Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.123.2026
Warszawa, 15 października 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa nr 2026-67a-9 dotycząca środków organizacyjnych i technicznych służących zwiększaniu poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa

Podstawa i cel rekomendacji

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1]. Jej celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa (KSC) poprzez zastosowanie odpowiednich środków organizacyjnych i technicznych.

Jednocześnie wdrożenie określonych w rekomendacji rozwiązań pozwoli nie tylko istotnie podnieść poziom cyberbezpieczeństwa podmiotu i znacząco ograniczyć możliwość dokonania skutecznego cyberataku na podmiot, ale także będzie wspierać spełnienie części obowiązków podmiotów KSC określonych w ustawie o KSC.

Rekomendowane środki organizacyjne i techniczne

1. Zarządzanie ryzykiem i polityki bezpieczeństwa

1.1 Szacowanie ryzyka

Wdrożenie i utrzymywanie procesu szacowania ryzyka wystąpienia incydentów cyberbezpieczeństwa oraz zarządzania tym ryzykiem. W szczególności zaleca się:

a) prowadzenie procesu identyfikacji, analizy i oceny ryzyka w sposób systematyczny i udokumentowany;

b) dokonywanie ponownej oceny ryzyka nie rzadziej niż raz w roku oraz każdorazowo po istotnych zmianach organizacyjnych, technologicznych lub infrastrukturalnych;

c) uwzględnianie nowych podatności, zagrożeń i wektorów ataku identyfikowanych przez właściwe zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), producentów oprogramowania oraz organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne (typu ISAC[2]);

d) dokumentowanie wyników szacowania ryzyka;

e) zapewnienie, aby wyniki analizy ryzyka stanowiły podstawę doboru środków organizacyjnych i technicznych.

[1] Dz. U. z 2026 r. poz. 20, z późn. zm. (dalej jako: „ustawa o KSC”).
[2] ISAC - Information Sharing and Analysis Center (Centra Wymiany i Analizy Informacji).

1.2 Polityki i procedury bezpieczeństwa

Opracowanie, wdrożenie i utrzymywanie aktualnej dokumentacji regulującej obszar cyberbezpieczeństwa. Dokumentacja powinna obejmować co najmniej:

a) politykę bezpieczeństwa informacji;

b) politykę szacowania i zarządzania ryzykiem;

c) procedury zarządzania aktywami;

d) procedury kontroli dostępu;

e) zasady bezpiecznej pracy zdalnej;

f) zasady bezpiecznego korzystania z poczty elektronicznej;

g) procedury reagowania na incydenty;

h) procedury wykonywania kopii zapasowych;

i) procedury zapewnienia ciągłości działania.

1.3 Odpowiedzialność i nadzór kierownictwa

Zapewnienie aktywnego udziału kierownictwa podmiotu w nadzorowaniu systemu zarządzania cyberbezpieczeństwem. W szczególności zaleca się:

a) formalne przypisanie odpowiedzialności za realizację obowiązków wynikających z ustawy o KSC;

b) zapewnienie corocznych szkoleń z zakresu cyberbezpieczeństwa dla kierownika podmiotu oraz osób odpowiedzialnych za cyberbezpieczeństwo;

c) określenie ról, kompetencji i odpowiedzialności uczestników procesów cyberbezpieczeństwa;

d) opracowanie i utrzymywanie macierzy odpowiedzialności (RACI);

e) okresowe raportowanie kierownictwu poziomu ryzyka oraz stanu realizacji obowiązków ustawowych.

2. Ochrona aktywów, tożsamości i kontrola dostępu

2.1 Zarządzanie aktywami

Prowadzenie kompletnej oraz aktualnej inwentaryzacji aktywów ICT (technologie informacyjne i komunikacyjne) oraz OT (technologie operacyjne). W szczególności zaleca się:

a) prowadzenie rejestru urządzeń końcowych, serwerów, urządzeń sieciowych, systemów OT, baz danych oraz oprogramowania;

b) przypisanie właścicieli poszczególnym aktywom;

c) klasyfikowanie aktywów według poziomu krytyczności;

d) identyfikację usług dostępnych publicznie z sieci Internet;

e) ewidencjonowanie wykorzystywanych portów, protokołów komunikacyjnych i zależności pomiędzy systemami.

2.2 Zarządzanie tożsamością i uprawnieniami

Wdrożenie systemu zarządzania tożsamością i dostępem opartego na zasadzie minimalnych uprawnień (Least Privilege) oraz zasadzie wiedzy niezbędnej (*Need-to-Know)*. W szczególności zaleca się:

a) przyznawanie użytkownikom i aplikacjom wyłącznie uprawnień niezbędnych do wykonywania przypisanych zadań;

b) wyłączanie niewykorzystywanych portów, usług i protokołów;

c) usuwanie lub blokowanie kont domyślnych i nieużywanych;

d) wdrożenie mechanizmów blokowania kont po wielokrotnych nieudanych próbach logowania;

e) okresowe przeglądy uprawnień;

f) niezwłoczne odbieranie lub modyfikowanie uprawnień osób zmieniających stanowisko lub kończących realizację zadań.

2.3 Uwierzytelnianie wieloskładnikowe i dostęp zdalny

W celu ograniczenia ryzyka nieuprawnionego dostępu do systemów i zasobów organizacji oraz zwiększenia bezpieczeństwa pracy zdalnej rekomenduje się:

a) obowiązkowe stosowanie uwierzytelniania wieloskładnikowego (MFA) dla dostępu zdalnego, poczty elektronicznej, systemów krytycznych i kont uprzywilejowanych;

b) wyłączenie bezpośredniego dostępu administracyjnego do urządzeń i serwerów z publicznej sieci Internet;

c) realizowanie dostępu administracyjnego wyłącznie za pośrednictwem bezpiecznych połączeń VPN zabezpieczonych MFA;

d) prowadzenie ewidencji i monitorowanie kont uprzywilejowanych.

3. Ochrona infrastruktury, cyklu życia systemów i kryptografia

3.1 Bezpieczeństwo w cyklu życia systemów

Stosowanie zasad bezpieczeństwa od samego początku (*Security by Design)* oraz domyślnego bezpieczeństwa *(Security by Default)*. W szczególności zaleca się:

a) uwzględnianie wymagań cyberbezpieczeństwa już na etapie planowania i zakupu systemów;

b) przeprowadzanie testów bezpieczeństwa przed uruchomieniem nowych systemów;

c) zapewnienie bezpiecznej eksploatacji oraz wycofania systemów z użytkowania;

d) wdrożenie procedur zarządzania urządzeniami i oprogramowaniem, dla których zakończono wsparcie producenta (EOL/EOSL).

3.2 Zarządzanie podatnościami i aktualizacjami

Właściwe zarządzanie podatnościami oraz terminowe wdrażanie aktualizacji stanowią podstawowy element ograniczania ryzyka wykorzystania znanych luk bezpieczeństwa. W tym zakresie rekomenduje się:

a) wdrożenie formalnego procesu zarządzania podatnościami;

b) regularne instalowanie aktualizacji i poprawek bezpieczeństwa;

c) prowadzenie regularnych skanów podatności infrastruktury, w tym z wykorzystaniem dostępnych narzędzi państwowych, jak system Artemis[3];

d) monitorowanie komunikatów publikowanych przez CSIRT oraz producentów oprogramowania;

e) prowadzenie rejestru wykrytych podatności i działań naprawczych.

3.3 Kryptografia i ochrona danych

Ochrona informacji o szczególnym znaczeniu dla organizacji powinna uwzględniać stosowanie adekwatnych środków kryptograficznych zarówno podczas przesyłania, jak i przechowywania danych. W szczególności zaleca się stosowanie szyfrowania danych osobowych, informacji prawnie chronionych oraz innych danych wrażliwych lub kluczowych z punktu widzenia działalności organizacji.

Rekomenduje się opracowanie i wdrożenie polityki stosowania środków kryptograficznych. W szczególności zaleca się:

a) szyfrowanie danych przesyłanych;

b) szyfrowanie danych przechowywanych;

c) stosowanie aktualnych i powszechnie uznawanych standardów kryptograficznych;

d) zarządzanie cyklem życia kluczy kryptograficznych;

e) dostosowanie poziomu ochrony kryptograficznej do klasyfikacji aktywów i poziomu ryzyka;

f) stosowanie szyfrowania danych osobowych, tajemnic prawnie chronionych oraz innych informacji, których ujawnienie mogłoby negatywnie wpłynąć na działalność organizacji;

g) wykorzystywanie odpowiednich rozwiązań technicznych do ochrony informacji przekazywanych drogą elektroniczną, w szczególności szyfrowania wiadomości e-mail (np. S/MIME lub OpenPGP) oraz zabezpieczania udostępnianych plików i archiwów za pomocą mechanizmów szyfrowania i haseł.

3.4 Bezpieczeństwo fizyczne i środowiskowe

Zapewnienie bezpieczeństwa fizycznego i środowiskowego infrastruktury teleinformatycznej stanowi istotny element ochrony przed zakłóceniem ciągłości działania oraz nieuprawnionym dostępem do zasobów organizacji. W tym zakresie rekomenduje się:

a) zabezpieczenie pomieszczeń technicznych przed dostępem osób nieuprawnionych;

b) stosowanie kontroli dostępu do serwerowni i szaf teleinformatycznych;

c) prowadzenie rejestrów wejść do pomieszczeń kluczowych dla realizacji zadań podmiotu;

d) zapewnienie monitoringu infrastruktury kluczowej dla realizacji zadań podmiotu;

e) stosowanie systemów zasilania awaryjnego (UPS);

[3] Usługa dostępna za pośrednictwem portalu cyber.gov.pl, poprzez moje.cert.pl.

f) zapewnienie redundancji zasilania dla infrastruktury kluczowej dla realizacji zadań podmiotu.

4. Kopie zapasowe i odtwarzanie po awarii

4.1 Tworzenie kopii zapasowych

Wdrożenie polityki wykonywania kopii zapasowych zgodnej z zasadą 3:2:1[4]. W szczególności zaleca się:

a) regularne wykonywanie kopii danych, konfiguracji oraz systemów;

b) stosowanie co najmniej dwóch różnych nośników lub technologii przechowywania;

c) utrzymywanie co najmniej jednej kopii poza podstawową lokalizacją lub w trybie offline;

d) zapewnienie logicznej lub fizycznej separacji środowiska backupowego od środowiska produkcyjnego;

e) ochronę kopii zapasowych przed usunięciem, modyfikacją lub zaszyfrowaniem.

4.2 Odtwarzanie po awarii

Zdolność do skutecznego odtworzenia danych i przywrócenia działania systemów po awarii lub incydencie cyberbezpieczeństwa ma kluczowe znaczenie dla zapewnienia ciągłości działania organizacji. W tym zakresie rekomenduje się:

a) regularne testowanie procedur odtwarzania danych;

b) dokumentowanie wyników testów;

c) opracowanie i utrzymywanie Planu Ciągłości Działania;

d) opracowanie i utrzymywanie Planu Odtwarzania po Awarii;

e) określenie docelowego czasu odtworzenia usług (*RTO - Recovery Time Objective*) oraz dopuszczalnego poziomu utraty danych (*RPO - Recovery Point Objective*) dla systemów kluczowych dla realizacji zadań podmiotu;

f) stosowanie bezpiecznych procedur odbudowy środowiska po incydencie cyberbezpieczeństwa.

5. Zarządzanie ryzykiem w łańcuchu dostaw

Wdrożenie procesu zarządzania ryzykiem dostawców produktów, usług i procesów ICT. W szczególności zaleca się:

a) przeprowadzanie oceny ryzyka przed wyborem dostawcy;

b) okresową ocenę dostawców w trakcie współpracy;

c) identyfikację zależności od podmiotów trzecich;

---

[4] Zasada 3-2-1 polega na utrzymywaniu co najmniej trzech kopii danych (oryginał oraz dwie kopie zapasowe), przechowywanych na co najmniej dwóch różnych nośnikach lub w dwóch różnych technologiach przechowywania, przy czym co najmniej jedna kopia powinna znajdować się poza podstawową lokalizacją lub być przechowywana w sposób odseparowany (offline). Celem tej zasady jest zapewnienie możliwości odtworzenia danych w przypadku awarii, błędu użytkownika, katastrofy lokalnej lub ataku ransomware.

d) analizę skutków niedostępności świadczonych usług;

e) uwzględnianie w umowach wymagań cyberbezpieczeństwa, poziomów świadczenia usług (SLA) oraz uprawnień audytowych;

f) kontrolowanie zakresu dostępów przyznawanych dostawcom;

g) ograniczanie ryzyka koncentracji usług u pojedynczego dostawcy;

h) uwzględnianie ostrzeżeń, decyzji i zaleceń dotyczących dostawców wysokiego ryzyka;

j) uwzględnianie, w przypadku zamówień publicznych, przesłanek odrzucenia ofert określonych w art. 226 ust. 1 pkt 16, 17 i 19 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych[5], odnoszących się do bezpieczeństwa publicznego, podstawowych interesów bezpieczeństwa państwa oraz dostawców produktów, usług i procesów ICT.

6. Monitorowanie, detekcja i reagowanie na incydenty

6.1 Monitorowanie i analiza zdarzeń

Wdrożenie mechanizmów ciągłego monitorowania bezpieczeństwa. W szczególności zaleca się:

a) objęcie systemów krytycznych monitoringiem bezpieczeństwa;

b) centralizację logów zdarzeń;

c) analizę logów pod kątem wykrywania anomalii i prób nieuprawnionego dostępu;

d) stosowanie narzędzi klasy SIEM lub rozwiązań równoważnych;

e) zabezpieczenie logów przed usunięciem lub modyfikacją;

f) zapewnienie monitorowania aktywów o wysokiej krytyczności adekwatnie do poziomu ryzyka, w tym w uzasadnionych przypadkach w modelu 24/7.

6.2 Reagowanie na incydenty

Skuteczne reagowanie na incydenty cyberbezpieczeństwa wymaga jasno określonych procedur, odpowiedzialności oraz sprawnych mechanizmów współpracy z właściwymi podmiotami krajowego systemu cyberbezpieczeństwa. W tym zakresie rekomenduje się:

a) opracowanie procedur obsługi incydentów;

b) określenie ścieżek eskalacji;

c) wyznaczenie osób odpowiedzialnych za obsługę incydentów;

d) zapewnienie możliwości zabezpieczenia materiału dowodowego;

e) terminowe zgłaszanie incydentów właściwemu CSIRT za pośrednictwem właściwych kanałów komunikacji, w tym przez system S46 w przypadkach przewidzianych przepisami prawa[6];

f) utrzymywanie gotowości do współpracy z CSIRT oraz właściwymi organami;

g) wdrożenie procedur ograniczania skutków ataków, w szczególności ataków DDoS.

---

[5] Dz. U. z 2026 r. poz. 793.

[6] Podmioty kluczowe i podmioty zobowiązane są zgłaszać incydenty za pośrednictwem systemu S46. Obowiązek ten wchodzi w życie od 3 kwietnia 2027 r.

7. Świadomość, edukacja i higiena cyfrowa

Prowadzenie stałego programu podnoszenia świadomości cyberbezpieczeństwa. W szczególności zaleca się:

a) organizowanie regularnych szkoleń dla pracowników;

b) dostosowanie programów szkoleniowych do pełnionych ról i poziomu dostępu do informacji;

c) przeprowadzanie ćwiczeń praktycznych oraz kampanii phishingowych;

d) promowanie zasad bezpiecznego korzystania z poczty elektronicznej;

e) stosowanie zabezpieczeń antyphishingowych i antymalware;

f) określenie zasad korzystania z urządzeń prywatnych;

g) edukowanie pracowników w zakresie obowiązku niezwłocznego zgłaszania podejrzanych zdarzeń;

h) wykorzystywanie dostępnych materiałów edukacyjnych, szkoleń i kampanii informacyjnych dostępnych w serwisie cyber.gov.pl oraz w bazie wiedzy o cyberbezpieczeństwie[7].

8. Nadzór, audyt i ciągłe doskonalenie

Wdrożenie mechanizmów okresowej oceny skuteczności stosowanych środków bezpieczeństwa. W szczególności zaleca się:

a) wyznaczenie co najmniej dwóch osób odpowiedzialnych za kontakty w sprawach cyberbezpieczeństwa;

b) zgłoszenie wymaganych punktów kontaktowych w odpowiednich systemach teleinformatycznych;

c) przeprowadzanie okresowych audytów bezpieczeństwa;

d) monitorowanie realizacji zaleceń poaudytowych;

e) prowadzenie regularnych testów skuteczności zabezpieczeń;

f) analizowanie przyczyn oraz skutków incydentów;

g) wykorzystywanie wyników audytów, testów i analiz do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji;

h) przedstawianie kierownictwu okresowych raportów dotyczących poziomu zgodności z wymaganiami ustawy o KSC oraz skuteczności wdrożonych środków bezpieczeństwa.

Wnioski końcowe

Wskazane środki powinny być wdrażane z uwzględnieniem charakteru działalności podmiotu, rodzaju świadczonych usług, znaczenia wykorzystywanych systemów informacyjnych, poziomu ryzyka, skali działalności, prawdopodobieństwa wystąpienia incydentu oraz potencjalnych skutków jego wystąpienia.

[7] https://www.gov.pl/web/baza-wiedzy/

Niniejsza rekomendacja ma charakter pomocniczy i stanowi katalog rekomendowanych środków służących realizacji obowiązków wynikających z ustawy o KSC. Nie zastępuje ona obowiązków określonych w przepisach prawa ani indywidualnej oceny ryzyka przeprowadzanej przez podmiot.

Krzysztof Gawkowski
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/