KRAJOWA IZBA GOSPODARCZA
ELEKTRONIKI I TELEKOMUNIKACJI

Warszawa, dn. 12.06.2026 r.
KIGEiT/1033/06/2026

Szanowny Pan
Zbigniew Muszyński
Dyrektor Rządowego Centrum Bezpieczeństwa

STANOWISKO KONSULTACYJNE
w przedmiocie projektu rozporządzenia Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej (numer z wykazu: RD301)

Szanowny Panie Dyrektorze,

w odpowiedzi na ogłoszone konsultacje publiczne projektu rozporządzenia Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej (dalej: „Projekt"), w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji przedstawiam uwagi w załączonej tabeli.

Z wyrazami szacunku

Prezes Zarządu
Stefan Kamiński

Signature Not Verified
Dokument podpisany przez Stefan Kamiński
Data: 2026.06.12 12:56:01 CEST
Powód: Złożenie podpisu

Załącznik: Tabela z uwagami do projektu rozporządzenia Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej (RD301)

ul. Stępińska 22/30
00-739 Warszawa
tel.: +48 22 8510309,
+48 22 8406522
e-mail: kigeit@kigeit.org.pl

NIP 5260029121
Konto: BNP PARIBAS O/Warszawa
nr: 52 1600 1374 0003 0052 2279 1
(e-Doręczenia): AE:PL-65582-55850-ADFTJ-12

kigeit.org.pl

Załącznik do pisma KIGEiT/1033/06/2026

Uwagi
do projektu rozporządzenia Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej (RD301)

Lp.	Podmiot wnoszący uwagę	Jednostka redakcyjna, do której wnoszona jest uwaga	Treść uwagi	Propozycja brzmienia przepisu
1	KIGEiT	Załącznik. I. Bezpieczeństwo fizyczne obiektów lądowych, ust 3, pkt 3	W pkt 3 ppkt 3 – zapis dotyczący - oceny możliwości i wyeliminowania przewidywanych scenariuszy ataków, a w przypadkach, gdy nie jest to możliwe – określenie niezbędnych czasów spowolnienia działania potencjalnych intruzów, powiązanych z rzeczywistym czasem interwencji sił bezpośredniej ochrony fizycznej – jest w kwestii „spowolnienia" działania potencjalnych intruzów" zapisem ogólnikowym, mało precyzyjnym. **W tym zakresie sugeruje się rozważenie możliwości doprecyzowania co rozumie się poprzez określenie „czas spowolnienia".**	
2	KIGEiT	Załącznik. I. Bezpieczeństwo fizyczne obiektów lądowych, ust 3, pkt 10	W pkt 3 ppkt 10 wprowadza się pojęcie: „testowanie systemów zabezpieczeń technicznych oraz całego systemu bezpieczeństwa fizycznego infrastruktury krytycznej". **Proponuje się rozważyć doprecyzowanie sposobu testowania systemów bezpieczeństwa fizycznego.**	
3	KIGEiT	Załącznik. I. Bezpieczeństwo fizyczne obiektów lądowych, ust 4 pkt 4	W pkt 4 ppkt 4 wprowadza się pojęcie: „stosowaniu środków spowalniających dotarcie intruza do stref ochrony". **Proponuje się rozważyć doprecyzowanie co należy rozumieć pod pojęciem środków spowalniających, mając na względzie zapisy z ustawy o ochronie osób i mienia.**	
4	KIGEiT	Załącznik. VI. Cyberbezpieczeństwo systemów sterowania przemysłowego, ust 1 pkt 6)	Obecne brzmienie pkt 6) mówi o fizycznej separacji systemów IT i OT. Proponuje się zmienić zapis ze względu na jego niespójność. Sformułowanie „fizyczną separację (…) z wykorzystaniem bram jednokierunkowych" jest nieprecyzyjne, ponieważ brama jednokierunkowa nie oznacza pełnej fizycznej separacji systemów. Zastosowanie bramy jednokierunkowej w praktyce oznacza istnienie fizycznego i logicznego połączenia między systemami, przy czym komunikacja jest ograniczona do jednego kierunku. Nie jest to więc fizyczna separacja w ścisłym znaczeniu (całkowity brak połączenia), lecz kontrolowana forma komunikacji. Usunięcie wyrazu „fizyczną" eliminuje tę niespójność i pozwala prawidłowo ująć katalog dopuszczalnych sposobów separacji, obejmujący zarówno separację	**6) zapewnia się separację systemów IT i OT poprzez: separację fizyczną lub wykorzystanie bram jednokierunkowych lub logiczną separację systemów IT i OT za pomocą strefy zdemilitaryzowanej (DMZ) z mechanizmami segregacji komunikacji między sieciami OT i IT na potrzeby badania stanu sieci OT i zbierania danych generowanych w ramach tej sieci;**

Lp.	Podmiot wnoszący uwagę	Jednostka redakcyjna, do której wnoszona jest uwaga	Treść uwagi	Propozycja brzmienia przepisu
			fizyczną (jako całkowitą izolację), jak i inne rozwiązania, takie jak bramy jednokierunkowe czy separacja logiczna.	
5	KIGEiT	Załącznik. VI. Cyberbezpieczeństwo systemów sterowania przemysłowego, ust 1	Proponowane jest uzupełnienie rozdziału VI. Cyberbezpieczeństwo systemów sterowania przemysłowego o dodatkowe zapisy. Proponowane zapisy wynikają z konieczności zapewnienia warunków do skutecznej obsługi incydentów bezpieczeństwa w systemach sterowania przemysłowego (OT), w tym incydentów o charakterze poważnym, wymagających zaangażowania CSIRT poziomu krajowego. W takich przypadkach zespoły zewnętrzne nie posiadają bieżącej wiedzy o architekturze i konfiguracji danego środowiska. Brak aktualnej dokumentacji systemu istotnie utrudnia lub wręcz uniemożliwia przeprowadzenie sprawnej analizy incydentu, identyfikację źródła problemu oraz określenie zakresu kompromitacji. W związku z tym konieczne jest zapewnienie utrzymywania dokumentacji technicznej obejmującej warstwę fizyczną, logiczną i usługową, a także interfejsy OT–IT oraz historię zmian. Kluczowe znaczenie ma również prowadzenie aktualnej ewidencji aktywów. Bez pełnej wiedzy o komponentach sprzętowych i programowych wchodzących w skład systemu sterowania przemysłowego nie jest możliwe ustalenie, czy dana podatność faktycznie występuje w środowisku ani jaka jest skala jej wpływu. Brak takiej ewidencji uniemożliwia efektywne zarządzanie podatnościami oraz podejmowanie adekwatnych działań ograniczających ryzyko. Wprowadzenie obowiązku synchronizacji czasu w systemach OT stanowi warunek konieczny dla prowadzenia analizy poincydentalnej. Niespójne znaczniki czasu pomiędzy urządzeniami i systemami uniemożliwiają prawidłowe odtworzenie sekwencji zdarzeń, co bezpośrednio wpływa na jakość i wiarygodność analizy incydentu. Z kolei wdrożenie formalnego procesu zarządzania zmianą ma na celu zapewnienie możliwości jednoznacznej oceny, czy aktualny stan konfiguracji systemu jest zgodny ze stanem zamierzonym, czy też stanowi rezultat nieautoryzowanych działań, w tym działań osoby atakującej. Brak kontroli nad zmianami utrudnia identyfikację anomalii oraz zwiększa ryzyko pozostawania niezauważonych modyfikacji w systemie. Proponowane wymagania mają charakter podstawowy i stanowią warunek niezbędny dla zapewnienia minimalnej zdolności do analizy i obsługi incydentów w środowiskach OT. Jednocześnie regulacje te nie wykraczają poza zakres działań racjonalnych i proporcjonalnych do ryzyka naruszenia bezpieczeństwa.	**Proponuje się dodać pkt 10-13 o brzmieniu:** **„10. Tworzy się oraz utrzymuje aktualną dokumentację techniczną systemów sterowania przemysłowego (OT), wspierającą analizę incydentów oraz odtworzenie przebiegu zdarzeń, umożliwiającą jej wykorzystanie przez wewnętrzne oraz zewnętrzne zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), obejmującą w szczególności** **a) warstwę fizyczną – opis i schematy połączeń infrastruktury, w tym urządzeń, okablowania, punktów dostępowych oraz powiązań między komponentami systemów OT,** **b) warstwę logiczną – architekturę sieci, w tym segmentację, adresację, konfigurację urządzeń sieciowych, wykorzystywane protokoły komunikacyjne oraz zależności między systemami,** **c) warstwę usługową – wykaz systemów, aplikacji i usług funkcjonujących w środowisku OT wraz z ich rolą, konfiguracją oraz powiązaniami,** **d) informacje o interfejsach pomiędzy systemami OT oraz systemami IT, w tym sposobach wymiany danych i mechanizmach zabezpieczeń,** **e) historię zmian wprowadzanych w architekturze, konfiguracji oraz oprogramowaniu systemów OT;** **11. Prowadzi się oraz utrzymuje aktualną ewidencję aktywów wchodzących w skład systemów sterowania przemysłowego (OT), obejmującą w szczególności urządzenia, oprogramowanie wraz z informacjami o wersjach i poziomach aktualizacji, w celu umożliwienia szybkiej identyfikacji komponentów podatnych na znane podatności oraz oceny wpływu tych podatności na funkcjonowanie środowiska OT;** **12. Wprowadza się oraz stosuje procedury zarządzania zmianą w systemach sterowania przemysłowego (OT), obejmujące w szczególności rejestrowanie, zatwierdzanie,**

Lp.	Podmiot wnoszący uwagę	Jednostka redakcyjna, do której wnoszona jest uwaga	Treść uwagi	Propozycja brzmienia przepisu
			Przedmiotowe wymogi odnoszą się do powszechnie uznanych praktyk w obszarze bezpieczeństwa systemów sterowania przemysłowego i nie nakładają nadmiernych obciążeń organizacyjnych ani technicznych. Regulacje te w istocie porządkują i formalizują działania, które powinny być standardowo realizowane przez odpowiedzialnego właściciela systemu OT w ramach należytej staranności w zarządzaniu bezpieczeństwem i ciągłością działania.	**testowanie oraz dokumentowanie zmian w konfiguracji urządzeń, oprogramowania i parametrów systemów OT, wraz z możliwością odtworzenia stanu sprzed zmiany, w celu ograniczenia ryzyka wprowadzenia błędów oraz ułatwienia analizy incydentów;** **13. Zapewnia się synchronizację czasu w urządzeniach i systemach OT z wykorzystaniem wiarygodnego źródła czasu oraz stosowanie jednolitych znaczników czasu w rejestrowanych zdarzeniach, w celu umożliwienia spójnej analizy incydentów i rekonstrukcji zdarzeń;"**
6	KIGEiT	Załącznik. VI. Cyberbezpieczeństwo przetwarzania danych w chmurze obliczeniowej, ust 1	Proponuje się uzupełnić ust. 1 poprzez dodanie dodatkowego pkt. po pkt. 12.	**W przypadku, kiedy dostawca usługi podlega pod The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) cyberbezpieczeństwo przetwarzania danych w chmurze obliczeniowej jest zapewniane poprzez szyfrowanie oparte na kluczach własnych (HYOK, BYOK).**
7	KIGEiT	Załącznik. VI. Cyberbezpieczeństwo przetwarzania danych w chmurze obliczeniowej, ust 1, pkt 8	Proponuje się uzupełnić pkt 8 zawarty w ust 1, poprzez uzupełnienie treści.	8) (…), dostawca zapewnia kontraktowo standard dostępności rozwiązania chmurowego na poziomie nie niższym niż 99%, **przy czym brak zapewnienia deklarowanej dostępności przez dostawcę usługi wiąże się z karami umownymi proporcjonalnymi do strat poniesionych w wyniku niedostępności przez odbiorcę usługi.**
8	KIGEiT	Załącznik. VI. Cyberbezpieczeństwo przetwarzania danych w chmurze obliczeniowej, ust 3	ust. 3 proponuje się dodać dwa dodatkowe pkt.	x) **wymóg posiadania przez podmiot, z którym zawarto umowę zdolności do rozwiązania zidentyfikowanych incydentów cyberbezpieczeństwa w czasie nie dłuższym niż 14 dni, a w przypadku incydentów istotnych w czasie nie dłuższym niż 7 dni.** y) **wymóg bezzwłocznego informowania przez podmiot, z którym zawarto umowę o wszystkich incydentach cyberbezpieczeństwa w infrastrukturze dostawcy, a dotyczących usług lub danych, których właścicielem jest odbiorca usługi.**