych udostępniających usługi online do węzła krajowego oraz potrzebą prowadzenia działań zapobiegającym naruszeniom bezpieczeństwa, o których mowa w art. 39b ust. 2 oraz w związku z art. 39i ustawy o usługach zaufania oraz identyfikacji elektronicznej przeprowadziliśmy badania ankietowe wśród kilkuset podmiotów.

Wyniki badania ankietowego pozwoliły na wyodrębnienie kluczowych kwestii dotyczących bezpieczeństwa informacji. Chcemy się z Państwem podzielić naszymi spostrzeżeniami w zakresie właściwego podejścia do zarządzania bezpieczeństwem informacji.

Uprzejmie proszę o przekazanie niniejszego pisma wszystkim osobom, które w Państwa podmiocie mają wpływ na bezpieczeństwo informacji.

Jednocześnie, na podstawie wyżej przytoczonych przepisów, **proszę o przesłanie do 27 kwietnia 2023 r. zwrotnej informacji o zapoznaniu się z niniejszym pismem**.

1. Dla właściwego opracowania, ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) niezbędnym jest objęcie tym systemem wszystkich informacji przetwarzanych w podmiocie. Niewystarczające jest np. powoływanie się jedynie na politykę ochrony danych osobowych i/lub instrukcję zarządzania systemem informatycznym. Zagadnienia dotyczące ochrony danych osobowych i danych przetwarzanych w systemach informatycznych stanowią bowiem węższy obszar względem zarządzania bezpieczeństwem informacji.

   Na marginesie dodam, że niegdyś funkcjonował w obrocie taki dokument jak *Instrukcja zarządzania systemem informatycznym*. Był on wymagany na podstawie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. Nr 100, poz.

Tel: +48 22 245 58 52
email: sekretariat.DTC@mc.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

1024). Rozporządzenie to obowiązywało przed wprowadzeniem RODO[1] i zostało formalnie uchylone z dniem 6 lutego 2019 roku.

Proponuję zweryfikować, czy w Państwa jednostce istnieje aktualna dokumentacja potwierdzająca opracowanie, ustanowienie i wdrożenie SZBI.

2. Jeśli integrację systemu teleinformatycznego z węzłem krajowym zleciliście Państwo podmiotowi zewnętrznemu musicie pamiętać, że w takiej sytuacji to na Was spoczywa obowiązek właściwego zabezpieczenia współpracy z podmiotem zewnętrznym. Ta współpraca powinna umożliwiać bieżącą ocenę bezpieczeństwa informacji przetwarzanych w systemie teleinformatycznym zintegrowanym z węzłem krajowym m.in. poprzez sprawną wymianę informacji z tym podmiotem zewnętrznym.

Można to osiągnąć np. poprzez stosowne klauzule umowne w zawieranej z takim podmiotem umowie. Pozwoli to zapobiec ewentualnym trudnościom związanym z uzyskaniem wymaganych w ankiecie informacji od podmiotów, którym zlecono utrzymanie systemu teleinformatycznego.

Zwracam więc uwagę, że to na podmiotach, którym decyzję o przyłączeniu do węzła krajowego wydał Minister Cyfryzacji spoczywa obowiązek opracowania, ustanowienia, wdrożenia, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji systemu integrowanego z węzłem krajowym, zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne.*

Oświadczenie o zobowiązaniu się do powyższych wymagań składaliście Państwo przed przyłączeniem systemu teleinformatycznego do węzła krajowego.

3. Wdrożony SZBI powinien obejmować System Teleinformatyczny DU w obszarze bezpieczeństwa informacji w relacjach z dostawcami i zarządzania usługami świadczonymi przez dostawców[2].

Utrzymanie uzgodnionego poziomu bezpieczeństwa informacji oraz jakości usług objętych umowami jest wymogiem koniecznym w każdym przypadku, kiedy system teleinformatyczny jest utrzymywany przy wykorzystaniu wykonawców zewnętrznych.

Umowy powinny z kolei uwzględniać parametry zapewnienia jakości usług takie jak czasy reakcji, czasy naprawy (SLA).

W zakresie świadczonych przez dostawców usług związanych z zapewnieniem atrybutów bezpieczeństwa stosuje się następujące zasady:

- czas reakcji nie mniejszy niż 1 godzina,
- czas przywrócenia pierwotnego stanu nie dłuższy niż 24 godziny.

Tym samym wszystkie te podmioty, które zleciły utrzymanie systemu teleinformatycznego zintegrowanego z węzłem krajowym zewnętrznym dostawcom

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz.Urz.UE.L Nr 119, str. 1).

[2] Szerzej o relacjach z dostawcami w pkt 11 cz. II PBI WK (str. 52) oraz w zał. nr 2.14 do PBI WK.

powinny szczegółowo zapoznać się z wymaganiami PBI WK w zakresie budowania z tymi dostawcami właściwych relacji. Należy też uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji w celu zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.

Zalecane jest opracowanie w podmiocie katalogu minimalnych wymagań/postanowień umownych uwzględniających bezpieczeństwo informacji w relacjach z dostawcami.

4. Opracowanie właściwie funkcjonującego SZBI powinno spełniać wymagania Polskiej Normy PN-ISO/IEC 27001.

   Należy mieć na uwadze, że stosowanie norm w polskim porządku prawnym jest co do zasady dobrowolne. Niemniej, zgodnie z rozporządzeniem w sprawie krajowych ram interoperacyjności[3] wymagania dotyczące zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001.

   Mając powyższe na uwadze należy pamiętać, że zgodnie z brzmieniem Polskiej Normy PN-ISO/IEC 27001 nie dopuszcza się pominięcia żadnego z wymagań określonych w rozdziałach od 4 do 10 tej normy, jeśli organizacja deklaruje zgodność z tą normą. Innymi słowy mimo braku obowiązku stosowania tej normy wymagania w niej określone muszą zostać spełnione aby można było uznać, że podmiot spełnia wymagania dotyczące zarządzania bezpieczeństwem informacji.

   Na marginesie można dodać, że istnieje możliwość uzyskania certyfikatu z zakresie zgodności z omawianą normą. Należy mieć na uwadze, że regulacje EU wskazują na zachęcanie do certyfikacji jako sposobu wykazywania zgodności zarówno w zakresie ochrony danych jak i certyfikacji cyberbezpieczeństwa. Niemniej jednak sama certyfikacja pozostaje czynnością dobrowolną.

5. Istotnym zagadnieniem dot. SZBI jest monitorowanie[4]. Poprzez monitorowanie należy rozumieć takie rozwiązania, które umożliwią ocenę działań na rzecz bezpieczeństwa informacji oraz skuteczności systemu zarządzania bezpieczeństwem informacji. Innymi słowy w ramach przyjętych rozwiązań należy wskazać:
   - co należy monitorować;
   - metody monitorowania (jak monitorować);
   - częstotliwość monitorowania;
   - osoby odpowiedzialne za monitorowanie;
   - częstotliwość dokonywania analizy wyników monitorowania;
   - osoby odpowiedzialne za analizę i ocenę wyników monitorowania.

   Bardzo istotną kwestią jest to aby zachować udokumentowane informacje jako dowód wyników monitorowania.

   Obowiązek rejestrowania zdarzeń dotyczy wszystkich podmiotów, które zintegrowały system teleinformatyczny z węzłem krajowym.

6. Wyjaśnienia wymaga czym jest obowiązek realizacji **przeglądu zarządzania**.

---

[3] § 20 ust. 3 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).
[4] Szerzej o monitorowaniu w pkt 5.1 cz. I PBI WK (str. 30) oraz pkt 8.5 cz. II PBI WK (str. 47).

Przegląd zarządzania jest to obowiązek spoczywający na najwyższym kierownictwie. Powinien być realizowany cyklicznie w odgórnie zaplanowanych odstępach czasu. Zgodnie z PBI WK powinien być realizowany co najmniej 1 raz do roku.

Powinien uwzględniać[5] m.in.:

- stan działań podjętych w następstwie wcześniejszych przeglądów zarządzania;
- zmiany czynników zewnętrznych i wewnętrznych, istotnych dla SZBI;
- informacje zwrotne o wynikach działań na rzecz bezpieczeństwa informacji, w tym trendach w zakresie niezgodności, wyników monitorowania, wyników audytów, spełniania zdefiniowanych celów bezpieczeństwa informacji;
- wyniki szacowania ryzyka i stan planów postępowania z ryzykiem.

Wynikiem przeglądu zarządzania powinny być **udokumentowane** decyzje najwyższego kierownictwa w zakresie możliwości doskonalenia SZBI i potrzeb jego zmiany.

Nie można uznać, że system zarządzania bezpieczeństwem informacji został skutecznie wdrożony, jeśli brak jest przeglądów zarządzania tego systemu.

7. Poprzedni punkt dotyczy **przeglądu zarządzania**, którego nie można mylić z pojęciem: **przegląd SZBI[6].**

Przeglądy SZBI obejmują przeglądy polityk i innych dokumentów składających się na SZBI pod kątem ich aktualności, przydatności i adekwatności. Poddawanie dokumentacji SZBI cyklicznym przeglądom to niezbędny element skutecznego zarządzania.

8. Niezwykle istotne z punktu widzenia bezpieczeństwa informacji jest właściwe zarządzanie incydentami[7].

Aby zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji należy ustanowić odpowiedzialność oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty.

Te procedury powinny być udokumentowane i obejmować system teleinformatyczny zintegrowany z węzłem krajowym.

9. Dla zapewnienia rozliczalności działania w systemach niezbędne jest przechowywanie dzienników zdarzeń (logów) przez określony czas.

Zgodnie z rozporządzeniem w sprawie krajowych ram interoperacyjności[8] informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata. Wymogi w tym zakresie dotyczą systemu WK, jak i systemów informatycznych z nim zintegrowanych.

---

[5] Szerzej o przeglądzie zarządzania: pkt 5.3 cz. I PBI WK (str. 31) oraz w pkt 14.2 cz. II PBI WK (str. 56).
[6] Szerzej o przeglądzie SZBI w pkt 1.2 cz. II PBI WK (str. 37).
[7] Szerzej o zarządzaniu incydentami w pkt 12 cz. II PBI WK (str. 53) oraz w zał. nr 2.5 do PBI WK.
[8] § 21 ust. 4 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).

Raz jeszcze należy podkreślić, że w każdym przypadku podmiot, którego system został zintegrowany z węzłem krajowym na mocy decyzji Ministra Cyfryzacji, jest zobowiązany do zapewnienia bezpieczeństwa informacji, w tym do zapewnienia rozliczalności działań w tym systemie.

10. Proszę przyjąć jeszcze dwie wskazówki, które mogą zwiększyć bezpieczeństwo informacji w kontekście zapewnienia rozliczalności:

- systemy powinny zapewniać pełną rozliczalność czynności w nich wykonywanych. Z tego względu ważne jest aby zapewnić tę rozliczalność w stosunku dla działań wszystkich użytkowników, szczególnie dla działań wymagających wyższych uprawnień / uprawnień administracyjnych. Przykładem właściwego rozwiązania w powyższym zakresie jest odnotowywanie działań administratora (w tym faktu usunięcia logów) w innym miejscu, gdzie administrator nie ma dostępu.
- wskazane jest założenie i prowadzenie rejestru użycia haseł awaryjnych. Odnotowywanie użycia haseł awaryjnych to zabezpieczenie w kierunku zapewnienia rozliczalności w systemie oraz prosty wskaźnik krytycznego zdarzenia / incydentu w eksploatacji systemu.

11. Jednym ze sposobów na zwiększenie świadomości wśród pracowników podmiotów jest prowadzenie szkoleń z zakresu bezpieczeństwa informacji, skutków jego naruszenia, w tym odpowiedzialności prawnej.

Podniesienie kompetencji w tym obszarze powinno zostać zapewnione również poprzez zapoznanie się z PBI WK całego personelu zaangażowanego w przetwarzanie informacji. Pracownicy i osoby lub podmioty świadczące usługi w systemie muszą potwierdzić zapoznanie się z obowiązującymi przepisami i zasadami oraz zobowiązać się do ich stosowania, poprzez podpisanie odpowiedniego dokumentu „Oświadczenie o zapoznaniu się i zobowiązaniu do stosowania zasad bezpieczeństwa informacji WK”[9].

12. Jednym z czynników ryzyka wpływających na bezpieczeństwo informacji w systemie teleinformatycznym jest dysponowanie przez podmioty kompletem dokumentacji danego systemu w zakresie:

- projektowym;
- wdrożeniowym;
- powdrożeniowym;
- eksploatacyjnym.

Prawidłowe zarządzanie systemem teleinformatycznym jest możliwe m.in. dzięki posiadaniu odpowiednich informacji na temat systemu, w tym udokumentowanych procedur. Proszę zweryfikować, czy dysponujecie Państwo kompletem dokumentacji w powyższym zakresie.

13. Zarządzanie ryzykiem wymaga przeprowadzania cyklicznej analizy ryzyka i opracowania rejestru ryzyk. W analizie ryzyka należy uwzględnić aspekty wynikające z faktu bycia właścicielem systemu teleinformatycznego[10].

14. Należy też pamiętać o obowiązku wykonywania testów bezpieczeństwa systemu teleinformatycznego zintegrowanego z węzłem krajowym.

---

[9] Wzór oświadczenia został określony w zał. nr 1.9 do PBI WK.
[10] Szerzej o zarządzaniu ryzykiem w pkt 3.2 PBI WK (str. 23) oraz w zał. nr 1.6 do PBI WK.

Obowiązek przeprowadzania raz na kwartał oceny podatności wynika wprost z PBI WK[11].

15. Istotnym obszarem jest również obszar ochrony danych osobowych.

Każdy podmiot podłączany do węzła krajowego oświadcza[12], że działa zgodnie z przepisami o ochronie danych osobowych.

Obowiązek ten realizowany powinien być m.in. poprzez opracowanie oceny skutków dla ochrony danych, co wynika z art. 35 RODO.

Na podmiotach spoczywa również obowiązek prowadzenia rejestru czynności przetwarzania obejmującego system teleinformatyczny zintegrowany z węzłem krajowym. Obowiązek prowadzenia takiego rejestru wynika z art. 30 RODO.

Pozostałe działania, jakie powinny być realizowane wynikają z RODO (regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych; audyty) i 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*[13] (okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji). Powinny one uwzględniać przetwarzanie danych osobowych w systemie teleinformatycznym zintegrowanym z węzłem krajowym.

16. Należy zauważyć, że system zarządzania bezpieczeństwem informacji nie może być kompletny bez zapewnienia audytu wewnętrznego, zarówno według wymagań 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*[14] jak i wymagań normy PN-ISO/IEC 27001.

17. Dla zwiększenia bezpieczeństwa przetwarzanych informacji zaleca się aby datacenter, gdzie znajduje się system teleinformatyczny spełniał określone wymagania, posiadał m.in.:

- minimum dwa źródła zasilania z dwóch oddzielnych stacji TRAFO;
- minimum dwa klimatyzatory;
- system gaszenia pożaru;
- system kontroli dostępu;
- backup zlokalizowany innym miejscu.

18. Dla wykrywania nieuprawnionych prób dostępu należy wprowadzić mechanizmy pozwalające na wykrycie prób nieautoryzowanych działań związanych z przetwarzaniem informacji w systemie teleinformatycznym.

---

[11] Zob. pkt 8.7 cz. II PBI WK (str. 48-49).
[12] Zgodnie z art. 21t ust. 1 pkt 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej (Dz. U z 2021 r. poz. 1797, tj.).
[13] Zob. § 20 ust. 2 pkt 14 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).
[14] 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 2017 r. poz. 2247).

System taki powinien wspomagać zapobieganie, wykrywanie i monitorowanie w zakresie działań związanych z próbami uzyskania nieuprawnionego dostępu[15].

Nie może zatem opierać się np. tylko na doraźnym przeglądzie logów.

Z wyrazami szacunku

Michał Kalinowski
/dokument podpisany elektronicznie/

[15] Zob. § 20 ust. 2 pkt 7 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).